

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I
MEĐUNARODNU SARADNJU

MASTER RAD

MREŽNI SKENERI I PROCENA UGROŽENOSTI
RAČUNARSKE MREŽE

Mentor:
Doc. dr Marko Šarac

Student:
Veliša Velović 410478/2011

Beograd, 2015. godine

SADRŽAJ

Uvod	- 4 -
Predmet istraživanja	- 5 -
Opis problema.....	- 5 -
Ciljevi	- 5 -
Motivacija	- 5 -
Potreba za bezbednim informacionim sistemom	- 6 -
Oblast rada	- 8 -
Organizacija master rada	- 9 -
1 Mrežni skeneri, način rada	- 10 -
1.1 Bezbednost računarske mreže	- 10 -
1.1.1 Skeniranje mreže	- 11 -
1.1.2 Procena ranjivosti računarske mreže	- 13 -
1.2 Poređenje mrežnih skenera i opis alata koje ćemo koristiti.....	- 18 -
1.2.1 Usporedni test različitih mrežnih skenera	- 18 -
1.2.2 Kratak pregled ostalih mrežnih skenera i njihove osnovne karakteristike....	- 20 -
1.2.3 NMAP (Network Mapper).....	- 21 -
1.2.4 OpenVAS	- 22 -
1.3 Zaključak ovog poglavlja	- 25 -
2 Predloženo rešenje i metodologija pristupa	- 26 -
2.1 Nedostaci postojećeg sistema sa predloženim rešenjem	- 26 -
2.1.1 Opšta arhitektura.....	- 27 -
2.2 Način implementacije	- 28 -
2.2.1 Definisane obima skeniranja	- 28 -
2.2.2 Procena ranjivosti	- 29 -
2.2.3 Kreiranje izveštaja	- 32 -
2.2.4 Testiranje	- 32 -
2.3 Plan projekta	- 32 -

3 Dizajn i razvoj.....	- 34 -
3.1 Prvi sloj: Osnovni servisi.....	- 35 -
3.1.1 NMAP logika skeniranja	- 35 -
3.1.2 OpenVAS	- 37 -
3.2 Drugi sloj: aplikativni modul.....	- 38 -
3.2.1 NMAP modul	- 38 -
3.2.2 OpenVAS modul	- 39 -
3.3 Treći sloj: aplikativni interfejs (slika 16)	- 42 -
3.4 Predložena rešenja za probleme	- 43 -
4 Rezultati testiranja i analiza.....	- 45 -
4.1 Prvi test: proces procene ranjivosti informacionog sistema.....	- 45 -
4.1.1 Izviđanje mreže.....	- 45 -
4.1.2 Prebrojavanje uređaja na mreži	- 50 -
4.1.3 Pronalaženje otvorenih portova i aktivnih servisa na uređajima	- 52 -
4.1.4 Detektovanje mrežnih propusta	- 54 -
4.2 Drugi test: NMAP modul	- 54 -
4.2.1 Opis testnog okruženja	- 54 -
4.2.2 Plan testa.....	- 54 -
4.3 Treći test: OpenVAS modul	- 67 -
4.3.1 Opis testnog okruženja	- 67 -
4.3.2 Plan testiranja	- 68 -
4.4 Četvrti test: OpenVAS izveštaj skeniranja određenih radnih stanica.....	- 69 -
4.4.1 Zaključak ovog testa.....	- 71 -
5 Zaključna razmatranja	- 72 -
Literatura	- 78 -

Uvod

Kako vreme prolazi svet postaje sve više i više povezano mesto zahvaljujući internetu, razvoju novih tehnologija i jeftinijem procesu proizvodnje. Internet je mreža otvorenog tipa i zbog toga sigurnosti računarskih mreža je posvećena posebna pažnja i pridaje joj se velika važnost. Razvojem novih tehnologija, mreža u oblaku¹, hosting provajdera koji nude sve više i više servisa, došlo se to toga da je danas neisplativo imati ozbiljniji informacioni sistem u manjim i srednjim preduzećima. Dosta organizacija svoje poslovanje prenosi na javnu mrežu, i tu se nalazi ogromna količina ličnih, komercijalnih i jako poverljivih podataka koji se nalaze na servrima i velikim data centrima. Isto tako dosta međunarodnih kompanije svoja predstavništva povezuje širom sveta kako bi u realnom vremenu mogli svi da komuniciraju sa svim zaposlenim. Zbog svega toga preduzimaju se razne mere kako se poverljivi podaci i sama mreža ne bi kompromitovali i kako bi se prava pristupa zabranila neovlašćenim osobama. Pristup mrežnim resursima od strane neovlašćenih osoba ili čak nezadovoljnog zaposlenog može dovesti do namernog uništenja ključnih informacija ili prosledjivanja informacija konkurenciji, što može jako loše uticati na profit organizacije i njen opstanak uopšte. Zbog svega ovoga, bezbednost informacionog sistema se nameće kao jedan od ključnih elemenata svakog preduzeća bez obzira na primarnu delatnost u cilju zaštite intelektualne svojine. Sigurnosne mere informacionog sistema uključuju i skeniranje mreže i analizu ranjivosti mreže, kao i testove penetracije.

Skeniranje računarske mreže je ključno za prikupljanje informacija o realnom stanju klijent/server operativnih sistema, kao i mrežnih uređaja. To je i način za identifikaciju i pronalaženje aktivnih mrežnih uređaja sa krajnjim ciljem da se uradi i procena bezbednosti meže. **Procena ranjivosti** je sistematska analiza bezbedonosnog stanja informacionog sistema. Obe ove tehnike su najsveobuhvatnije za reviziju, testove penetracije, izveštavanje i instaliranje zakrpa za informacioni sistem bilo koje organizacije.

Skeniranje računarske mreže i testiranje na potencijalne ranjivosti oslanja se na alate i procese za skeniranje računarskih mreža i mrežnih uređaja na ranjivosti. Ove alate i sredstva treba uključiti u sigurnosnu politiku svake organizacije čiji se posao oslanja na informacioni sistem, kako bi se potencijalni propusti i ranjivosti mreže otkrili na vreme, a kasnije preduzele sigurnosne mere koje će pružiti odgovarajuću zaštitu informacionog sistema koju organizacija očekuje i zahteva. Mrežni administratori bi trebalo da povremeno sprovedu testove ranjivosti i probojnosti mreže koji bi im pomogli da otkriju propuste u bezbednosti mreže koji mogu dovesti do kompromitovanja važnih informacija ili uređaja ili čak uništena zlonamernim softverom.

Na tržištu postoje razni alati namenjeni mrežnom skeniranju i svaki od njih je poseban za sebe i ima različite izveštaje i načine skeniranja mreže i otkrivanja propusta. Svi ovi izveštaji su uglavnom dosta heterogeni i to dalju analizu i izbor alata čini prilično izazovnim zadatkom. U ovom radu obradjena su dva osnovna mrežna skenera otvorenog koda i to su NMAP² i OpenVAS³. Ova dva alata za mrežno skeniranje mogu da se integrišu i daju pouzdane informacije o stanju mreže iz pristojnog grafičkog okruženja.

Zbog nedostataka koje imaju NMAP i OpenVAS, iskorišćene su prednosti oba ova alata i time su njihove mane prevaziđene. Ova dva mrežna skenera skeniraju mrežu i

¹ Cloud networks

² <https://nmap.org>

³ <http://www.openvas.org>

pronalaže aktivne uređjaje na mreži, njihov operativni sistem i instalirane programe. Pored pronalaženja aktivnih uređjaja na mreži, ovi skeneri takodje pronalaze otvorene portove na uređjajima i pokrenute servise na njima. Dalje skeniranje na ranjivosti se vrši upoređivanjem informacija dobijenih tokom skeniranja mreže sa podacima koji se nalaze u bazi podataka mrežnog skenera i tako se dobija lista potencijalnih ranjivosti koje postoje u informacionom sistemu.

Predmet istraživanja

Opis problema

Prepoznati i identifikovati interne i eksterne pretnje procenom ugroženosti koristeći mrežni skener za procenu ranjivosti. Koristiti grafičko⁴ okruženje kojem se pristupa iz internet pretraživača da bi se otkrile slabosti na klijentskim radnim stanicama, mrežnim uređjajima, mreži.

Istraživanje prepoznaje važnost bezbednosti informacionog sistema i posebno mrežnih skenera današnjice. Cilj je da se poboljša proces procene ugroženosti informacionog sistema i da se smanji opterećenje na mrežne administratore.

Ciljevi

1. Da se uradi sveobuhvatan pregled operativnih sistema i servisa koji opslužuju informacioni sistem;
2. Pronalazak loše konfigurisanih uređjaja na mreži, kao što su loše konfigurisan (nezaštićen) mail server, firewall, itd.
3. Da se identifikuju kritične slabe tačke mreže, bilo na loše konfigurisanim radnim stanicama ili na serverima.

Alati i tehnologija koju koriste:

1. NMAP, OpenVAS, PHP, MySQL;
2. Testno okruženje: Informacioni sistem „Wurth“ d.o.o. Beograd

Motivacija

Informacioni sistem je nešto znatno više od hardvera i softvera koji ga pokreće. On obuhvata polise i procedure jednog preduzeća ili organizacije prema kojima se taj hardver i softver konfigurišu i koriste. Informacioni sistem se konfiguriše prema zahtevima i potrebama zaposlenih i on živi sa kompanijom i vremenom se unapređuje i nadograđuje. Bezbednosni propusti mogu da se pojave na raznim mestima. Kada napadač neovlašćeno upadne u informacioni sistem on koristi propuste u procedurama ili tehnologiji (ili oboje) dozvoljavajući sebi neovlašćeni pristup i neovlašćene radnje. Gubljenje kontrole u mreži se naziva ranjivost mreže ili bezbednosni propust. A kršenje sigurnosne politike mreže od strane napadača se naziva iskorišćavanje sigurnosnog propusta.

Da bi imali sigurnu mrežu, potrebni su mehanizmi koji mogu da ispune sledeće:

⁴ GUI - Graphical user interface

1. Zaštita mrežnih uređaja;
2. Smanjenje bezbednosnih propusta u aplikacijama i klijentskim sistemima koji su na mreži;
3. Zaštita informacija tokom prenosa preko mreže.

Da bi se mreža zaštitila potrebno je preduzeti određene mere koje će smanjiti osetljivost mreže na napade i pretnje. Da bi se obezbedila mreža postoje brojni alati otvorenog koda, kao i oni komercijalni koji znatno smanjuju vreme mrežnim administratorima u pronalaženju potencijalnih propusta i omogućavaju im preventivno delovanje i zaštitu mreže pre no što se napad dogodi.

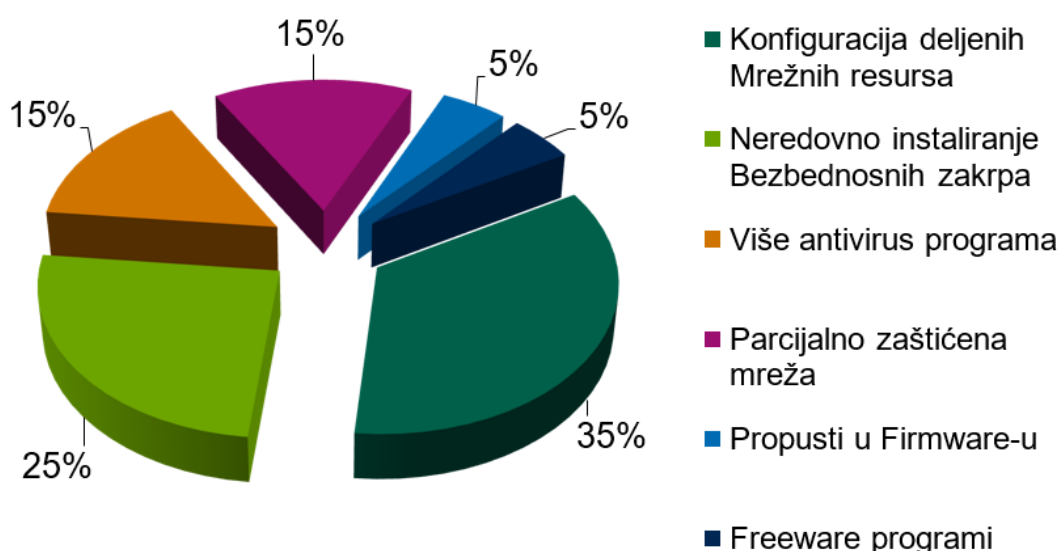
Potreba za bezbednim informacionim sistemom

Svrha politike bezbednosti informacionog sistema neke organizacije biće jasnija kada se pokažu i razlozi kako neka računarska mreža postaje ranjiva:

1. Kompleksnost: Mnogo je više propusta i nenamernih pristupnih tačaka u velikim i kompleksnim mrežama
2. Poznavanje: koristeći standardni, dobro poznati softver, operativni sistem i/ili čak i hardver povećava verovatnoću da napadač već poseduje znanje ili vrlo lako može da pronadje alate da iskoristi propust u mreži
3. Povezanost: više fizičkih konekcija, privilegija većem broju korisnika, otvorenih portova, primena različitih protokola i servisa povećava ranjivost mreže
4. Politika korisničkih lozinki: krajnji korisnici uglavnom koriste slabe lozinke koje se lako mogu otkriti i najprimitivnijim napadima kao što je „brute force“. Zatim korisnici čuvaju svoje lozinke na računaru gde se programom može lako pristupiti i koriste iste lozinke za različite programe i sajtove.
5. Osnovne mane operativnih sistema: dizajneri operativnih sistema podrazumevane vrednosti istih ne postavljaju na najviši nivo kako bi olakšali rad korisnicima, naročito kućnim. Tako na primer operativni sistem sa podrazumevanim vrednostima dozvoljava svakom programu i svakom korisniku puna prava pristupa celokupnom sistemu. Mana operativnog sistema je ta što će dozvoliti i virustima i malverima da svoje komande izvršavaju kao administratori.
6. Internet pretraživanje: pojedini sajtovi sadrže štetne špijunske programe koji se instaliraju na računar automatski pri poseti sajtu. Oni kasnije prikupljaju podatke i šalju ih tvorcu ovog programa.

7. Greške u softveru: programeri prilikom pravljenja softvera mogu napraviti propuste koji mogu dovesti napača da kroz tzv. zadnja vrata⁵ pristupi računaru i na taj način zloupotrebi nenameran propust u aplikaciji.
8. Neproveren pristup korisnika.

Istraživanje[18] koje je sproveda poznata antivirus kompanija „Kasperski“ označila je malware koji se učestalo vraćaju i nakon čišćenja kao problem na koji se žale mnogi korisnici. Zaposleni kompanije „Kasperski“ razvili su antivirus softver koji je u stanju da efikasno ukloni viruse, malware i ostale zlonamerne programe, ali problem predstavlja to što se kroz isti propust u mreži, radne stanice ponovo inficiraju istim zlonamernim soferima. Najveći procenat od čak 35% incidenata dešava se zato što mrežni administratori previde prava koja daju deljenim mrežnim resursima tako što mnogi korisnici imaju izvršna prava i prava pisanja u zajedničkim direktorijumima. U ovakvim slučajevima može se desiti da se na određenim direktorijumima postavi potpun pristup svim korisnicima mreže kako bi lakše mogli da koriste javne dokumente, oglasnu tablu i slično.



Izvor: Kaspersky Lab

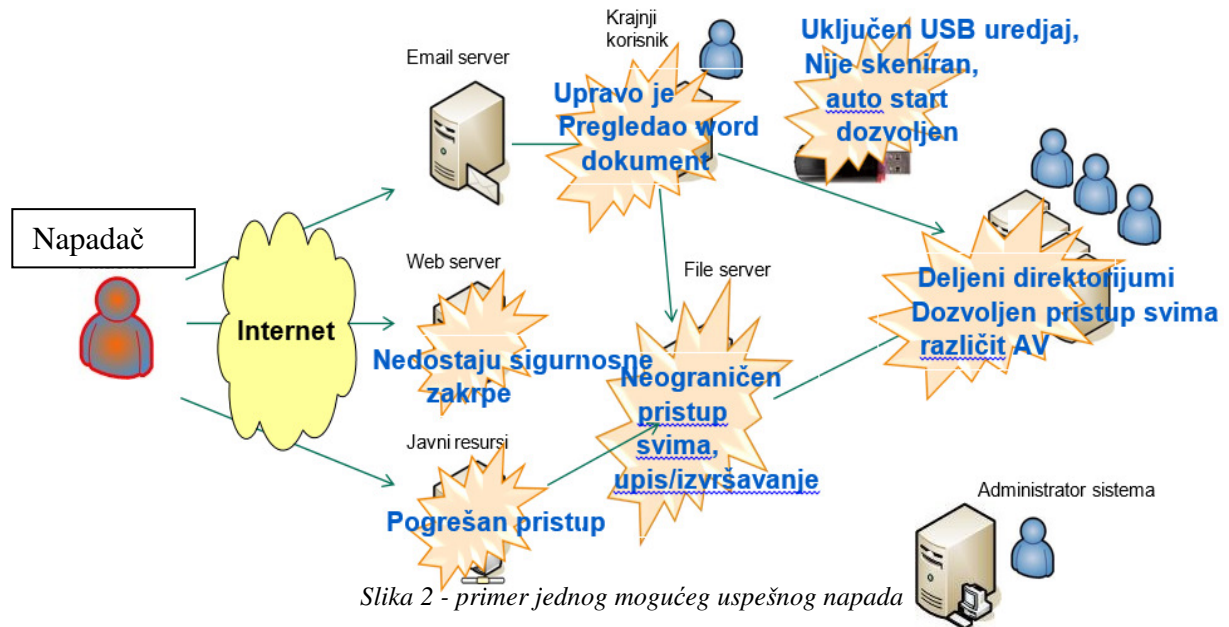
Slika 1 - Istraživanje kompanije Kasperski

Mreža kojoj fali samo jedna bezbednosna zakrpa proizvođača softvera može biti u velikoj opasnosti. Nažalost, ovo je čest slučaj u svim organizacijama, jer se mrežni administratori pribojavaju potencijalnih problema koji dolaze sa novim zakrpama žele prvo da testiraju te zakrpe na manjem broju računara kako bi videli da li će naići na probleme. zbog ovog tipa propusta, čak četvrtina računara se zarazi.

Korišćenje više različitih antivirus rešenja u različitim delovima mreže uzrok je 15% ukupno zarađenih mreža. Problem kod različitih dobavljača zaštitnog softvera je u

⁵ backdoor

tome što se može desiti da jedan alat odreaguje kasno na novonastale pretnje i time zarazi celu mrežu. Ne izbacuju svi antivirus proizvođači zavrpe redovno, a nekada se može desiti da prodju nedelje, čak i meseci dok se ne reši propust. Delimično zaštićena mreža predstavlja mrežu gde je antivirus softver instaliran na jednom delu mreže, ostavljajući ostatak mreže nezaštićenim. Ovakav tip propusta odgovoran je za 15% zaraženih računara.



Propusti u firmveru se dešavaju na 5% uredjaja i dešavaju se kada mrežni administratori ne prate sve uredjaje za koje su zaduženi. Ovo se odnosi na rutere, zaštitni zid, mrežne štampače, svičeve. S vremena na vreme proizvođači hardvera objavljuju nove verzije i rešavaju neke probleme sa uredjajima, ali velika većina IT stručnjaka se ne obazire na nadogradnju firmvera dok ne nastane problem.

Oko 5% sigurnosnih incidenata se dešava zbog besplatnog softvera koji se preuzima sa interneta. Kroz ovaj tip softvera se uglavnom kao opcija nude i još neka dodatna funkcionalnost ili ekstenzija za internet pregledač, koji su u stvari zlonameran softver koji ostaje na računaru.

Tako da i pored antivirus zaštite, mreža treba da se maksimalno obezbedi i da se s vremena na vreme njena sigurnost proverava. Mrežni skeneri mogu umanjiti slabosti radnih stanica i problema koji uzrokuju krajnji korisnici tako što će izolovati i pokazati na koje interne i eksterne pretnje je sistem ranjiv.

Oblast rada

Cilj ovog rada je da prateći zahteve organizacije napravim bezbednosnu procenu koristeći grafičko okruženje alata za skeniranje mreže.

Cilj:

1. Proveriti konfiguraciju uredjaja;
2. Procena ranjivosti mreže;

3. Automatsko skeniranje mreže.

Očekivanja od konačnog izveštaja:

1. Skeniranje portova i identifikacija svih pokrenutih servisa;
2. Skeniranje ranjivosti mreže;
3. Istraživanje poznatih propusta pokrenutih servisa;
4. Otkrivanje lozinki metodom „Brute force“
5. Generisanje svih zapisa za konačan izveštaj

Organizacija master rada

Nakon ovog uvoda, poglavlje 1 predstavlja osnovno znanje o mrežnim skenerima. To uključuje istraživanja dosadašnjeg rada do danas u domenu mrežnih skenera i procene ranjivosti koji su relevantni za ovaj rad.

Poglavlje 2 predlaže pristup koji se zasniva na postavljanju pitanja i zaključak koji se nalazi na kraju poglavlja. Ovde je opisan plan projekta, implementacija i metode testiranja.

U trećem poglavlju je predstavljena arhitektura i korišćenje alata koji su razvijani.

U 4. poglavlju predstavljen je testni uzorak i rezultati skeniranja. U ovom poglavlju dokazano je kako ovi alati rešavaju pitanja razmatrana u poglavlju jedan.

Poslednje 5. poglavlje zaključuje tezu diskusijom ograničenja ovih alata i kakva se poboljšanja mogu očekivati u budućnosti.

1 Mrežni skeneri, način rada

Povezanost sa različitim otvorenim mrežama, kao što je internet omogućava korisne kanale kroze koje napadač može doći do neke interne mreže i napraviti problem krajnjim korisnicima. Štaviše i sami korisnici privatne mreže mogu nesvesnim radnjama podrivati bezbednost i sigurnost mreže. Ukoliko postoji mogućnost da je samo jedan uređaj na internoj mreži kompromitovan, on može ugroziti kompletnu mrežu. Tako da internet, kao i intranet omogućavaju jako pogodne kanale kojima napadači (i eksterni i interni) mogu kompromitovati informacioni sistem. Zbog toga bezbednost informacionog sistema igra jako važnu ulogu svake organizacije.

1.1 Bezbednost računarske mreže

Bezbednost računarske mreže uključuje odbranu i od eksterne i od interne pretnje sa punim paketom zaštitnih mehanizama koji se bore protiv opasnosti na mreži. U ove zaštite uključujemo sledeće mehanizme:

1. Fizičko-tehničko obezbeđenje server sale i mrenih uređaja;
2. Tehnička kontrola unutar mrežne infrastrukture da bi se smanjila njena ranjivost na sigurnosne pretnje;
3. Kontrole koje se primenjuju u okviru životnog ciklusa neke akcije da bi se otkrile pretnje koje ugrožavaju mrežnu infrastrukturu;
4. Informacije i bezbednosne procedure koje se koriste da bi se detektovali bezbednosni incidenti, reagovalo na njih i u najgorem slučaju procedure za oporavak nakon bezbednosnog incidenta.

Kontrole na spoljne pretnje mrežne bezbednosti praktično se sprovode na zaštititi spoljnih mrežnih interfejsa. Zaštite koje se sprovode unutar mreže namenjene su da detektuju, reaguju i oporave od napada i pretnji iz unutrašnje mreže i da daju detaljnu analizu odbrane od spoljnih opasnosti.

Bezbednost mreže se zasnica na specifičnim principima i konceptima koja se odnose na sredstva zaštite. Pre svega, upoznaćemo se sa najčešćim terminima i njihovim definicijama koje se tiču zaštite imovine i intelektualne svojine:

Digitalna imovina – Digitalna imovina je bilo koja datoteka na mreži ili eksternom uređaju koja je bitna nekoj organizaciji[18]. Kada ynamo koju digitalnu imovinu treba da štitimo, koja je njena vrednost, gde se nalazi i kome je sve izložena, određeno vreme, radni sati i novac mogu biti utrošeni u obezbeđivanje digitalne imovine.

Ranjivost – Ranjivost se može pokazati kao mana ili slabost bilo koje aplikacija koja je instalirana na mreži i čiji bagovi mogu dovesti do toga da napadač pristupi mreži i izvede nepoželjne operacije ili neovlašćeno pristupi poverljivim dokumentima[18]. Prisustvo ranjivih aplikacija predstavlja pretnju korisniku aplikacije jer ona može dovesti do kompromitovanja podataka i informacija. Primer: Buffer Overflow.

Pretnja – događaj ili radnj koja može ugroziti sigurnost[18]. Pretnja se može opisati i kao potencijalno kršenje bezbednosti. Primer: virusi.

Rizik – rizik predstavlja verovatnoću da će upotrebom specifične vrste napada doći do neželjene ranjivosti sistema koja će za kasnije imati nepoželjne posledice. Ukoliko ranjivost u sistemu postoji, ali nema pretnje koja tu ranjivost može da iskoristi, onda praktično nema ni rizika.

Napad – Bilo koja aktivnost na mreži koja pokušava da naruši bezbednost mreže. Primer: Brute force napda [18].

Eksplloit – Deo neke komande ili deo podatka čiji je cilj da iskoriste manu ili ranjivost u bilo kojoj aplikaciji. Primer: MS 12-020 RDP eksplloit [18].

U trenutku kada se bezbednos mreže planira / ocenjuje / ispituje, mrežni administrator mora biti svestan sledećih stvari:

1. Pretnje (ili mogući napadi) koji mogu komrpomitovati bezbednost mračunarske mreže;
2. Povezani faktori rizika od raznih pretnji. Ovo se odnosi na to koliko su te pretnje relevantne na određeni sistem;
3. Rashodi koji su potrebni da bi se preduzele sve potrebne bezbednosne mere u cilju zaštite od pretnji;
4. Trošak u odnosu na dobit preduzeća da bi se donela odluka da li je isplativo finansirati sve bezbednosne mere i reduzeti sve te korake.

Sada ćemo se upoznati sa konceptima vezanim za mrežnu bezbednost i to:

1. Mrežni skeneri;
2. Procena ranjivosti;
3. Testovi penetracije.

1.1.1 Skeniranje mreže

Mrežni skeneri ili enumeracija mreže⁶ je kada koristeći odredjeni softver sistematizujemo podatke i dolazimo do korisničkih imena, naziva računara, deljenih mrežnih resursa i servisa. Mrežno skeniranje ili sigurnosno mrežno skeniranje je čitav paket raznih programa različitih proizvođača koje uključuje širok spektar alata za praćenje mreže, nadgledanje sigurnosti mreže, pronalaženje ranjivih delova računarske mreže i još mnogo toga što sistem administratori treba da koriste u svom svakodnevnom radu kako bi preduzeli sve preventivne korake da ne bi došlo do kompromitovanja mreže. Da bi se pronašli propusti koji se ne nalaze na HTTP i HTTPS portovima (koji su standardno otvoreni na svim sistemima), neophodno je da se mrežni skener pokuša povezati i na druge portove i da pokuša slanjem posebno kreiranih paketa da ispita propuste na mreži.

U suštini, ovi alati mogu se podeliti u 6 osnovnih grupa i to:

⁶ Enumeraija ili nabranjanje je termin koji se koristi u matematici ili u informatici i znači isto što i nabranjanje koje ima konačan broj. U našem slučaju se to odnosi na mrežne portove.

1. **IP skener:** IP skener je alat koji se koristi da bi se proverilo da li je odredjeni uredjaj dostupan na mreži. Takodje se koristi da se proveri da li mrežna kartica na računaru na kojem ima pristup mreži, kao i da se proveri brzina mreže. Ping alat funkcioniše tako što šalje „echo zahtev“⁷ koristeći ICMP⁸ protokol ka ciljnom uređaju i čeka na ICMP odgovor. Dalje se meri vreme od slanja paketa do prijema odgovora i beleži ukoliko je došlo do gubitaka paketa. Rezultati operacije se ispisuju u statističkom obliku, uključujući minimuma, maksimum i srednje povratno vreme. Ping ne ocenjuje niti izračunava vreme za uspostavljanje veze, već samo daje srednje vreme na već uspostavljenoj vezi. Ping alatka može biti zloupotrebljena kao jednostavni oblik hakerskog napada za uskraćivanje servisa⁹ u obliku ping poplava¹⁰, u kojima napadač zagušuje žrtvu sa ICMP echo zahtev paketima.
2. **Skener host računara:** Ovaj skener može da skenira i da prepozna aktivne host računare i pretpostavi koji operativni sistem koriste, kao i koji su sve programi instalirani na njima. Pored identifikovanja računara na mreži mogu se mapirati i portovi i lista servisa koja je aktivna na računarima.
3. **Provera ranjivosti:** skener za proveru ranjivosti je softver koji je dizajniran da pretraži radne stanice na mreži u potrazi za otvorenim portovima i njihovim potencijalnim propustima. Ovi programi funkcionišu tako što na otvorene portove primenjuju poznate skripte i proveravaju koliko je mreža zaštićena i da li je moguće probiti je sa već poznatim i istraženim metodama. Mrežni administratori ga uglavnom koriste za proveru sigurnosti njihove mreže, a hakeri da bi kompromitovali nečiju mrežu.
4. **Skener portova:** ovo je program koji pretražuje mrežu i pronalazi otvorene portove na njoj. Može biti TCP ili UDP skeniranje. Uglavnom ga koriste administratori mreže da bi proveravali stanje mreže. U TCP/IP mrežnim protokolima radne stanice i servisi koji se pokreću na njima koriste dve komponente: IP adresu i broj porta. Ukupno odvojenih i upotrebljivih brojeva za portove ima 65536. Ograničeni opseg brojeva se koristi od strane većine usluga (ti brojevi su po pravilu manji od 1024), a kada neki novi servis postane dovoljno važan, eventualno će dobiti svoj broj od autorizovanog tela za dodelu brojeva portovima¹¹.
5. **NSLOOKUP** je program koji koriste i Windows i Linux sistemi da pronađe DNS¹² servere i njihove osnovne podatke, kao što su IP adresa određenog računara na mreži, MX¹³ zapis i NS¹⁴ zapise određenog domena.

⁷ Echo request

⁸ Internet Control Message Protocol

⁹ Denial-of-service

¹⁰ Ping flood

¹¹ Internet Assigned Numbers Authority

¹² Domain Name System

¹³ mail exchanger

¹⁴ Name server

6. **Traceroute** je alat koji se koristi da bi se saznala putanja kojom se kreću paketi kroz određenu mrežu. Analitičari koriste ovu komandu da bi prikupili podatke o mrežnoj infrastrukturi. Ovaj program nam daje podatke o arhitekturi mreže tako što obeležava putanju kojom su se kretali paketi. Ovaj alat se često koristi kada treba rešiti neke probleme u mreži kada uređaji ne komuniciraju međusobno ili kada cela mreža jako uspori. Da bi se identifikovala putanja kojom se paket kretao u mreži, paketi korisniku šalju listu rutera kroz koje su prošli. Ova komanda pomaže da se pronađu problemi sa ruterima ili zaštitnim zidovima koji blokiraju saobraćaj. Ova komanda se koristi i za testove penetracije kada napadači žele da otkriju strukturu mreže.

1.1.2 Procena ranjivosti računarske mreže

Procenom ranjivosti mreže IT stručnjaci dobijaju povratne informacije koje se tiču potencijalnih bezbednosnih propusta i omogućavaju im da vide mrežu na način na koji to vide potencijalni zlonamerni korisnici (hakeri). Na ovaj način može da se vidi potencijalni prostor za napad uskraćanjem servisa ili dobijanju informacija koristeći analizator paketa¹⁵. Mrežni skeneri uglavnom imaju i ocene za sve propuste koje uoče i tako daju manje ili veće prioritete potencijalnim opasnostima dodeljujući im manju ili veću ocenu na osnovu toga šta potencijalni haker može učiniti ako iskoristi baš taj propust u mreži. Ovo omogućava mrežnim administratorima da odrede prioritete i da krenu da ispravljaju stvari koje su od najvećeg bezbednosnog rizika ka manjem.

U proceni ugroženosti mreže bitno je znati koji su to ranjivi delovi mreže, koji su tipovi propusta koji mogu biti pronađeni i kako se oni kategorišu. Takođe, bitno je napomenuti i koji su to alati koji su korišćeni za procenu ranjivosti i njihova ograničenja.

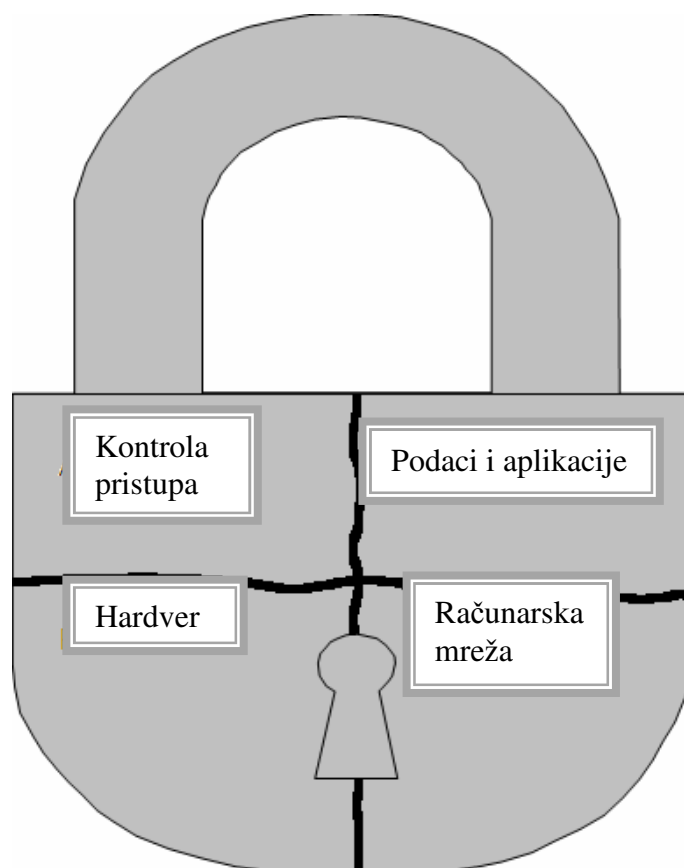
1.1.2.1 Gde sve mreža može postati ranjiva, ranjivi delovi mreže[5]

Prilikom izrade platforme rizika ili procene rizika neke organizacije postoje četiri oblasti ranjivosti. Te oblasti su:

1. Kontrola pristupa;
2. Zaštita podataka i aplikacija;
3. Zaštita hardvera kod klijenta i
4. Zaštita računarske mreže.

Sigurnosni mehanizmi su tehnike i tehnologije koje se koriste u svakoj od ovih oblasti da bi se ispunili uslovi koje propisuju bezbednosne polise. Sigurnosne polise i politika sigurnosti diktiraju nivo zaštite i sigurnosnih mehanizama koji će biti implementirani u informacionom sistemu.

¹⁵ Packet sniffer



Slika 3- ranjivi delovi mreže

Kontrola pristupa: predstavlja proceduru kojom se korisnici predstavljaju mreži, mreža ih prepoznaje i dodeljuje im određene privilegije nad informacijama i resursima. Kontrolisanje kako se te privilegije dobijaju i kako se pristupa resursima je jedna od najbitnijih stvari na koju treba obratiti pažnju kako bi sačuvali privatne i poverljive informacije od neželjenih korisnika. Tehnologije koje se koriste za kontrolu pristupa identifikuju korisnike i potvrde njihov identitet tokom procesa autentifikacije. Sistem kontrole pristupa treba da beleži sve aktivnosti, komunikaciju i transakcije korisnike, kako bi kasnije mogao biti proveren na sigurnosne propuste i nepravilnosti u radu.

Zaštita podataka i aplikacija: ovaj vid zaštite se tiče bezbednosti operativnog sistema, aplikacija koje su instalirane, kao i podataka koji se nalaze na računarima. Cilj je obezbediti što bolju i bržu dostupnost aplikacija i podataka (npr. brz odziv i brzo čitanje iz baze podataka), smanjiti rizik od potencijalnog gubitka podataka i sačuvati integritet podataka.

Neki mehanizmi za ovu vrstu zaštite su unapred definisane i planirane konfiguracije operativnog sistema i aplikacija koje se koriste, redovno instaliranje zakrpa koje se pojavljuju, anti virus, korišćenje anti spam filtera, šifrovanje podataka i digitalno potpisivanje dokumenata.

Hardverska zaštita: ovaj vid zaštite se odnosi na fizičko tehničko obezbeđenje samog hardvera kod korisnika. Potencijalne pretnje mogu biti krađa uređaja, manipulacija podacima obelodanjivanje podataka u javnosti ili uništavanje podataka.

Zaštita računarske mreže: ovaj vid zaštite se odnosi na pokušaje napada u mreži, a i na zaštitu od napada na mrežne protokole. U napadima na računarsku mrežu dolazi do pokušaja da se kompromituje sistem kroz mane u internet protokolima. Ovi napadi se uglavnom koriste kako bi se pristupilo sistemu, aplikacijama i podacima koji se nalaze na mreži. Ovi napadi mogu biti sprovedeni tako da izazovu otkaz servisa kako bi odvratili korisnike da pokušavaju da pristupe mrežnim resursima. Prvi napad na mrežu spolja je uglavnom ulaznica u računarsku mrežu, a kasnije slede napadi na određene klijente ili dalje na mrežu.

1.1.2.2 Tipovi ranjivosti

Za svaki ranjivi deo mreže pomenut u prethodnom poglavlju, koji se deli pos mestu nastanka ranjivosti, postoje i četiri vrste ranjivosti i to[2]:

1. Ranjivost hardvera – uključuje fizičku interakciju sa samim hardverom, a može se odnositi na uklanjanje uređaja, poplavu ometanje saobraćaja, fizički napad;
2. Ranjivost softvera – Ovde može doći do ugrožavanja bezbednosti brisanjem softvera, modifikacije koda logičkim bombama, trojanski konji, virusi, curenje informacija usled greške u dizajniranju softvera itd.
3. Ranjivost podataka – sigurnost podataka se obezbeđuje poverljivošću, tako da neovlašćeno objavljivanje podataka može izazvati problem. Za jako bitne podatke u računarskom sistemu važno je predvideti kolika je mogućnost gubljenja podataka od strane hakera tako što će se izvesti napadi na mrežu i proveriti sigurnost iste. Za jako osetljive podatke najčešći sistem zaštite je šifrovanje podataka. Ranjivost podataka može biti u vidu gubljenja podataka, neovlašćenog pristupa ili hakovanjem sistema od strane hakera.
4. Ranjivosti bazirane na veb aplikacijama – veb aplikacije i servisi su najčešći način da kompanije svoje servise i podatke učine dostupnim na internetu. Nažalost, sa većim brojem aplikacija i servisa i porastom njihove kompleksnosti, raste i broj i kompleksnost ranjivih delova ovih aplikacija i jako je važno imati dobru zaštitu i konstantne provere ovih sistema.

1.1.2.3 Kategorije ranjivosti

Svaki poznati mrežni propust se mapira i beleži u određenu kategoriju ranjivosti [15], a njihov spisak je prikazan u tabeli 1. Ove kategorije uključuju propuste, potencijalne propuste i informacije prikupljene tokom provere. Kada određenu mrežnu ranjivost možemo svrstati u više različitih kategorija [19] servis određuje koja kategorija najviše odgovara tom tipu propusta i dodeljuje je toj kategoriji. Prema podacima sajta <http://www.internetbankingaudits.com/> 99% neovlašćenih provala u mrežne sisteme radi se kroz već identifikovane i poznate propuste.

<i>Tabela 1: Kategorije mrežnih ranjivosti</i>				
BACK DOORS AND TROJAN HORSES	BRUTE FORCE ATTACK	CGI	DATABASE	DNS AND BIND
E-COMMERCE	FILE TRANSFER PROTOCOL	FINGER	FIREWALL	GENERAL REMOTE SERVICES
HARDWARE	INFORMATION (NIS, YP, WHOIS)	INFORMATION GATHERING	MAIL SERVICES	NEWS SERVER
NFS	PROXY	RPC	SMB / NETBIOS	SMTP AND MAIL SERVER
SNMP	TCP/IP	WEB SERVER	WINDOWS	X-WINDOW

Izvor: <http://www.internetbankingaudits.com/domains.htm>

1.1.2.4 Tipovi mrežnih skenera

Postoje dva tipa mrežnih skenera, aktivni i pasivni [2].

Aktivni skeneri prenose pakete to mrežnih čvorišta, a kasnije ispituju odgovore koje dobiju i detaljno ih obrađuju da vide da li određeni uređaj u mreži predstavlja slabu tačku mreže ili ne. Mrežni administratori takođe mogu da koriste aktivne skenere da simuliraju napad na mrežu i tako otkriju potencijalne slabosti mreže koje bi hakeri mogli da otkriju ili da ispituju napadnuti uređaj u mreži i da otkriju propust koji je zlonamerni korisnik već iskoristio da kompromituje mrežu. Aktivni skeneri mogu čak i da preduzmu određene akcije i da samostalno reše sigurnosne probleme tako što bi blokirali potencijalno opasne IP adrese.

Pasivni skeneri identifikuju aktivne operative sisteme, aplikacije i otvorene portove u mreži, prateći aktivnosti svih njih da bi detektovale mrežne propuste. Ovi skeneri mogu da pruže informacije o propustima, ali ne mogu da preduzmu ništa da bi rešili probleme. Ovi skeneri mogu proveriti trenutne verzije softvera na mrežnim uređajima i obavestiti nas o zastarelim verzijama softvera koje predstavljaju potencijalnu metu hakerima ili trojanskim napadima i upute nas na adresu odakle možemo preuzeti najnovije softverske zakrpe za date aplikacije. Sistem administratori mogu ovaj tip skenera podesiti da rade neprekidno ili da skeniraju mrežu u određenom intervalu.

1.1.2.5 Ograničenja mrežnih skenera

Kod mrežnih skenera postoji i određen broj ograničenja i mana koje ćemo pomenuti[19].

Iako su mrežni skeneri od velike pomoći za testiranje bezbednosti mreže, oni ipak ne mogu zameniti znanje koje poseduju IT stručnjaci. Ovi skeneri ponekad mogu dati i pogrešne pozitivne rezultate i preporučiti problem tamo gde on ni ne postoji, kao i pogrešne negativne rezultate, kada skener zanemari stvarni bezbednosni propust. IT

stručnjaci treba detaljno da pregledaju izveštaje koje dobiju od mrežnih skenera kako bi ustanovili da li postoje i nepravilni rezultati i nešto što su skeneri možda preskočili.

Drugi problem mrežnih skenera je autentifikacija. Čak i kada su ispravno konfigurisani i prijavljeni na mrežu sa punim pravima, oni mogu da detektuju samo one propise koji su već poznati, opisani i kategorisani i nalaze se u biblioteci propusta. S druge strane iako anonimno (neautentifikovano) skeniranje ima neke prednosti, neuspeh da iskoristi autentifikovano skeniranje, drastično smanjuje efikasnost skenera. Autentifikovano skeniranje je skeniranje kada skener poseduje prava pristupa celoj mreži, uključujući i aktivni direktorijum, SSH pristup itd.

Treći ključni problem ovih skenera je to što ne mogu da rade sa aplikacijama rađenim po narudžbini koje se ne nalaze u široj ponudi na tržištu. Ranjivosti bazirane na CVE¹⁶ su vrlo mali skup ranjivosti u odnosu na prostor koji napadači imaju kada planiraju napad. Sigurnosne provere postoje samo za najpoznatije i najšire korišćene aplikacije i operativne sisteme koji se nalaze u mreži, ali šta raditi sa aplikacijama koje organizacije razvijaju za svoje potrebe ili koje im izrađuju programeri po narudžbini? Ovakve aplikacije se nalaze svuda i variraju od ključnih aplikacija za posao preduzeća do malih dodatnih programa za jednokratnu upotrebu koje su i najčešće veoma ranjive. Sve ove aplikacije se nalaze ispod radara modernih skenera i za aplikacije rađene po narudžbini ne postoje CVE biblioteke.

Iako ovi skeneri uglavnom mogu otkriti i obavestiti nas šta je potencijalna ulazna tačka napadača, oni su vrlo ograničeni u predviđanju kompleksnih radnji koje napadač može preduzeti u pokušaju da kompromituje računarsku mrežu. Prvi korak napadača će biti da nađe najslabiju tačku u našoj mreži i da je iskoristi (to može biti softver bez novih zakrpa, ranjivosti raznih aplikacija ili sama konfiguracija mreže). Kada napadač iskoristi ovaj propust i dođe makar do jednog korisničkog naloga u mreži ili makar jednog sistema, on će pokušati sa tog sistema da otkrije sledeće propuste kako bi došao do podataka na mreži koji mu trebaju. Ni jedan mrežni skener današnjice nas neće upozoriti na pokušaje i korišćenje jednog istog naloga i lozinke na mreži na različitim uređajima u kratkom vremenskom roku. A nakon inicijalnog kompromitovanja mreže, ovo je najčešći način kojim napadači dolaze do podataka pretražujući mrežu.

Konačno, svi mrežni skeneri ukoliko skeniraju celu mrežu, a to moraju da rade u radno vreme, kada su svi uređaji u funkciji i normalnom režimu rada, zauzimaju jako veliki propusni opseg i potencijalno mogu usporiti celu mrežu.

1.1.2.6 Poređenje između skeniranja mreže, procene ranjivosti i testova penetracije

Skeniranje mreže se sastoji od raznih uslužnih programa. Skeniranje ne predstavlja rupu u mreži, već moguće posledice ranjivosti mreže ili napada.

Procena ranjivosti predstavlja metodologiju identifikovanja i prebrojavanja propusta u mreži. To je detaljna procena stanja mreže, koje nam pokazuje moguće nedostatke mreže i daje nam dobre i detaljne smernice kako da te nedostatke otklonimo ili njihov rizik svedemo na prihvatljiv nivo[9]. Da bi smo sve to ostvarili većina procena ranjivosti se pokreće nakon ovih standardnih koraka:

¹⁶ Common Vulnerabilities and Exposures

1. Katalogizacija sredstava i digitalne imovine u mreži;
2. Procena vrednosti svih mrežnih resursa i digitalne imovine;
3. Identifikovanje propusta ili potencijalne opasnosti svakog od ovih resursa;
4. Ublažavanje ili uklanjanje većine istinskih propusta za najvrednije resurse u mreži.

Nakon toga testovima penetracije simuliraju se interni i eksterni napadi koji se očekuju od potencijalnog napadača i pokušava se probiti sigurnosna barijera određenog informacionog sistema. Koristeći razne alate i tehnike, osobe koje se bave testovima penetracije pokušavaju da se probiju u mrežu i da dođu do osetljivih podataka. U zavisnosti od dogovora, ovi testovi mogu ići toliko daleko da će uključiti i socijalni inženjering na zaposlenima, kao i pokušaj proboja fizičko-tehničkog obezbeđenja.

Glavna razlika između testa procene ranjivosti mreže i testa penetracije je da se sa testom procene ranjivosti pitamo: „Koje su naše slabosti i kako to da popravimo?“, a testom penetracije se pitamo: „Može li neko probiti sistem zaštite i upasti u našu mrežu i šta može ugroziti tim upadom?“

Procenom ugroženosti mreže pokušava se unaprediti bezbednost mreže i delovati tako da se još više poboljša sigurnosna politika i smanji rizik od potencijalnog neovlašćenog upada u mrežu. S druge strane testom penetracije dobićemo samo prikaz trenutnog sigurnosnog stanja u mreži. Zbog ovakvog načina pristupa, testovi procene ranjivosti su mnogo zahvalniji i bolji nego testovi penetracije.

1.2 Poređenje mrežnih skenera i opis alata koje ćemo koristiti

Na tržištu danas postoji znatan broj mrežnih skenera koji se međusobno razlikuju, kako po kvalitetu i načinu rada, tako i po ceni. Predstavićemo najvažnije mrežne skenere i njihove glavne osobine[21]. Zbog besplatne licence i kvalitetnog softvera, smatram da je najbolji izbor za mrežni skener **OpenVAS** i **NMAP** čiji su detaljniji opisi dati na kraju poglavlja.

1.2.1 Uporedni test različitih mrežnih skenera

Hackertarget.com[13] 2012. godine je testirao i uporedio najvažnije mrežne skenere današnjice. Među njima su se našli Nessus, OpenVAS, Nexpose i NMAP. Test je sproveden na virtualnoj mašini za koju se poznaju sve ranjivosti od ranije i koja je služila za testiranje.

Način testiranja i podešavanje skenera:

1. Testiranje se radilo sa OpenVAS verzijom 5, kompletno skeniranje svih TCP portova sa Nmap-om i najvažnijih 100UDP portova. Nisu instalirani nikakvi dodaci na OpenVAS osim Nmap-a.
2. Drugi alat koji se koristio je Nessus verzije 5 koristeći eksterni profil za skeniranje.
3. Nexpose skener je podešen sa kompletnom proverom.

4. Svim skenerima su podešene podrazumevane vrednosti i nije bilo nikakvojg dodatnog podešavanja.
5. Ovo je bilo eksterno skeniranje, tako da nikakva autentifikacija nije korišćena.

Prvi dobijeni rezultati su pokazali potpuno različite rezultate kod različitih skenera i na prvi pogled uneli konfuziju pre detaljnije obrade. U tabeli 2 su prikazani korektno otkriveni propusti svih skenera nakon filtriranja. Otkriveno je 7 od 15 propusta testiranog sistema i oni su prikazani u tabeli 3.

Tabela 2 - poređenje rezultata, broj propusta koje je svaki skener pronašao

Nessus	OpenVAS	Nexpose	Nmap
7	7	7	6

Izvor: <https://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable/>

Tabela 3 - 7 mrežni propusti otkriveni skeniranjem u testnom okruženju

Sigurnosni propust testnog okruženja	Nessus	OpenVAS	Nexpose	Nmap
FTP 21 Anonymous FTP Access	✓	✓	✓	✓
FTP 21 VsFTPD Smiley Face Backdoor	✓	✓		
FTP 2121 ProFTPD Vulnerabilities		✓		
SSH 22 Weak Host Keys	✓	🔍	✓	
PHP-CGI Query String Parameter Injection	✓	✓	✓	✓
CIFS Null Sessions	✓	✓	✓	✓

INGRESLOCK 1524 known backdoor drops to root shell				
NFS 2049 /* exported and writable	🔍	✅	🔍	
MYSQL 3306 weak auth (root with no password)	✅	✅	✅	✅
RMI REGISTRY 1099 Insecure Default Config				
DISTCCd 3632 distributed compiler				
POSTGRESQL 5432 weak auth (postgresql)				
VNC 5900 weak auth (password)			✅	
IRC 6667 Unreal IRCd Backdoor				✅
Tomcat 8180 weak auth (tomcat/tomcat)	✅		✅	✅

Izvor: <https://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable/>

1.2.2 Kratak pregled ostalih mrežnih skenera i njihove osnovne karakteristike

Nessus – Ovo je jedan on najpopularniji i najposobniji mrežnih skenera, naročito na UNIX sistemima. U početku je bio besplatan, ali su njegovi tvorci 2005. godine zatvorili kod i komercijalizovali su ovaj program. Njegova trenutna cena za jednu licencu godišnje iznosi 2190\$, što je i dalje znatno niže od većine konkurencije. Nessus se konstantno razvija, sa više od 70000 različitih modula.

Core Impact – Ovaj skener se smatra kao najbolje rešenje na tržištu danas. Sadrži ogromnu bazu podataka koja se redovno dopunjuje i poseduje neke funkcije koje ostali skeneri nemaju. Jedna od njih je da kada uspe da se probije do jedne mašine u sistemu, može da uspostavi kriptovani tunel kroz tu mašinu do sledećeg ranjivog uređaja u mreži.

Ostale funkcije vredne pomena su Metasploit i Canvas koji su takođe komercijalni alati. Njegova mana je cena koja počinje od 30000\$.

Nexpose – Rapid7 Nexpose je mrežni skener koji se razvija u smeru da će podržavati sve što je potrebno za istraživanje propusta u mreži i da osim njega neće trebati koristiti druge alate. On podržava pronalaženje mrežnih uređaja, detekciju, proveru, klasifikaciju rizika, analizu uticaja, izveštavanje i ublažavanje visokorizičnih sigurnosnih propusta. Prodaje se kao samostalna aplikacija, virtualna mašina ili kao iznajmljeni servis. Sve opcije su dostupne preko internet pretraivača. Licenca za Komercijalnu verziju košta oko 2000\$ godišnje.

GFI LanGuard – skener koji je razvijen da bi pomogao u održavanju sistema sa najnovijim softverskim zakrpama, praćenju mreže i softvera, i procenama ranjivosti. Cena se bazira po broju IP adresa koje žele da se prate, a besplatna verzija omogućava rad sa do pet različitih IP adresa.

QualysGuard – je popularan po tome što predstavlja softver kao servis. Pravljen je kao internet aplikacija koja nudi opcije otkrivanja mreže i mapiranja, prioritet digitalne imovine, pravljenje izveštaja o proceni mrežne ranjivosti i praćenja sanacije mrežnih propusta u skladu sa rizikom poslovanja.

MBSA – je Majkrosoftov softver koji je prilično lak za korišćenje i predviđen je za rad u malim i srednjim preduzećima da proverava da li su sigurnosna podešavanja mreže u skladu sa preporukama sigurnosne politike Majkrosofta.

Secunia PSI – je besplatan sigurnosni alat dizajniran da detektuje zastarele verzije softvera i njihove propuste, kao i dodatke softveru koji mogu biti izloženi napadima. Napadi na ranjivi softver se vrlo retko blokiraju od strane antivirus programa i zato je ovo dobro rešenje za proveru. Bestplana verzija može biti pokrenuta samo na mašini na kojoj je instalirana, dok komercijalna varijanta može da skenira celu mrežu.

Nipper – nadgleda sigurnost mrežnih uređaja kao što su svičevi, ruteri i zaštitni zidovi. Radi tako što analizira konfiguracione datoteke uređaja koje korisnik mora da mu dostavi. Ovo je prvobitno bila besplatna verzija, a kasnije je njen tvorca komercijalizovao i pokušao da sakrije kod koji je prethodno bio slobodan na tržištu.

SAINT – je skener poput Nessusa i isto kao i Nessus je bio besplatan, ali je danas komercijalan. Za razliku od svih ostalih softvera, SAINT je jedan od retkih skenera koji uopšte ne podržava Windows. Može da radi na Linux i Mac sistemima.

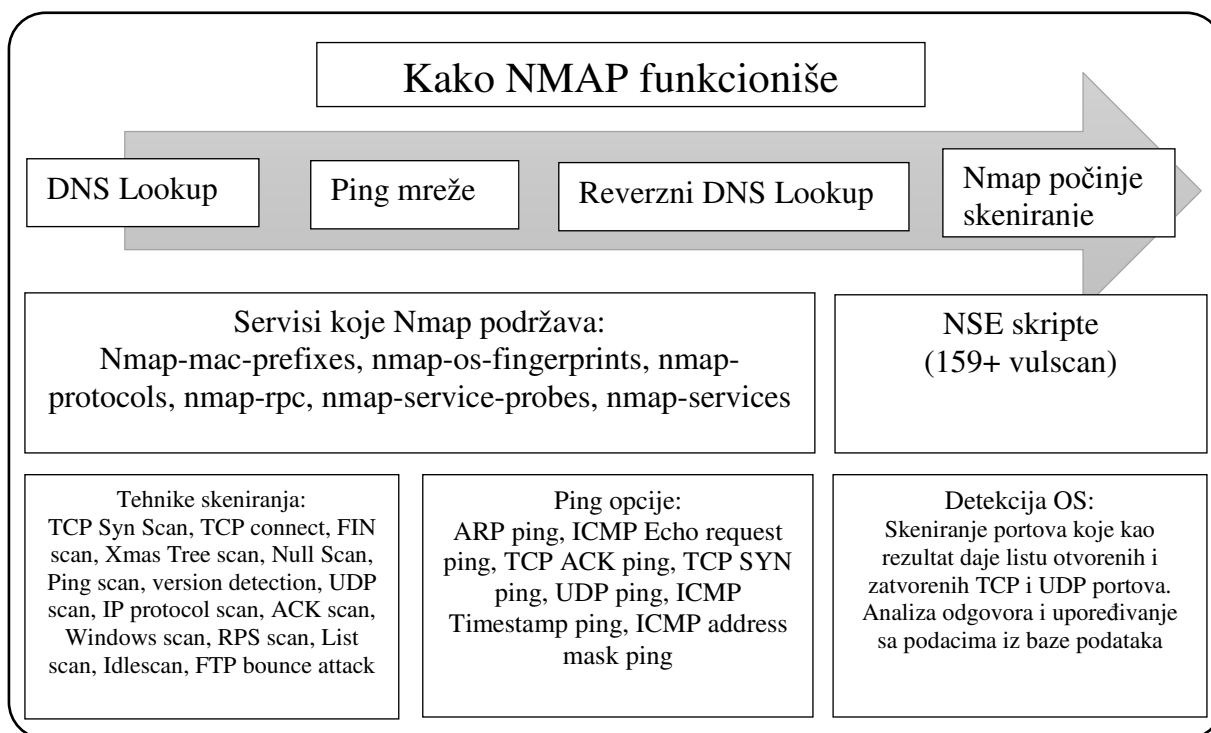
1.2.3 NMAP (Network Mapper)

NMAP je alat koji je besplatan i otvorenog je koda. Koristan je za otkrivanje uređaja na mreži i sigurnosnu proveru. Mnogi mrežni administratori koriste ovaj alat da bi napravili spisak mrežnih uređaja, zatim da bi nadgledali nadogradnju servisa i softvera u mreži kroz zadato vreme, kao i da bi pratili koliko su neki uređaji aktivni na mreži. NMAP koristi IP pakete da bi utvrdio koji uređaji se nalaze na mreži, koje servise ti uređaji koriste, koji operativni sistem je pokrenut na računarima, koji način filtriranja saobraćaja (zaštitni zid) se koristi itd. Dizajniran je tako da vrlo brzo skenira velike mreže i sisteme, ali radi sasvim lepu i na samo jednom računaru. Radi na svim poznatim operativnim sistemima današnjice. Nmap uključuje određen broj različitih alata i to: napredno grafičko

okruženje za pregled rezultata (Zenmap), fleksibilan način transfera podataka, redirekciju i alat za otklanjanje grešaka (Ncat), alat za upoređivanje rezultata skeniranja (Ndiff) i alat za generisanje IP paketa i analizu prihvaćenih odgovora (Nping). Prikaz rada Nmap softvera je predstavljen na slici 4.

Prednosti NMAP softvera:

1. Neograničen broj IP adresa koje možemo skenirati;
2. Lak za instalaciju i korišćenje;
3. Veoma brzo skeniranje.



šematski prikaz rada Nmap softvera

Mane Nmap softvera: najveći potencijalni problem za Nmap projekat može da bude to što je tržište već dovoljno zasićeno sličnim proizvodima, a s obzirom na prirodu zajednice otvorenog koda, moguće je da Nmap neće dovoljno razvijati u budućnosti i da će mu programeri posvetiti manje pažnje.

1.2.4 OpenVAS¹⁷

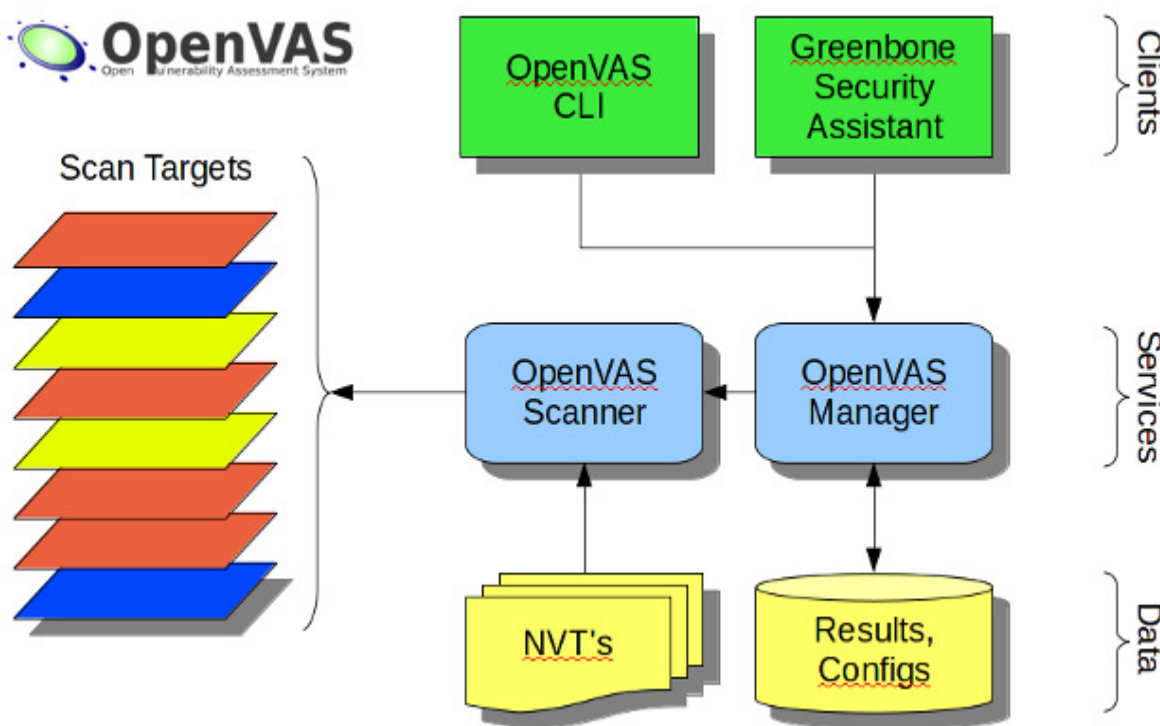
OpenVAS je mrežni skener koji se razvio od poslednje slobodne verzije Nessusa pre no što je ovaj postao komercijalan 2005. godine. Moduli za OpenVAS se i dalje pišu i razvijaju pod Nessusovim NASL jezikom. Ovaj projekat je jedno vreme izgledao zapostavljen, ali se ipak nastavilo sa njegovim razvojem i čestim nadogradnjama. Danas je OpenVas čini okosnicu nekoliko alata i servisa koji pružaju dalekosežne i uticajne mrežne skenre[12]. Ovaj mrežni skener je danas jako popularan i svakodnevno se njegova baza ažurira novim testovima na mrežne propuste. Aprila 2013. godine baza je imala preko 30000 različitih testova. Još jedna bitna karakteristika OpenVas skenera je to što je

¹⁷ Open Vulnerability Assessment System

OpenVas „daljinski skener“ iz razloga što ne mora biti instaliran na klijentskim računarima da bi sproveo test nad njima. OpenVas se instalira i konfiguriše na jednom serveru i odatle skenira sve ostale uređaje u mreži.

Arhitektura OpenVas softvera je prikazana na slici 5. Srce arhitekture ovog softvera obezbeđenog SSL sertifikatom je njegov OpenVAS skener. Skener veoma efikasno sprovodi testove na ranjivost mreže¹⁸ koji se dopunjavaju svakodnevno.

OpenVAS manager je centralni servis koji objedinjuje običan mrežni skener u kompletno rešenje za upravljanje mrežnim propustima. OpenVAS manager kontroliše skener preko OTP¹⁹ protokola, a rezultate dobija u XML formatu. Sva inteligencija ovog skenera je implementirana u OpenVas manager delu tako da je moguće podesiti sve klijente da se ponašaju konzistentno, npr. u vezi filtriranja ili sortiranja rezultata. OpenVAS manager takođe kontroliše i bazu podataka gde se čuva kompletna konfiguracija softvera i rezultati skeniranja. I konačno OpenVas manager takođe kontroliše i prava pristupa korisnika koji se mogu ubacivati u grupe kojima se dodeljuju pravila.



Slika 4- OpenVas arhitektura

Greenbone Security Assistant (GSA) je osnovni veb-servis koji olakšava rad sa OpenVAS platformom. Pristupa mu se iz internet pregledača i pruža na, bogato grafičko okruženje u kojem možemo da organizujemo skeniranje mreže, obrađujemo podatke koje smo dobili skeniranjem itd.

OpenVAS CLI sadrži se od „OMP“ softvera kojem se pristupa iz komandne linije i omogućava nam bolje upravljanje OpenVAS menadžerom, jer možemo kreirati procese

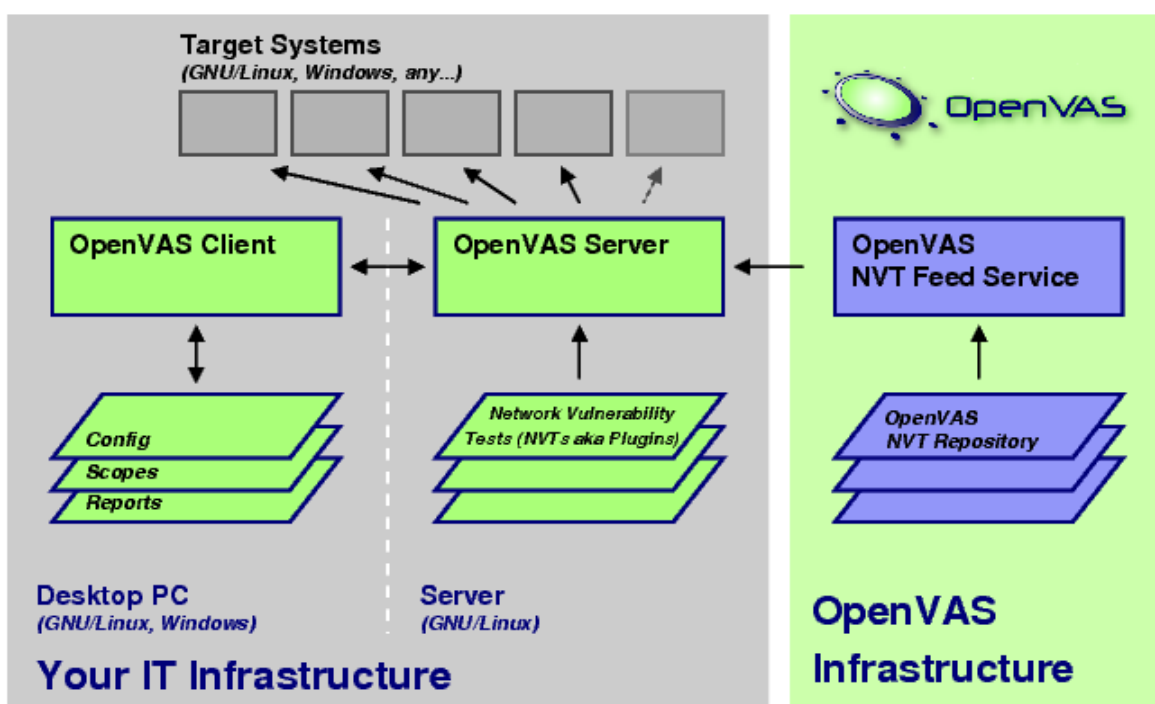
¹⁸ Network Vulnerability tests (NVTs)

¹⁹ OpenVAS transfer protocol

koji se izvršavaju u određenim vremenskim intervalima i zadati mu da odradi nešto u zadato vreme.

1.2.4.1 Rad sa OpenVAS softverom

Većina mrežnog saobraćaja kao što su elektronska pošta i veb-sajtovi obavlja se preko TCP/IP skupa protokola. Da bi se ovaj saobraćaj odvijao nesmetano i da ne bi došlo do preklapanja jednog sadržaja sa drugim, fizička povezanost sa mrežom podeljena je na mnogo logičkih veza koje se zovu portovi. Svi mrežni uređaji mogu imati otvoreno dosta portova, a na nekima od njih rade i neke aplikacije i servisi. OpenVAS radi tako što skenira svaki port na kompjuteru i prikazuje nam šta se na njemu izvršava, tj. koja aplikacija ili servis su pokrenuti. Nakon provere servisa koji se vrti na tom portu, OpenVAS proverava svoju bazu podataka i traži da li za dati port i datu aplikaciju postoji neki poznati propust koji zlonamerni korisnici mogu iskoristiti da nam kompromituju sistem.



Slika 5- Princip rada OpenVAS

Na slici 5[17] je prikazan način rada OpenVAS skenera. Jedan od prvih koraka u planiranju praćenja stanja mreže sa OpenVAS skenerom je testiranje stanja mreže na trenutne testove ranjivosti koji se nalaze u OpenVAS bazi podataka. Drugim rečima, OpenVAS koordiniše izvršavanje velikog broja NVT testova na veliki broj mrežnih uređaja i prikuplja rezultate za sve njih pojedinačno.

Prednosti OpenVAS skenera:

1. Potpuno besplatan, bez obzira na veličinu mreže i broj klijenata;
2. Odlična podrška OpenVAS zajednice;
3. Nakon skeniranja stanja mreže, moguće je napraviti razne izveštaje;
4. Čuva kompletnu istoriju prethodnih skeniranja
5. Koristi se i u ozbiljnim sistemima kao što je Nemačka vlada, tako da nema bojazni za njegov dalji razvoj.

1.3 Zaključak ovog poglavlja

Procena ranjivosti je jedna od osnovnih bezbednosnih procedura koje bi svaka organizacija trebala da implemmentira kako bi osigurala svoju IT infrastrukturu i preudpredila potencijalne napade, kako spoljne, tako i unutrašnje. Ove sigurnosne provere potrebno je ponavljati u određenom vremenskom intervalu i najveće propuste uklanjati pre no što neko zlonameran to iskoristi i napravi mnogo veću štetu od cene koštanja ovih provera.

Na osnovu svega opisanog do sada, naišli smo na sledeće probleme kod ova dva alata koja ćemo koristiti:

Procena ranjivosti: NMAP nema mnogo skripti u svojoj bazi i daje dosta lažnih pozitivnih rezultata.

Kompleksnost instalacije/konfiguracije: OpenVAS je veoma komplikovan i da se instalira i da se konfiguriše za rad. Srećom, od poslednjih nekoliko verzija, postoji već konfigurisana virtualna mašina koja se može preuzeti sa OpenVAS sajta.

Trajanje skeniranja: Detaljno i kompletno skeniranje OpenVAS softverom traje prilično dugo, naročito u većim mrežama.

Većina organizacija bi trebalo da koristi procenu ranjivosti svoje IT infrastrukture u skladu sa svojim mogućnostima i najbolje je testirati okruženje u realnim uslovima kada svi zaposleni obavljaju svoje redovne aktivnosti.

Poređenje rezultata različitih skenera nam je pokazalo značajnu razliku među njima i to da treba da obratimo pažnju na konfigurisanje alata, kao i to da dobijene rezultate detaljno proverimo i razdvojimo lažne pozitivne rezultate od stvarnih pozitivnih, kao i da uočimo one propuste koje su mrežni skeneri preskočili (lažni negativni rezultati).

Po ovako opisanoj metodologiji, proceni ranjivosti treba da pristupati na sledeći način:

1. Konfigurisati mrežne skenere u skladu sa potrebama;
2. Dobijene rezultate analizirati, stavku po stavku;
3. Koristiti dodatne alate, kao što je NMAP (kojim se mogu dobiti dodatni rezultati i/ili dodatni alati). Podešavanjem raznih alata koji su dostupni može se doći do značajnog povećanja obima u otkrivanju i otklanjanju mrežnih propusta.

2 Predloženo rešenje i metodologija pristupa

2.1 Nedostaci postojećeg sistema sa predloženim rešenjem

Na osnovu svega opisanog u prethodnom poglavlju o mrežnim skenerima, sada ćemo se bazirati na moguće probleme i izazove u radu sa OpenVAS i NMAP skenerom koje ćemo koristiti za testiranje naše mreže. Takođe, analiziraćemo i moguća rešenja kako bi pronašli optimalno rešenje za naš mrežni skener. Svaki od ova dva skenera prenosi znatnu količinu različitih informacija o računarima koje skeniraju. Da bi dobili relevantnu i realnu sliku za precizniju analizu, neophodni su nam kombinovani rezultati oba ova skenera. U tabeli 4 predstavljeni su izazovi i problemi svakog skenera, kao i predloženo rešenje koje ćemo primeniti.

Tabela 4 - Mane OpenVAS i NMAP skenera i način njihovog prevazilaženja

br.	Mane		Rešenja
	NMAP	OpenVAS	
1	Procena ranjivosti		
	Sadrži dosta manje NSE su dostupne, a konačni rezultati skeniranja daju dosta lažnih pozitivnih rezultata.	Nema (NVT skripte se redovno dopunjuju)	Integracija NMAP i OpenVAS skenera preko NMAP dodatka za OpenVAS.
2	Kompleksnost intalacije/konfiguracije		
	jednostavno	Veoma kompleksno	Veb grafički interfejs. Nema nikakve instalacije niti konfiguracije na klijentskim radnim stanicama.
3	Generisanje izveštaja		
	Samo u pdf formatu	Mogu se generisati samo predviđeni izveštaji, bez mogućnosti dodatnog podešavanja i filtriranja.	Kreiranje raznih tipova izveštaja u drugim formatima.
4	Trajanje skeniranja		
	Veoma brzo	Detaljno skeniranje samo jedne radne stanice može da potraje.	Integracija NMAP i OpenVAS skenera.

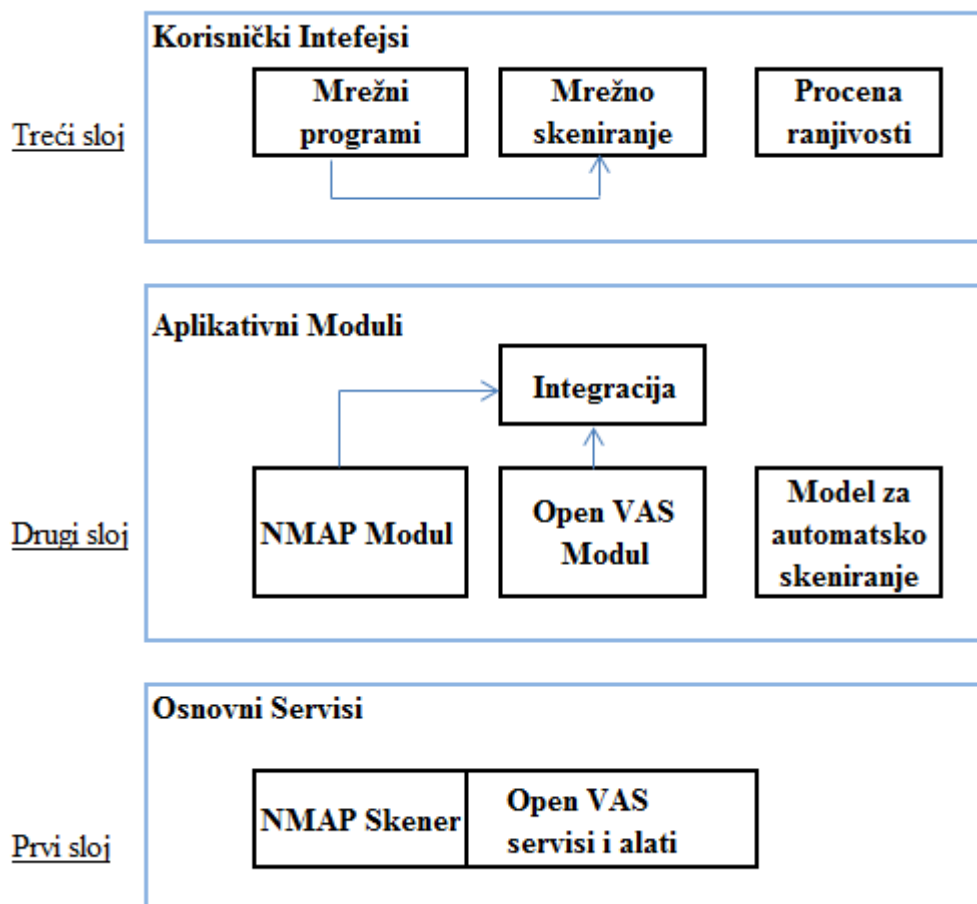
Na osnovu predloženih rešenja iz tabele 4, pristupamo njihovoj realizaciji koju objašnjavamo u sledećem poglavlju.

2.1.1 Opšta arhitektura

Da bi mogli da razmatramo rezultate oba mrežna skenera, u implementaciji integrisane platforme dva skenera imamo sledeće izazove:

1. Platforma mora biti u mogućnosti da kontroliše aktivnosti oba skenera (i NMAP i OpenVAS);
2. Platforma mora imati opciju izbora sa kojim od dva skenera želimo da skeniramo mrežu i mogućnost skeniranja mreže sa oba skenera odjednom.

Na osnovu prethodne dve stavke i predloženog rešenja, arhitektura našeg skenera je prikazana na slici 6. Slika 6 grubo prikazuje arhitekturu integrisane platforme za mrežno skeniranje.



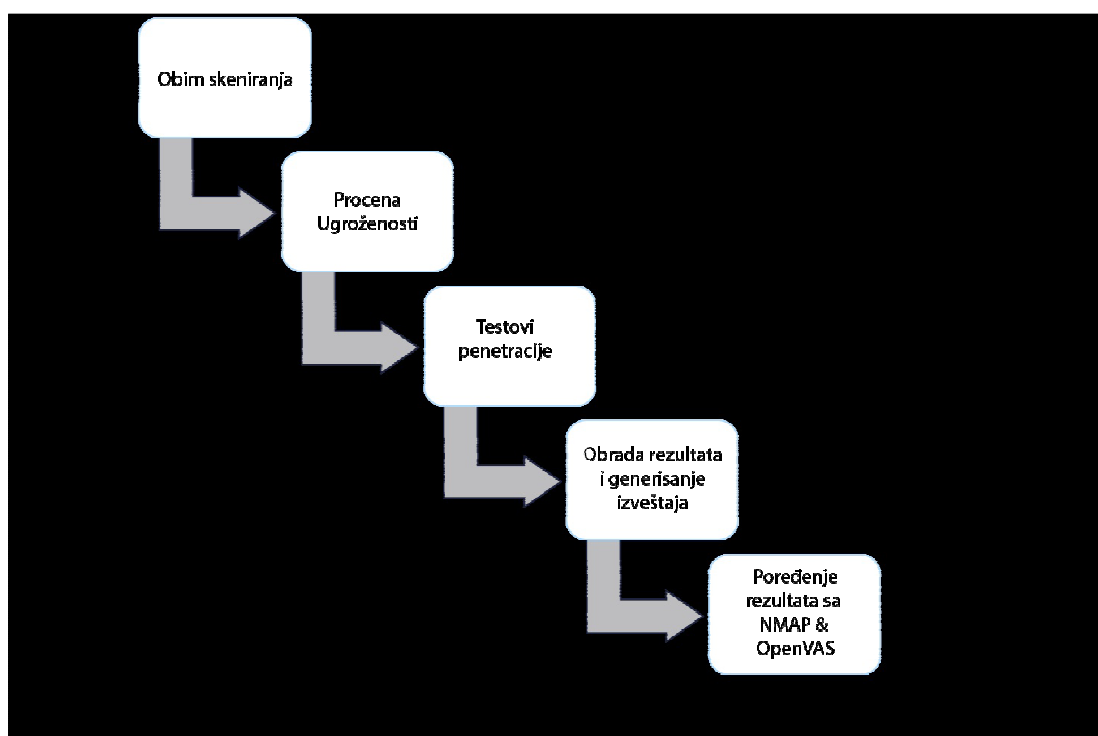
Slika 6 - Arhitektura mrežnog skenera

1. Prvi sloj se sastoji od osnovnih servisa koji rade ceo posao skeniranja;
2. Drugi sloj se sastoji od raznih modula koji prihvataju zahteve, procesuiraju ih, pozivaju osnovne servise i generišu izveštaje;
3. Treći sloj sadrži korisnički interfejs.

2.2 Način implementacije

Različiti mrežni uređaji zahtevaju i različit pristup skeniranja i testiranja. Vrsta skeniranja treba da se uskladi sa vrednošću podataka na ciljnoj radnoj stanici i potrebom da se ta radna stanica povezuje na određeni servis. Predloženi način implementacije ima 5 koraka i to:

1. Definisanje obima skeniranja;
2. Izvršavanje procene ranjivosti koristeći NMAP i OpenVAS;
3. Dobijanje rezultata i kreiranje izveštaja;
4. Testom penetracije pokušati proboj mreže na ranjivim radnim stanicama koje skener pronade;
5. Upoređivanje NMAP i OpenVAS rezultata.



Slika 7- šematski prikaz implementacije

2.2.1 Definisanje obima skeniranja

Prvi korak počinje preliminarnim proučavanjem meže. Pre samog početka tehničkog dela procene sigurnosnog stanja mreže, važno je odrediti i razumeti ciljni obim mrežnog okruženja. Takođe je važno znati da obim skeniranja može da se odnosi na jedan entitet mreže ili na više entiteta u zavisnosti od arhitekture mreže. Šta će se skenirati, kako će se skenirati, koji uslovi u mreži će biti tokom testiranja, koja ograničenja će imati izvršavanje testiranja, koliko vremena će trebati da se testiranje završi i šta će biti postignuto nakon testiranja za unapređenje informacionog sistema su sva osnovna pitanja na koja treba odgovoriti pod definisanjem skeniranja[8].

1. **Obim skeniranja:** Testiranje ciljanih uređaja ili testiranje cele mreže je zadatak na koji treba da odgovori mrežni administrator. Da li će skenirati samo određene uređaje u mreži, za koje proceni da su najizloženiji napadu (na primer zaštitni zid), ili će pokrenuti kompletno skeniranje cele mreže. Ideaalno rešenje je skenirati celu mrežu, a posebnu pažnju posvetiti analizi rezultata onim uređajima koji su direktno izloženi javnoj mreži.

Ciljano testiranje uključuje:

- Rutere i svičeve;
 - DNS server, veb server fajl server, DC kontroler i ostale aplikativne servere;
 - Zaštitni zid, i interni i eksterni;
 - Sigurnosne sisteme za detekciju upada (IDS).
2. **Lokacija testiranja:** testiranje iz lokalne mreže ili sa udaljene lokacije je sledeći korak o kojem mrežni administrator treba da razmisli i koju od ove dve opcije da izabere. Ova odluka najviše zavisi od toga koje uređaje u mreži želimo da testiramo na ranjivost, kao i na trenutne sigurnosne mere u mreži.
 3. **Biranje osobe za testiranje:** Na kraju, neko iz vrha kompanije treba da odabere da li će kompanijski IT službenici obaviti testiranje ili će to biti neka ekspertska firma sa strane. Ovo se nas ne tiče, jer nam je cilj da testiramo mrežu, dakle lokalni IT administrator će obaviti testiranje.

2.2.2 Procena ranjivosti

Proces procene ranjivosti je podeljen u dva dela. Prvi deo se odnosi na otkrivanje propusta pronalazeći ili prateći propuste koji postoje u datom sistemu. Drugi deo se odnosi na eliminisanje ili izbegavanje tih propusta iz kompletnog sistema i to je uloga mrežnog administratora.

Proces procene ranjivosti mreže se odvija sledećim koracima:

1. Otkrivanje mreže, takozvano izviđanje;
2. Prebrojavanje uređaja na mreži;
3. Određivanje aktivnih servisa na uređajima;
4. Pronalaženje i proveravanje poznatih propusta koji se pronađu na svakom uređaju;
5. Kreiranje izveštaja o svim propustima;

Pored svega navedenog u praksu procene ugroženosti spada i sledeće:

1. Ručno skeniranje;
2. Doneti na nivou kompanije strategiju i plan skeniranja mreže u redovnim intervalima, kao što su dnevni, nedeljni, mesečni ili godišnji;
3. Pokretanje hitnog skeniranja mreže u trenutku kada je mreža napadnuta i kada zlonamerni korisnici pokušavaju da probiju postojeću zaštitu.

Na osnovu arhitekture i svega navedenog, sada ćemo definisati potrebe našeg mrežnog skenera kojim ćemo testirati mrežu.

2.2.2.1 Funkcionalni zahtevi

Svaki funkcionalni zahtev je podeljen i svrstan u jedan od četiri modula i to:

1. Mrežni programi koji uključuju izviđanje i otkrivanje uređaja na mreži:
 - a. Ping;
 - b. Traceroute;
 - c. whoIS lookup;
 - d. Nslookup;
 - e. DNS prebrojavanje.
2. Skeniranje mreže koristeći NMAP:
 - a. Prikazivanje otvorenih i filtriranih portova svake radne stanice koji je skeniran u poslednjih 7 dana. Ovo skeniranje pokazuje da li je bilo nekih promena u konfiguraciji uređaja;
 - b. Skeniranje NMAP softverom koristeći različite profile skeniranja;
 - c. Skeniranje NSE skriptama da bi se sproveo test ranjivosti;
 - d. Promena profila korisnika, da bi se napravili novi profili ili menjali postojeći;
 - e. Preuzimanje i čuvanje dobijenih rezultata;
 - f. Učitavanje sačuvanih izveštaja;
 - g. Vizualizacija izlaznih fajlova u različitim formatima:
 - i. 2D grafik;
 - ii. 3D pregled;
 - iii. Tabelarni prikaz;
 - iv. PDF izveštaj.
3. Skeniranje mreže koristeći OpenVAS:
 - a. Komandni interfejs koji nam daje sledeće informacije:
 - i. Pregled:
 - Trenutni status zadataka (novi, pokrenut, pauziran, stopiran);
 - Ukupan broj mrežnih ranjivosti svakog skeniranja;
 - Ukupan broj mrežnih ranjivosti svakog pojedinačnog zadatka
 - Pregled resursa (broj zadataka, ciljnih grupa, konfiguracije);
 - Najveći mrežni propust otkriven do datog trenutka;

- Zadaci sa najvećim propustima otkrivenim do datog trenutka
- ii. Detalji OpenVAS skenera;
- iii. Konfiguracija mrežnog skenera;
- iv. Spisak mrežnih uređaja za skeniranje;
- b. Zadaci OpenVAS skenera:
 - i. Spisak svih zadataka;
 - ii. Zadaci za start, pauzu, nastavak i zaustavljanje skeniranja;
 - iii. Podešavanja za kreiranje ciljnih mrežnih uređaja;
 - iv. Podešavanja za kreiranje zadataka;
 - v. Kreiranje zadataka koji će pokrenuti NMAP skener kao ulaz, kako bi smanjio vreme skeniranja;
- c. Izveštaji:
 - i. Različiti formati izveštaja se kreiraju dodavanjem različitih detalja. Ovi detalji uključuju:
 - ii. Vreme početka, zaustavljanja i spisak uređaja za skeniranje;
 - iii. Pregled svih propusta pronađenih u zadatku;
 - iv. Spisak svih otvorenih portova svakog uređaja i kategorizacija njihove potencijalne pretnje (visokorizična, srednje, slabo);
 - v. Broj svih pretnji sortiran po kategorijama.
- 4. Auto skeniranje:
 - a. Pravljenje grupe IP adresa;
 - b. Izbor vrste skeniranja koju želimo da pokrenemo i učitavanje NMAP profila ili OpenVAS konfiguracije ili obe;
 - c. Dodeljivanje prioriteta ovoj grupi, tj. kada da počne skeniranje i/ili u kojim intervalima (dnevni, nedeljni, mesečni, godišnji);
 - d. Podešavanje opcija za ovu vrstu skeniranja;
 - e. U slučaju detektovanja napada na mrežu, izvršiti testiranje na propuste i poslati izveštaj administratoru.

2.2.2.2 Nefunkcionalni zahtevi:

1. Mrežni skener mora biti otvorenog koda, dakle jeftino rešenje sa mogućnošću modifikovanja i nadogradnje u budućnosti;
2. Ovaj skener mora imati opciju skeniranja različitih operativnih sistema pošto kompanija ima uređaje koji rade i u Windows i u Linux okruženju;
3. Rezultati moraju biti tačni i precizni, jer će dobijeni izveštaji direktno uticati na odluke sistem administratora koje su vezane za bezbednost mreže.

2.2.3 Kreiranje izveštaja

Nakon kompletne bezbednosne procene mrežnih propusta, administrator treba da analizira sve podatke dobijene tokom prethodnog skeniranja. Mogućnost generisanja raznih izveštaja u različitim formatima je jako bitno u sumiranju rezultata i predstavljanja dobijenih informacija višim instancama u kompaniji.

Mrežni skener izistava i pravi prioritete pronađenih propusta tako što ih svrstava u kategorije bazirane na CVSS²⁰ faktoru kao propuste slabog, srednjeg i jakog propusta i propisuje moguće rešenje za saniranje tih propusta. Skener takođe može dati i dodatne informacije za te ranjivosti, kao što su internet linkovi ili linkovi ka zakrpkama koje rešavaju problem ranjivosti skeniranih aplikacija. Konačan izveštaj treba da sadrži sledeće delove:

1. Grafičku prezentaciju: 2D grafik i 3D prezentaciju nakon skeniranja;
2. Izveštaji o propustima koji sadrže otkrića o svim ranjivim uređajima, čije se ranjivosti kategorišu po prioritetima rizika i odgovarajuće sugestije o rešavanju tih propusta, sa dodatnim informacijama o propustima.

2.2.4 Testiranje

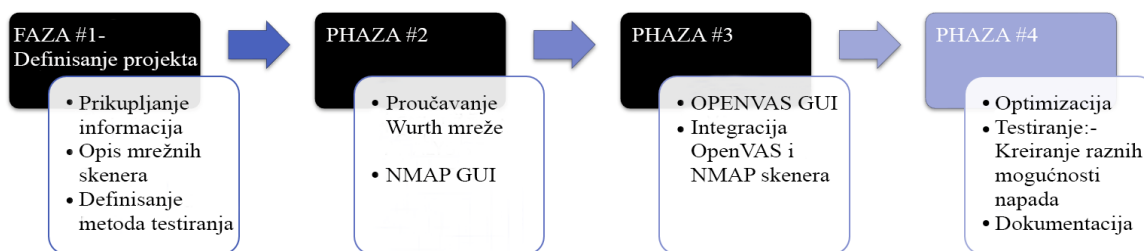
Testiranje se sprovodi u samoj mreži i ono uključuje:

1. Skeniranje portova i identifikacija pokrenutih servisa koristeći NMPA: prvi zadatak skenera je da otkrije šta se nalazi na mreži, koji servisi su pokrenuti i koje operativne sisteme pokreće svaki računar. On pokušava da otkrije koje aplikacije i servisi su pokrenuti na ovim sistemima, kao i njihovu konfiguraciju i verziju;
2. Testiranje ranjivosti koristeći OpenVAS: Izvršiti skeniranje mreže koristeći i OpenVAS i NMAP posebno, a i koristeći ih kao integrisano rešenje. Mrežni skener se oslanja na bazu podataka OpenVAS softvera koja sadrži sve podatke potrebne da bi se sistem proverio na potencijalne propuste;
3. Detektovanje promene u konfiguraciji: skener će biti podešen da na dnevnom nivou skenira kritične uređaje. Biće podešen tako da šalje mail upozorenja ukoliko primeti bilo kakvu promenu u konfiguraciji uređaja. Ovo se radi zato što ovakve promene mogu da izvrše lica koja nisu ovlašćena da prave promene u konfiguraciji kritičnih mrežnih uređaja.

2.3 Plan projekta

Na osnovu zahteva ovog alata i koraka za implementaciju koji su nabrojani, ovaj projekat je podeljen u faze prikazane na slici 8. prva faza uključuje osnovnu studiju projekta. Druga faza uključuje proučavanje interne mreže, skeniranje mreže i implementaciju NMAP modula. U trećoj fazi se definiše mehanizam za integraciju ova dva

²⁰ Common Vulnerability Scoring System



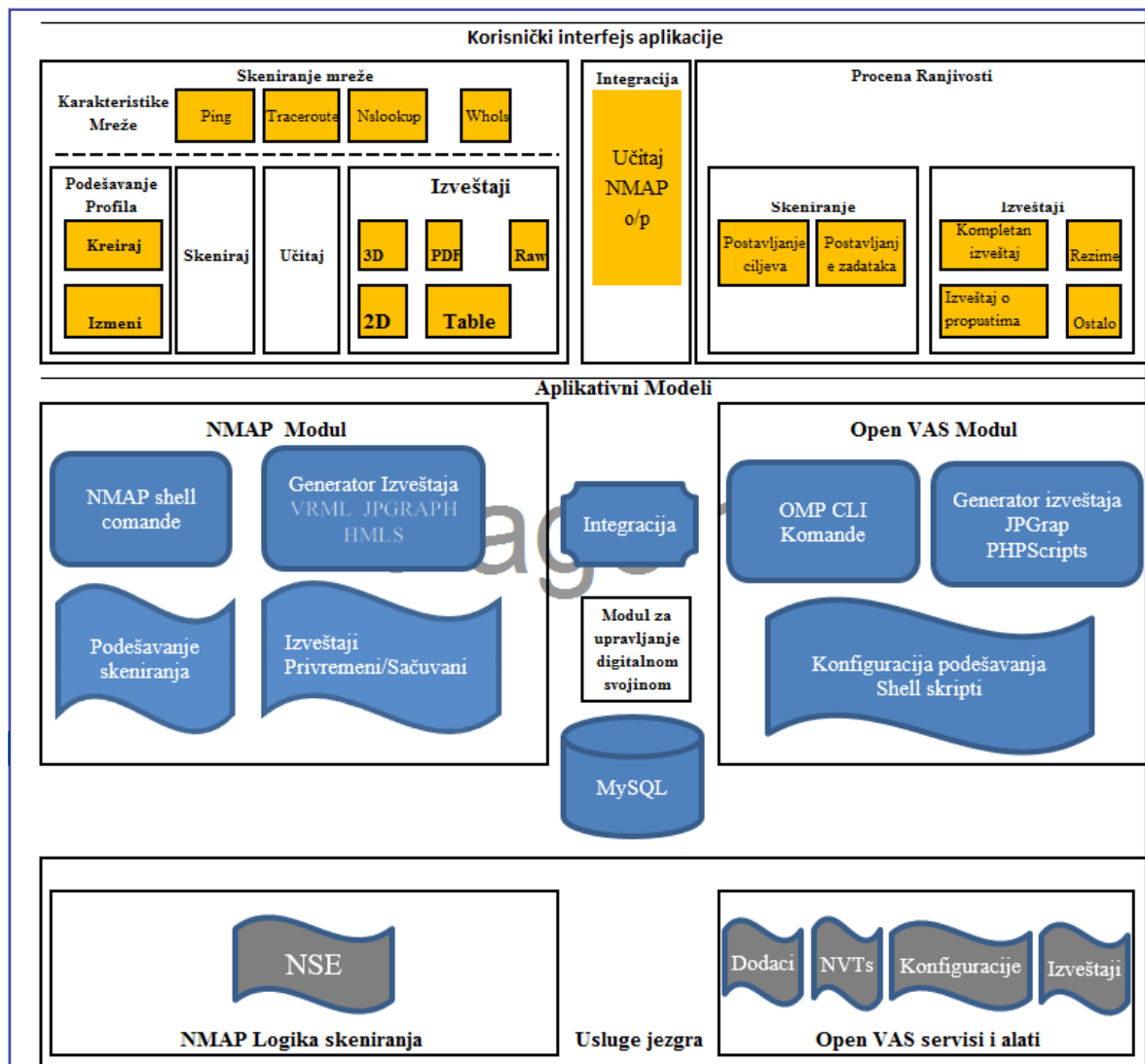
Slika 8 - Plan projekta

skenera. Četvrta faza sastoji se od razvoja modula za automatsko skeniranje. U ovoj fazi se još i sprovode razni testovi napada na mrežu, zasnovani na već pronađenim propustima. Ali ovi testovi nisu u oblasti ovog rada. Ova ispitivanja se vrše samo za razumevanje mrežnih skenera.

3 Dizajn i razvoj

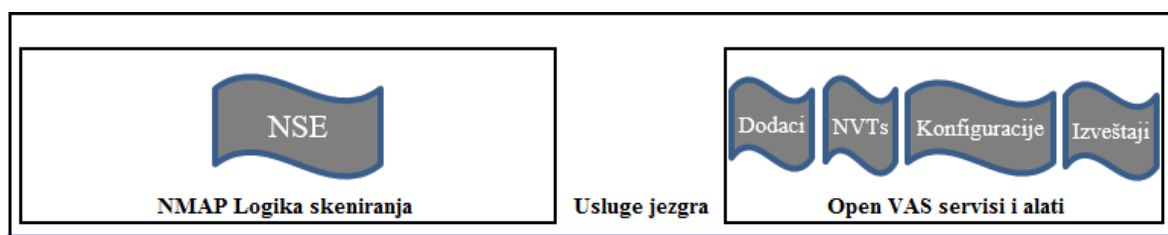
Mrežni skener koji ćemo koristiti je veb aplikacija i za NMAP i za OpenVAS. Iskoristićemo najbolje opcije od oba skenera. Takođe, ovom integracijom nadoknađeni su brojni nedostaci koje svaki od ova dva alata ima pojedinačno.

U ovom poglavlju, detaljno je objašnjena arhitektura mrežnog skenera koja je prikazana na slici 9. Objašnjeni su glavni servisi (i NMAP i OpenVAS skenera) i kako i zašto su iskorišćeni.



Slika 9 - detaljna arhitektura mrežnog skenera

3.1 Prvi sloj: Osnovni servisi



Slika 10 - osnovni servisi

Osnovni servisi skenera obuhvataju integrisane osnovne servise NMAP i OpenVAS skenera.

3.1.1 NMAP logika skeniranja

Osnovne karakteristike NMAP skenera su već pomenute u prethodnim poglavljima, a sada ćemo detaljno objasniti svaku njegovu opciju i način rada.

Upotreba NMAP-a:

1. Servis sa kojim NMAP počinje rad je NMAP Ping. Pre no što NMAP skenira bilo koji uređaj, on proverava da li je taj uređaj stvarno dostupan na mreži. NMAP ima dosta različitih Ping opcija koje može da koristi i to su:

ARP Ping (-PR) – ARP ping šalje ARP²¹ paket uređajima na lokalnoj podrmeži. Pošto ovo nije IP okvir, ova vrsta pinga ne može biti korišćena da bi identifikovala uređaje kroz različite podmreže.

ICMP Echo Request Ping (-PE) – ovaj ping je „pravi“ ping, zato što ICMP echo request šalje paket ciljnom uređaju i čeka za ICMP echo reply. Problem kod ove vrste pinga je taj što većina pametnih zaštitnih zidova blokiraju ICMP saobraćaj, te stoga ova opcija nije naročito korisna kada se upotrebljava u zaštićenim mrežama.

TCP ACK Ping (-PA) – Kada podrazumevani NMAP ping radi, to je zato što TCP ACK ping dobija odgovor. ACK ping šalje proizvoljni TCP ACK paket na port 80 drugom uređaju, a drugi uređaj na neispravan ACK paket odgovara tako što traži dodatni odgovor.

TCP SYN Ping (-PS) – Ovaj tip pinga funkcioniše na isti način kao i NMAP TCP SYN skeniranje, sa razliko što koristi samo jedan port. Podrazumevano koristi HTTP port 80, ali može koristiti bilo koji port koji se podesi da bi se olakšalo pingovanje uređaja koji su dobro zaštićeni i od kojih je teško dobiti odgovor regularnim putem.

UDP Ping (-PU) – Sa ovim tipom pingovanja želimo da pogodimo port koji je zatvoren iz razloga što zatvoreni UDP portovi uglavnom daju odgovore da je traženi ICMP port nedostižan i nedostupan. Ova poruka signalizira NMAPu da je mašina aktivna i dostupna. Ostale greške koja UDP ping vrati uglavnom signaliziraju da je mašina nedostupna. Ukoliko je port otvoren većina servisa će samo ignorisati poruku i neće vratiti nikakav odgovor.

²¹ Address Resolution Protocol

ICMP Timestamp ping (PP) – Timestamp ping koristi ICMP funkciju „get timestamp“. Ova funkcija je korisna, ali sa ograničenjem da se i ona oslanja na ICMP da će dobiti odgovor od uređaja kojem šalje ICMP paket. I ovaj ping treba izbegavati u mrežama koje su zaštićene.

ICMP Address Mask ping (-PM) – Ovo je jedna neobična ping funkcija, ali većina mrežnih uređaja i radnih stanica neće odati informaciju kao što je maska mreže. I, naravno, i ova verzija pinga ima ista ograničenja kao i sve ostale ping opcije zasnovane na ICMP paketima.

Neke od ovih ping opcija mogu odgovarati u jednom, neke u drugom slučaju, u zavisnosti šta korisnik želi da postigne i da dobije od uređaja koji pinguje. Na primer, ako je NMAP skener fokusiran na pronalaženje UDP portova, onda će UDP ping opcija biti najprikladnija da se primeni na ciljnom mrežnom uređaju.

Ostale NMAP ping funkcije se uglavnom ređe koriste, ali itekako mogu biti korisne. Čak i ICMP address mask ping može biti koristan da bi na neobičan način saznali masku mreže i podmreže u nekim starijim sistemima koji nisu ažurirani i koji mogu da odgovore na ovu vrstu pinga.

2. **Tehnike NMAP skeniranja** – nakon ping procedure i otkrivanja svih klijenata na mreži, NMAP može započeti proces skeniranja. Kada se NMAP pokrene da radi kao privilegovani korisnik, podrazumevani način skeniranja je TCP SYN skeniranje, a kada NMAP radi kao neprivilegovani korisnik, podrazumevani način skeniranja je TCP connect() skeniranje. Ostale tehnike skeniranja prikazane su na slici 10[14].

Tabela 5- NMAP tehnike skeniranja

NMAP Scan	Sintaksa	Zahteva prava pristupa	Identifikuje TCP Portove	Identifikuje UDP Portove
TCP SYN Scan	-sS	DA	DA	NE
TCP connect()Scan	-ST	NE	DA	NE
FIN Scan	-sF	DA	DA	NE
Xmas Tree Scan	-sX	DA	DA	NE
Null Scan	-sN	DA	DA	NE
Ping Scan	-sP	NE	NE	NE
Version Detection	-sV	NE	NE	NE
UDP Scan	-sU	DA	NE	DA
IP Protocol Scan	-sO	DA	NE	NE
ACK Scan	-sA	DA	DA	NE
Window Scan	-sW	DA	DA	NE
RPC Scan	-sR	NE	NE	NE
List Scan	-sL	NE	NE	NE
Idlescan	-sI	DA	DA	NE
FTP Bounce Attack	-b	NE	DA	NE

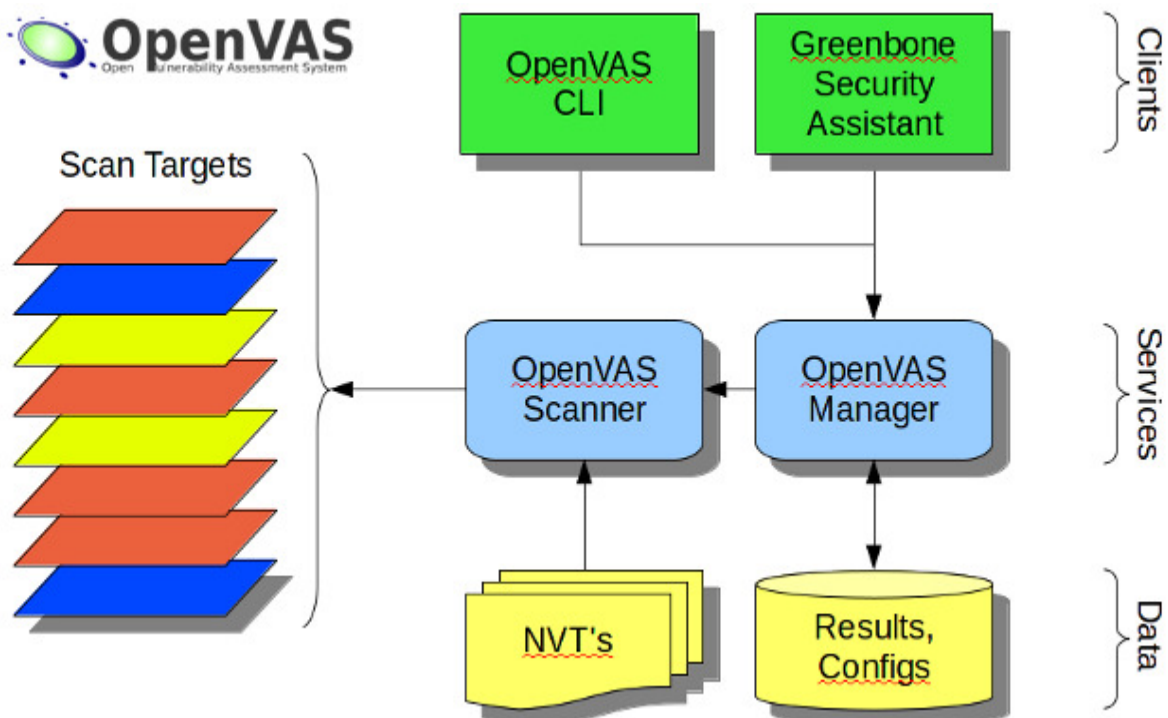
3. **NMAP skeniranje mrežnih propusta** - skeniranje se može obaviti koristeći NMAP skripte koje su osnova NMAP programa za skeniranje i koje automatizuju mrežne zadatke. To je modularni sistem za proširivanje NMAP-a koji koristi Lua interpreter da bi pokretao sve ove skripte. Ove skripte se pokreću povremeno, one mogu pristupiti osnovnim podacima skeniranja i u mogućnosti su da pretražuju mrežu.

Drugi pristup skeniranju koristeći vulscan – modul koji se zove „Vulscan“ omogućava NMAP-u funkcionalnost kompletnog mrežnog skenera. Da bi se utvrdili potencijalni nedostaci po identifikovanom produktu, koristi se opcija „-sV“ u NMAP-, a ova opcija nam omogućava detekciju verzije kao poseban servis. Izlazni rezultat se nakon toga pretražuje u bazi podataka mrežnih propusta.

- Instalacija Vulscan modula:** Preuzima se binarna datoteka i instalira u folder gde je i NMAP instaliran;
- Korišćenje:** da bi se pokrenuo osnovni mrežni skener, korisnik treba da unese sledeću komandu: `nmap -sV {script = vulscan www.example.com [{script-args "vulscandb = db-name"]}`
- Baze podataka koje se koriste:** cve, exploitdb, openvas, scipvuldb, securityfocus, securitytracker, xforce;
- Mane:** veliki broj lažnih pozitivnih rezultata

3.1.2 OpenVAS

Arhitektura OpenVAS skenera je već detaljno opisana u ranijim poglavljima, sada ćemo objasniti samo još neke funkcionalnosti koje smo propustili.



Slika 11 - OpenVAS arhitektura

Protokoli koji su implementirani u OpenVAS skener:

1. OTP: OpenVAS transfer protocol;
2. OMP: OpenVAS management protocol;
3. OAP: OpenVAS Administrative protocol.

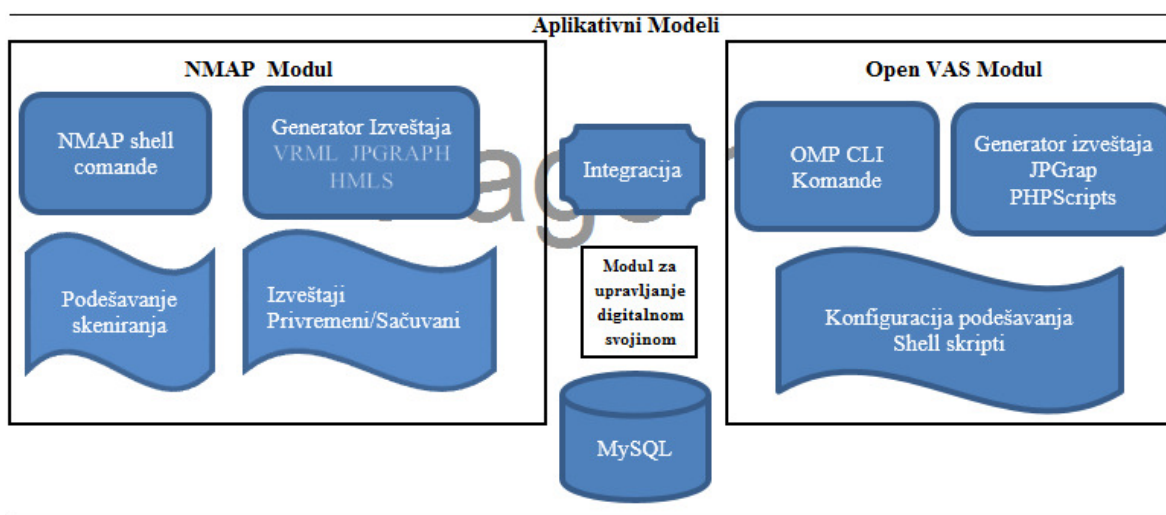
3.1.2.1 OpenVAS funkcije

OpenVAS skener: OpenVAS skener može skenirati mnogo uređaja istovremeno. Skener koristi OpenVAS transfer protocol koji ima i SSL podšku.

OpenVAS manager: OpenVAS manager zavisi od OpenVAS management protocol-a (OMP). Da bi mogao da izvrši svoje zadatke kao što su zakazivanje zadataka u određeno vreme, paralelno upravljanje zadacima koji se izvršavaju istovremeno, zaistavljanje, pauziranje i nastavljavanje procesa skeniranja, upravljanje lažnim pozitivnim rezultatima i upravljanje zapisima skeniranih rezultata its. OpenVAS manager koristi SQL bazu podataka (SQLite) za čuvanje svoje konfiguracije i rezultata skeniranja. Izveštaji koje kreira OpenVAS mogu biti u raznim formatima (za neke su potrebni i posebni dodaci): XML, HTML, LateX, itd.

OpenVAS CLI: je klijent koji se izvršava iz komandne linije za OMP. Može da radi i na Linux i na Windows operativnim sistemima.

3.2 Drugi sloj: aplikativni modul



Slika 12 - aplikativni modul

3.2.1 NMAP modul

Nmap modul je razvijen tako da bi mogao da ispuni sve funkcionalne zahteve. On izvršava sledeće funkcije:

Otkrivanje hostova na mreži: skener proverava dostupnost ciljanih hostova na mreži (radnih stanica i mrežnih uređaja). Za svaki zadati uređaj skener proverava da li je on povezan na mrežu i da li on odbija sve dolazeće konekcije. Za otkrivanje hostova koristimo ping servis koji koristi ICMP, TCP i UDP pakete. TCP i UDP paketi se šalju na

podrazumevane portove najčešćih servisa i uglavnom je to HTTP port na broju 80, ali se koriste i portovi protokola kao što su DNS, TELNET, SMTP i SNMP. Ukoliko na makar jedan od ovih paketa NMAP dobije pozitivan odgovor, to je znak da je ciljani uređaj na mreži i da se odaziva. Različite vrste pretraživanja mreže i lista portova koji treba da budu provereni tokom otkrivanja hostova na mreži se mogu podešavati u opcijama NMAP programa. Ukoliko host nije aktivan, proces skeniranja neće ni otpočeti. Korisnik može odlučiti da skener pokuša da skenira sve uređaje koji nisu dostupni, ali ovo nije preporučljivo čak ni u mrežama iz C klase, jer drastično povećava vreme skeniranja.

Nakon otkrivanja svih aktivnih uređaja na mreži, sledeći koraci koje NMAP preduzima su jako brzi, a ti koraci su: skeniranje portova, otkrivanje operativnog sistema, otkrivanje aktivnih servisa i otkrivanje mrežnih propusta ukoliko je i ta opcija odabrana i ukoliko je „vulscan“ modul instaliran.

Skeniranje portova: Skener otkriva sve TCP/UDP portove na skeniranim mrežnim uređajima. Korisnik ima opciju da izabere koje portove će skenirati da li samo TCP ili samo UDP ili neke specifične portove.

Otkrivanje operativnog sistema: Nakon skeniranja portova, sledeći korak je otkrivanje operativnih sistema instaliranih na radnim stanicama. Ovo NMAP radi koristeći opciju „stack fingerprint“ koja rešava problem otkrivanja operativnog sistema na jedinstven način.

Otkrivanje aktivnih servisa i aplikacije: U trenutku kada NMAP pronade otvorene TCP ili UDP portove, skener koristi nekoliko različitih metoda za otkrivanje koji servisi su sve pokrenuti na tim portovima, jer pojedini servisi i aplikacije koriste iste portove, a neki servisi čak koriste i potpuno proizvoljne portove koje korisnik odabere te je stoga bitno sa što manje grešaka utvrditi koji tačno servisi i aplikacije rade na određenim otvorenim portovima.

Generisanje izveštaja:

1. Neobrađeni izveštaj završenog skeniranja;
2. 2D i 3D grafički izveštaji završenog skeniranja;
3. PDF izveštaji i tabelarni prikaz.

3.2.2 OpenVAS modul

Ovaj modul je zavistan od OMP CLI, kako bi mogao da izvršava svoje funkcije

3.2.2.1 OMP CLI

OpenVAS komandni interfejs (openvas-cli) je jedan od dva načina skeniranja mreže. Komandnu liniju za skeniranje uglavnom biramo kada želimo da skeniramo veći broj računara i kada želimo da automatizujemo procese. Da bi mogli da koristimo OMP CLI potrebno je dodatno instalirati ovaj paket.

OMP za većinu komandi ima dosta prečica, ali da bi se istražile kompletne mogućnosti OpenVAS management protokola zasnovanog na XML-u najbolje je koristiti njegove –xml komande sa XML zahtevima[20].

Na primer ukoliko korisnik sa korisničkim imenom „korisnik“ i lozinkom „lozinka“ želi da stupi interakciju sa OpenVAS manager-om koji je aktivan na portu 9390 na lokalnoj mašini (127.0.0.1), koristiće sledeću komandu:

```
omp -u korisnik -w lozinka -h 127.0.0.1 -p 9390 --xml='<help/>'
```

Primer skeniranja radne stanice korišćenjem OMP:

Prvo što treba da uradimo je da izaberemo koji test ćemo da pokrenemo – Da bi skenirali određenu radnu stanicu, treba da izaberemo sve opcije skeniranja, koje će reći OpenVAS softveru koje dodatke i opcije da koristi. OpenVAS sadrži 4 različito podešene konfiguracije koje možemo videti koristeći komandu „**omp -g**“, a kao izlaz dobićemo rezultat kao na slici 13.

```
afnarel@debian:~$ omp -u admin -w tagada -g
daba56c8-73ec-11df-a475-002264764cea Full and fast
698f691e-7489-11df-9d8c-002264764cea Full and fast ultimate
708f25c4-7489-11df-8094-002264764cea Full and very deep
74db13d6-7489-11df-91b9-002264764cea Full and very deep ultimate
085569ce-73ed-11df-83c3-002264764cea empty
```

Slika 13 - izlaz komande `omp -g`

Ukoliko koristimo XML komandu, dobićemo znatno više informacija čiji izlaz je prikazan na slici 14 – „`omp --xml='<get_configs/>'`“

```
afnarel@debian:~$ omp -u admin -w tagada -iX '<get_configs/>'
<get_configs_response status="200" status_text="OK">
  <config id="daba56c8-73ec-11df-a475-002264764cea">
    <name>Full and fast</name>
    <comment>Most NVT's; optimized by using previously collected information.</comment>
    <family_count>49
      <growing>1</growing>
    </family_count>
    <nvt_count>30533
      <growing>1</growing>
    </nvt_count>
    <in_use>1</in_use>
    <writable>0</writable>
    <tasks></tasks>
  </config>
  <config id="698f691e-7489-11df-9d8c-002264764cea">
    <name>Full and fast ultimate</name>
    <comment>Most NVT's including those that can stop services/hosts; optimized by using previously collected information.</comment>
    <family_count>49
      <growing>1</growing>
    </family_count>
    <nvt_count>30533
      <growing>1</growing>
    </nvt_count>
    <in_use>1</in_use>
    <writable>0</writable>
    <tasks></tasks>
  </config>
  <config id="708f25c4-7489-11df-8094-002264764cea">
    <name>Full and very deep</name>
    <comment>Most NVT's; don't trust previously collected information; slow.</comment>
    <family_count>49
      <growing>1</growing>
    </family_count>
    <nvt_count>30533
      <growing>1</growing>
    </nvt_count>
```

Slika 14 - Korišćenje XML komande `omp --xml='<get_configs/>'`

Mi ćemo skeniranje obaviti testom „Full and very deep ultimate“, za koji je bitno zapamtiti njegov tačan ID koji glasi: 74db13d6-7489-11df-91b9-002264764cea.

Nakon izbora testa, sada treba da izaberemo radnu stanicu koju želimo da skeniramo. Po podrazumevanim podešavanjima, samo je računar na kojem radimo dostupan, a dodavanje novih radnih stanica je prilično jednostavno, samo treba dodati ime računara i IP adresu koju želimo da skeniramo:

```
omp -xml='  
<create_target>  
<name>Target Name</name>  
<hosts>10.94.1.147</hosts>  
</create_target>
```

Ukoliko želimo da uradimo još detaljniji test, potrebno je skeneru da damo i SSH pristup kako bi mogao da se uloguje na računar i sprovede dodatne testove sa samog računara.

Skeniranje započinjemo komandom (slika 15):

```
„omp -xml='<start_task task_id="267a3405-e84a-47da-97b2-5fa0d2e8995e"/>'“
```

```
root@debian:/home/atnarel/Documents/OpenVAS/scripts# omp -u admin -w tagada --xml=  
'<start_task task_id="80493ba8-503a-4d20-98d1-bf42d6b98b10"/>'  
<start_task_response status="202" status_text="OK, request submitted"><report_id>9  
a726da2-7d39-4870-aae2-f785b5c106ea</report_id></start_task_response>
```

Slika 15 - početak skeniranja

Ovaj zadatak možen biti pauziran i zaustavljen pre no što se završi, ukoliko za tim ima potrebe koristeći komande:

```
„omp -xml='<stop_task task_id="267a3405-e84a-47da-97b2-5fa0d2e8995e"/>'“  
„omp -xml='<pause_task task_id="267a3405-e84a-47da-97b2-5fa0d2e8995e"/>'“
```

Trenutni status različitih zadataka možemo dobiti komandom „omp -G“

Dobijanje izveštaja:

Na kraju svakog skeniranja, kreiraju se izveštaji koji se mogu dobiti u nekom od željenih formata. Da bi dobili određeni izveštaj potrebno je da saznamo njegov ID broj koristeći komandu: „omp -iX ‘<get_tasks details="1"/>’ „. Ova komanda će nam izlistati sve izveštaje skeniranja koji postoje u bazi. Kada pronađemo rezultate skeniranja za koje želimo izveštaj, pokrećemo komandu:

```
„omp -iX ‘<get_tasks task_id="77ba3c2e-ff61-44b7-86ed-f10d213008ee" details="1"/>'“
```

Druga stvar koja nam je potrebna je i ID formata u kojem želimo da vidimo naš izveštaj. Dostupni formati su tekstualni, XML, PDF i NBE format. Da bi saznali ID brojeve ovih formata koristimo komandu: „omp -iX ‘<get_report_formats/>’“

Na kraju, rešili smo da vidimo naš izveštaj u PDF formatu i pokrećemo komande:

„omp -iX ‘<get_reports report_id=’68d3bf25-591e-4be6-97af-1e66fd8924ab’
 „format_id=’c402cc3e-b531-11e1-9163-406186ea4fc5’/’>’“

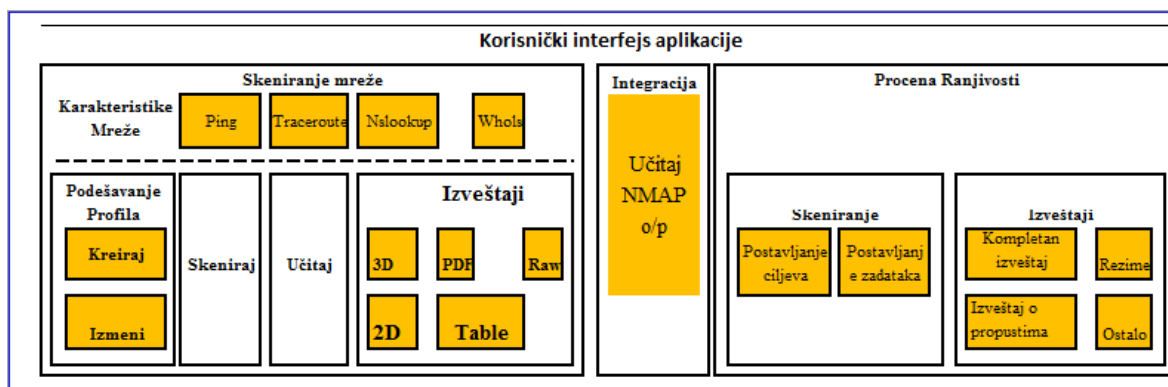
Razumevanje povratnih kodova nakon pokrenute komande:

Povratni kodovi koje nam daje OMP nakon izvršene komande su veoma slični kodovima koje šalje HTTP protokol. Kodovi su prikazani u tabeli 6.

Tabela 6- OMP povratni kodovi

Statusni kod	Statusna poruka
2xx	Komanda uspešna (primljena, razumljiva i prihvaćena)
200	U redu
201	U redu, resurs napravljen
202	U redu, zahtev predat
4xx	Komanda ne može biti izvršena zbog neke greške
400	Sintaksna greška
401	Potrebna autentifikacija
403	Pristup resursima nije dozvoljen
404	Resurs ne postoji
409	Resurs zauzet
5xx	
500	Interna greška
503	Servis nije dostupan/ Servis privremeno oboren

3.3 Treći sloj: aplikativni interfejs (slika 16)



Slika 16 - Aplikativni interfejs

Da bi uspjeli da implementiramo i sprovedmo sve zadatke koje smo pomenuli u ovom poglavlju, sledeće osobine i funkcije aplikativni interfejs mora da ponudi korisniku:

1. Mrežni programi:
 - a. Ping;
 - b. Traceroute;

- c. WhoIs Lookup;
- d. Browser Profiling;
- 2. NMAP grafičko okruženje:
 - a. Skeniranje mreže;
 - b. Različiti formati i oblici izveštaja (2D, 3D, PDF, itd.);
 - c. Kreiranje / konfigurisanje profila za skeniranje;
 - d. NSE skeniranje na mrežne propuste.
- 3. OpenVAS grafičko okruženje:
 - a. Kreiranje zadataka;
 - b. Dodavanje mrežnih uređaja;
 - c. Kreiranje i dodavanje profila za skeniranje
 - d. Različiti formati i oblici izveštaja (rezime skeniranja, kompletan izveštaj, itd.)
- 4. Integrirani mrežni interfejs:
 - a. Kreiranje grupe IP adresa za skeniranje;
 - b. Dodeljivanje profila za skeniranje izabranoj grupi;
 - c. Dodeljivanje vremenskog intervala za skeniranje (dnevni, nedeljni, mesečni, godišnji, neko specifično vreme)
 - d. Dodavanje zadatka u cronTab da bi se pokrenuo u zadato vreme.

3.4 Predložena rešenja za probleme

Do sada su objašnjene razne osobine, karakteristike, specifičnosti i način rada mrežnog skenera. Integracijom dva skenera većina problema se može prevazići koji su navedeni u tabeli 4. U tabeli 6 je sada detaljnije prikazano koja su sve rešenja predložena na svaki problem na koji smo naišli.

Tabela 7 - prevazilaženje mana OpenVAS i NMAP skenera integracijom u jedan skener

Tabela 7 – prevađanje mana OpenVAS i NMAP skenera integracijom u jedan skener			
br.	Mane		Rešenja
	NMAP	OpenVAS	
1	Procena ranjivosti		
	Dosta manje NSE skripti su dostupne, a konačni rezultati skeniranja daju dosta lažnih pozitivnih rezultata.	Nema (NVT skripte se redovno dopunjuju)	Integracija NMAP i OpenVAS skenera preko NMAP dodatka za OpenVAS. Administratoru je ostavljena opcija da može da pristupi servisima oba skenera.
2	Kompleksnost instalacije/konfiguracije		

	jednostavno	Veoma kompleksno	Veb grafički interfejs. Nema nikakve instalacije niti konfiguracije na klijentskim radnim stanicama.
3	Generisanje izveštaja		
	Samo u pdf formatu	Mogu se generisati samo predviđeni izveštaji, bez mogućnosti dodatnog podešavanja i filtriranja.	NMAP modul mrežnog skenera omogućava nam razne izveštaje koji mogu biti neobrađeni podaci skeniranja, 3D i 2D grafički izveštaji, tabelarni prikaz i PDF izveštaji. Takođe, dostupne su i opcije čuvanja i ponovnog otvaranja izveštaja. OpenVAS modul mrežnog skenera omogućava razne izveštaje kao rezime skeniranja, kompletan izveštaj, detalji radnih stanica, ukupan broj propusta...
4	Trajanje skeniranja		
	Veoma brzo	Detaljno skeniranje samo jedne radne stanice može da potraje.	Korišćenje NMAP NASL Wrapper modula za OpenVAS

4 Rezultati testiranja i analiza

Svrha ovog testiranja je da prilagodimo i konfigurišemo aplikacije za skeniranje mreže, zatim skeniramo testni informacijski sistem i detektujemo potencijalne mrežne propuste u tom informacijskom sistemu. Istovremeno, dok mrežni skener skenira ciljne uređaje u mreži i njihove propuste, sistem za detekciju upada - IDS²² će pratiti sav dolazni i odlazni mrežni saobraćaj. IDS program koji će pratiti i detektovati skeniranje mreže zove se SNORT²³ sa posebno podešenim pravilima za detekciju. Sistem za detekciju upada osluškuje mrežu i reaguje na svaku sumnjivu aktivnost koja mu je nepoznata, sumnjiva ili ima neku lošu nameru.

SNORT je sistem za detekciju upada otvorenog koda koji u realnom vremenu analizira mrežni saobraćaj, prepoznaje mrežne napade i reaguje na njih.

Ovi testovi stanja mreže uključuju sledeće:

1. Proces procene ranjivosti mreže;
2. Korisnost ovih alata: da li alati pružaju sve potrebne funkcionalnosti ili ne?
3. Provera konfiguracije mrežnih uređaja: NMAP skripte za skeniranje i OpenVAS mrežni skener daju obaveštenje ukoliko postoji neki problem u konfiguraciji mrežnih uređaja;
4. Skeniranje mrežnih propusta: na kraju, dat je prikaz skeniranja oba alata koja smo koristili;
5. Poređenje OpenVAS skenera i NMAP mrežnog skenera.

4.1 Prvi test: proces procene ranjivosti informacionog sistema

Svrha ovog testa: Ovde razmatramo svaki korak u proceni mrežne ranjivosti i objašnjavamo kako se on može uraditi pomoću NMAP mrežnog skenera.

4.1.1 Izviđanje mreže

Izviđanjem mreže mi otkrivamo sve uređaje koji se nalaze na mreži, njihove IP adrese, otvorene portove, operativni sistem instaliran na radnim stanicama, itd. Alati koji su korišćeni su u okviru NMAP programa i već su instalirani na Kali Linux distribuciji koja je na našoj mreži instalirana kao virtualna mašina na jednoj radnoj stanici. Mreža koja se testira naziva se „Wurth.yu“, a privatna adresa mreže je 10.94.1.0/24. na mreži se nalazi 10 servera različitih namena, radne stanice i mrežni štampači. Na svim radnim stanicama su Windows 7 operativni sistemi, na serverima su mešovito Windows i Linux operativni sistemi. Informacije i rezultati koje smo prikupili izviđanjem mreže dobijeni su sledećim alatima:

1. **Traceroute** – Komandom traceroute na javnu IP adresu mreže dobićemo informacije koje su vidljive spoljnom svetu (rezultat prikazan na slici 17):

²² Intrusion Detection System

²³ <https://www.snort.org>

```

C:\Users\Velisa>tracert 195.252.110.18

Tracing route to 195.252.110.18 over a maximum of 30 hops

  1  <1 ms    <1 ms    <1 ms    192.168.1.1
  2  23 ms    33 ms    13 ms    212.200.179.72
  3  20 ms    13 ms    22 ms    212.200.179.73
  4  14 ms    14 ms    13 ms    212.200.6.161
  5  17 ms    14 ms    15 ms    79.101.105.102
  6  17 ms    17 ms    17 ms    satelitko.beotel.net [194.106.168.250]
  7  18 ms    18 ms    17 ms    195.252.68.66
  8  24 ms    22 ms    25 ms    194.106.175.218
  9  *         *         *         Request timed out.
 10  *         *         *         Request timed out.
 11  *         *         *         Request timed out.
 12  *         *         *         Request timed out.
 13  *         *         *         Request timed out.
 14  *         *         *         Request timed out.
 15  *         *         *         Request timed out.
 16  *         *         *         Request timed out.
 17  *         *         *         Request timed out.
 18  *         *         *         Request timed out.
 19  *         *         *         Request timed out.
 20  *         *         *         Request timed out.
 21  *         *         *         Request timed out.
 22  *         *         *         Request timed out.
 23  *         *         *         Request timed out.
 24  *         *         *         Request timed out.
 25  *         *         *         Request timed out.
 26  *         *         *         Request timed out.
 27  *         *         *         Request timed out.
 28  *         *         *         Request timed out.
 29  *         *         *         Request timed out.
 30  *         *         *         Request timed out.

Trace complete.

```

Slika 17 - traceroute komanda

2. **Ping** – najjednostavnijim „pingovanjem“ domena „**wurth.yu**“, već smo saznali ime jednog DNS servera, a rezultati su sledeći:

PING wurth.yu (10.94.1.11) 56(84) bytes of data.

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=1 ttl=128 time=2.64 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=2 ttl=128 time=1.70 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=3 ttl=128 time=1.67 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=4 ttl=128 time=1.58 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=5 ttl=128 time=1.62 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=6 ttl=128 time=1.64 ms

64 bytes from dc2.wurth.yu (10.94.1.11): icmp_seq=7 ttl=128 time=1.61 ms

^C

--- wurth.yu ping statistics ---

7 packets transmitted, 7 received, 0% packet loss, time 6012ms

rtt min/avg/max/mdev = 1.589/1.785/2.649/0.355 ms

3. **DNS enumeracija:** Razni alati [8] se koriste da bi se pridobile informacije o DNS²⁴ serverima i sada ćemo ih isprobati i prikazati njihove rezultate. U ovom slučaju razmatramo domen "Wurth.yu".

a. **Dnsenum:** je alat koji se koristi da bi se pronašlo što više informacija o kompletnom spisku IP adresa, imena računara koja su vezana za njih, kao i da se saznaju DNS i mail serveri. Ovaj softver može da izvrši i DNS Zone Transfer napad. Takođe, poseduje i druge mehanizme da bi saznao što više podataka o mreži, uključujući i Google pretragu, brute force napad, napad rečnikom itd. Komanda koju koristimo za istraživanje mreže je osnovna komanda: „**dnsenum wurth.yu**“, kojom dobijamo spisak DNS servera u mreži i njihove IP adrese. Zone transfer napad nije moguć iako imamo više DNS servera, jer je „Zone transfer“ na njima isključen. Rezultat koji dobijamo **dnsenum** alatom je:

----- wurth.yu -----

Host's addresses:

wurth.yu.	5	IN	A	10.94.1.10
wurth.yu.	5	IN	A	10.94.1.3
wurth.yu.	5	IN	A	10.94.1.11

Name Servers:

dc1.wurth.yu.	5	IN	A	10.94.1.3
dc2.wurth.yu.	5	IN	A	10.94.1.11

Mail (MX) Servers:

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for wurth.yu on dc2.wurth.yu ...

AXFR record query failed: RCODE from server: REFUSED

Trying Zone Transfer for wurth.yu on dc1.wurth.yu ...

AXFR record query failed: RCODE from server: REFUSED

brute force file not specified, bay.

b. **Dnsmap:** Ovaj alat koristi sličan pristup kao i **dnsenum** i **dnswalk** da bi pronašao hostove i njihove detalje. Dnsmap dolazi sa već definisanim rečnikom kojim može da izvrši napad i pronađe nazive uređaja priključenih na mrežu. Koristeći osnovni ugrađeni rečnik²⁵ i najosnovniju komandu **dnsmap wurth.yu** za nešto manje od jednog minuta dobijamo određeni

²⁴ Domain Name System

²⁵ Ovde treba uzeti u obzir da je ugrađeni rečnik prilagođen Engleskom govornom području, a okruženje u kojem se testira ovaj alat je u Srbiji i većina računara ima nazive po vlastitim imenima njihovih vlasnika.

spisak hostova, uglavnom servera, koji su se u OpenVAS testiranju pokazali prilično ranjivim.

dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

*[+] searching (sub)domains for wurth.yu using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests*

access.wurth.yu

IP address #1: 10.94.1.39

[+] warning: internal IP address disclosed

exchange.wurth.yu

IP address #1: 10.94.1.8

[+] warning: internal IP address disclosed

hr.wurth.yu

IP address #1: 10.94.1.91

[+] warning: internal IP address disclosed

moodle.wurth.yu

IP address #1: 10.94.1.105

[+] warning: internal IP address disclosed

postman.wurth.yu

IP address #1: 10.94.1.4

[+] warning: internal IP address disclosed

webmail.wurth.yu

IP address #1: 10.94.1.8

[+] warning: internal IP address disclosed

[+] 6 (sub)domains and 6 IP address(es) found

[+] 6 internal IP address(es) disclosed

[+] completion time: 57 second(s)

c. **Dnsrecon:** ovaj alat je napisan u Ruby jeziku, a funkcija mu je slična kao i prethodno pomenuti alati. Komanda koju koristimo je „**dnsrecon -d wurth.yu**“ gde otkrivamo SRV ²⁶zapise koji pokazuju koji servisi su aktivni i na kom portu na DNS serverima:

²⁶ Service record

```

Performing General Enumeration of Domain: wurth.yu
[-] DNSSEC is not configured for wurth.yu
[*] SOA dc1.wurth.yu 10.94.1.3
[*] NS dc1.wurth.yu 10.94.1.3
[*] NS dc2.wurth.yu 10.94.1.11
[-] Recursion enabled on NS Server 10.94.1.11
[-] Could not Resolve MX Records for wurth.yu
[*] A wurth.yu 10.94.1.10
[*] A wurth.yu 10.94.1.11
[*] A wurth.yu 10.94.1.3
[*] Enumerating SRV Records
[*] SRV _kerberos._udp.wurth.yu dc1.wurth.yu 10.94.1.3 88 100
[*] SRV _kerberos._udp.wurth.yu dc2.wurth.yu 10.94.1.11 88 100
[*] SRV _gc._tcp.wurth.yu dc1.wurth.yu 10.94.1.3 3268 100
[*] SRV _gc._tcp.wurth.yu dc2.wurth.yu 10.94.1.11 3268 100
[*] SRV _ldap._tcp.wurth.yu dc2.wurth.yu 10.94.1.11 389 100
[*] SRV _ldap._tcp.wurth.yu dc1.wurth.yu 10.94.1.3 389 100
[*] SRV _kerberos._tcp.wurth.yu dc1.wurth.yu 10.94.1.3 88 100
[*] SRV _kerberos._tcp.wurth.yu dc2.wurth.yu 10.94.1.11 88 100
[*] SRV _ldap._tcp.pdc._msdcs.wurth.yu dc1.wurth.yu 10.94.1.3 389 100
[*] SRV _ldap._tcp.dc._msdcs.wurth.yu dc2.wurth.yu 10.94.1.11 389 100
[*] SRV _ldap._tcp.dc._msdcs.wurth.yu dc1.wurth.yu 10.94.1.3 389 100
[*] SRV _kpasswd._udp.wurth.yu dc1.wurth.yu 10.94.1.3 464 100
[*] SRV _kpasswd._udp.wurth.yu dc2.wurth.yu 10.94.1.11 464 100
[*] SRV _kerberos._tcp.dc._msdcs.wurth.yu dc2.wurth.yu 10.94.1.11 88 100
[*] SRV _kerberos._tcp.dc._msdcs.wurth.yu dc1.wurth.yu 10.94.1.3 88 100
[*] SRV _kpasswd._tcp.wurth.yu dc1.wurth.yu 10.94.1.3 464 100
[*] SRV _kpasswd._tcp.wurth.yu dc2.wurth.yu 10.94.1.11 464 100
[*] SRV _ldap._tcp.gc._msdcs.wurth.yu dc1.wurth.yu 10.94.1.3 3268 100
[*] SRV _ldap._tcp.gc._msdcs.wurth.yu dc2.wurth.yu 10.94.1.11 3268 100
[*] SRV _ldap._tcp.ForestDNSZones.wurth.yu dc2.wurth.yu 10.94.1.11 389
100
[*] SRV _ldap._tcp.ForestDNSZones.wurth.yu dc1.wurth.yu 10.94.1.3 389 100
[*] SRV _ldap._tcp.ForestDNSZones.wurth.yu testdc.wurth.yu no_ip 389 100

```

d. **Fierce:** Upotreba ovog programa je slična prethodno pomenutim alatima, ali za razliku od njih, njegova prednost je što Fierce može da pronađe i ostale IP adrese iz mreže i nazive računara u domenu koji ispituujemo i može skenirati domen koristeći istovremeno više različitih tehnika napada. Komanda koju koristimo je „**fierce -dns wurth.yu**“, a nakon nekoliko neuspešnih pokušaja i šaljivih poruka koje dobijamo od programa ipak dobijamo spisak DNS servera i svih računara priključenih na mrežu sa njihovim IP adresama:

```

DNS Servers for wurth.yu:
dc2.wurth.yu
dc1.wurth.yu

```

Trying zone transfer first...

Testing dc2.wurth.yu

Request timed out or transfer not allowed.

Testing dc1.wurth.yu

Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)

Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...

Nope. Good.

Now performing 2280 test(s)...

10.94.1.24 hyperv-mail.wurth.yu

10.94.1.19 hyperv.wurth.yu

10.94.1.18 hal9000.wurth.yu

10.94.1.13 extrem.wurth.yu

10.94.1.8 exchange.wurth.yu

10.94.1.3 dc1.wurth.yu

10.94.1.2 spiderman.wurth.yu

10.94.1.4 postman.wurth.yu

10.94.1.5 konan.wurth.yu

10.94.1.6 wand.wurth.yu

10.94.1.7 hulk.wurth.yu

10.94.1.9 titan.wurth.yu

10.94.1.10 testdc.wurth.yu

10.94.1.11 dc2.wurth.yu

10.94.1.12 ex-konan.wurth.yu

10.94.1.20 crmtest1.wurth.yu

10.94.1.22 eufrat.wurth.yu

...

10.94.1.245 magacin3.wurth.yu

10.94.1.246 andreaalap.wurth.yu

10.94.1.251 magacin3.wurth.yu

10.94.1.254 acerone1.wurth.yu

10.94.1.39 access.wurth.yu

10.94.1.8 webmail.wurth.yu

Subnets found (may want to probe here using nmap or unicornscan):

10.94.1.0-255 : 213 hostnames found.

Done with Fierce scan: <http://ha.ckers.org/fierce/>

Found 213 entries. Have a nice day.

4.1.2 Prebrojavanje uređaja na mreži

Kada smo prikupili osnovne informacije o mreži, ključnim serverima, i IP adresama radnih stanica, jednostavne NMAP komande mogu nam pokazati koji

uređaji na mreži su aktivni, a koji ne. Komandom „**nmap -sP 10.94.1.0/24**“ za nešto više od tri sekunde dobijamo imena svih računara na mreži, njihove IP adrese, kao i da li se odazivaju na ping:

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-18 15:05 EDT

Nmap scan report for 10.94.1.0

Host is up (0.00028s latency).

Nmap scan report for 10.94.1.1

Host is up (0.0016s latency).

Nmap scan report for spiderman.wurth.yu (10.94.1.2)

Host is up (0.00029s latency).

Nmap scan report for dc1.wurth.yu (10.94.1.3)

Host is up (0.00090s latency).

Nmap scan report for postman.wurth.yu (10.94.1.4)

Host is up (0.0035s latency).

Nmap scan report for konan.wurth.yu (10.94.1.5)

Host is up (0.0019s latency).

Nmap scan report for wand.wurth.yu (10.94.1.6)

Host is up (0.0011s latency).

Nmap scan report for hulk.wurth.yu (10.94.1.7)

Host is up (0.0019s latency).

Nmap scan report for exchange.wurth.yu (10.94.1.8)

Host is up (0.0014s latency).

Nmap scan report for titan.wurth.yu (10.94.1.9)

Host is up (0.0014s latency).

Nmap scan report for testdc.wurth.yu (10.94.1.10)

Host is up (0.0018s latency).

Nmap scan report for dc2.wurth.yu (10.94.1.11)

Host is up (0.0068s latency).

Nmap scan report for ex-konan.wurth.yu (10.94.1.12)

Host is up (0.0023s latency).

Nmap scan report for extrem.wurth.yu (10.94.1.13)

Host is up (0.0017s latency).

Nmap scan report for 10.94.1.14

Host is up (0.00090s latency).

Nmap scan report for 10.94.1.15

Host is up (0.0023s latency).

Nmap scan report for 10.94.1.16

Host is up (0.0023s latency).

Nmap scan report for 10.94.1.17

Host is up (0.0015s latency).

Nmap scan report for hal9000.wurth.yu (10.94.1.18)

Host is up (0.000049s latency).

Nmap scan report for hyperv.wurth.yu (10.94.1.19)

Host is up (0.0032s latency).

Nmap scan report for crmtest1.wurth.yu (10.94.1.20)

Host is up (0.000083s latency).

Nmap scan report for 10.94.1.21

Host is up (0.0023s latency).

Nmap scan report for eufrat.wurth.yu (10.94.1.22)

```

Host is up (0.000063s latency).
Nmap scan report for 10.94.1.23
Host is up (0.0022s latency).
Nmap scan report for hyperv-mail.wurth.yu (10.94.1.24)
Host is up (0.0068s latency).
Nmap scan report for nenadzdrlap.wurth.yu (10.94.1.25)
Host is up (0.000083s latency).
...
...

Host is up (0.000074s latency).
Nmap scan report for 10.94.1.252
Host is up (0.000033s latency).
Nmap scan report for 10.94.1.253
Host is up (0.00016s latency).
Nmap scan report for acerone1.wurth.yu (10.94.1.254)
Host is up (0.00033s latency).
Nmap scan report for 10.94.1.255
Host is up (0.00057s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 3.53 seconds

```

4.1.3 Pronalaženje otvorenih portova i aktivnih servisa na uređajima

Sada kada imamo spisak svih računara, pomoću NMAP skenera možemo da proverimo koji su portovi otvoreni i koji su servisi aktivni na svakom od njih. U naredna dva primera dat je pregled jedne radne stanice običnog korisnika, radne stanice sistem administratora i jednog servera. Koristeći komandu „**nmap IP adresa**“ dobijamo željene rezultate.

Prvo skeniramo jedan računar koji koriste obični korisnici:

```

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-18 19:22 EDT
Nmap scan report for magacin6.wurth.yu (10.94.1.94)
Host is up (0.0013s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5800/tcp   open  vnc-http
5900/tcp   open  vnc

```

Zatim proveravamo računar sistem administratora, na kojem se pored standardnih kompanijskih servisa i podešavanja nalaze i određeni programi za testiranje i razni alati koji komuniciraju sa serverima, i tu nalazimo znanto više potencijalnih propusta:

```

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-18 19:25 EDT
Nmap scan report for dusan.wurth.yu (10.94.1.147)
Host is up (1.7s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE

```

80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft-ds
514/tcp	filtered	shell
902/tcp	open	iss-realsecure
912/tcp	open	apex-mesh
990/tcp	filtered	ftps
2607/tcp	open	connection
2869/tcp	open	icslap
3389/tcp	open	ms-wbt-server
5800/tcp	open	vnc-http
5900/tcp	open	vnc
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49157/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 18.02 seconds

I na kraju provera otvorenih portova na DNS serveru daje sledeće rezultate:

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-18 19:28 EDT

Nmap scan report for dc1.wurth.yu (10.94.1.3)

Host is up (1.1s latency).

Not shown: 974 closed ports

PORT	STATE	SERVICE
------	-------	---------

53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
514/tcp	filtered	shell
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapsl
1311/tcp	open	rxmon
1688/tcp	open	nsjtp-data
2161/tcp	open	apc-agent
3052/tcp	open	powerchute
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl
3389/tcp	open	ms-wbt-server
5800/tcp	open	vnc-http
5900/tcp	open	vnc
6547/tcp	open	powerchuteplus
49152/tcp	open	unknown
49153/tcp	open	unknown

```
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
```

Nmap done: 1 IP address (1 host up) scanned in 55.61 seconds

4.1.4 Detektovanje mrežnih propusta

Ranjive tačke na mreži mogu biti pronađene koristeći i NMAP i OpenVAS, što je i objašnjeno kako u narednim testovima. Koristeći NMAP mi pored portova možemo otkriti i koji su sve servisi aktivni na radnim stanicama. Razne NMAP komande i podešavanja su prikazana u dodatku 1.

4.2 Drugi test: NMAP modul

Svrha ovog testa: prikazati mogućnosti i korisnost NMAP skenera i kako NMAP skenira mrežu na ranjivosti. Ovaj test simulira PC sa kojeg napadač pokušava da skenira druge računare u mreži. NMAP mrežni skener će biti pokrenut i lokalnoj mreži. Razne NMAP skripte će se izvršavati skenirajući portove i potencijalne propuste na ciljanim računarima u mreži. Takođe, na serveru je instaliran i SNORT softver za detekciju upada koji će osluškivati mrežu i beležiti dolazni/odlazni mrežni saobraćaj na testnim računarm.

SNORT sistem za detekciju upada će koristiti i podrazumevana podešavanja, a i dodatna podešavanja korisnika da bi se detektovao bilo koji pokušaj probijanja sistema i da bi se kreirali izveštaji o pokušajima napada. SNORT IDS će upisivati svaki pokušaj upada u sistem (kao što je npr. skeniranje portova) sa napadačeve strane u lokalnu MySQL bazu za kasnije analiziranje.

4.2.1 Opis testnog okruženja

Testno okruženje se nalazi na Linux virtualnoj mašini koja se nalazi u lokalnoj mreži i na kojoj je instaliran NMAP skener odakle se skenira ostatak mreže sa Windows operativnim sistemima. Za prikupljanje dodatnih podataka koristićemo i SNMP²⁷ mrežni protokol kako bi otkrili više podataka o mrežnim uređajima.

4.2.2 Plan testa

Prva faza: osnovni program će biti implementiran da bi proverili da li NMAP radi kako je i predviđeno.

Druga faza: Identifikovanje mrežnih ranjivosti na ciljanim računarima.

4.2.2.1 Faza 1

Ovde su predstavljene razne karakteristike i mogućnosti NMAP modula:

²⁷ Simple network management protocol

1. **Otkrivanje aktivnih računara na mreži** koristeći komandu „nmap -n -sn 10.94.1.2-16“²⁸ gde za rezultat dobijamo 15 aktivnih radnih stanica i servera;

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-20 21:13 EDT

Nmap scan report for 10.94.1.2

Host is up (0.029s latency).

...

Nmap done: 15 IP addresses (15 hosts up) scanned in 0.47 seconds

2. **Skeniranje portova i otkrivanje aktivnih servisa:** komandom nmap -p1-1000 -sV 10.94.1. 147 skeniramo 3 računara na mreži u potrazi za svim mogućim otvorenim portovima i aktivnim servisima na njima.

Host is up (1.0s latency).

Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

80/tcp	open	http	Microsoft IIS httpd 7.5
--------	------	------	-------------------------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
---------	------	-------------	----------------------------------

443/tcp	open	https	
---------	------	-------	--

445/tcp	open	microsoft-ds	(primary domain: WURTH)
---------	------	--------------	-------------------------

514/tcp	filtered	shell	
---------	----------	-------	--

902/tcp	open	ssl/vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
---------	------	-----------------	--

912/tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
---------	------	-------------	---

990/tcp	filtered	ftps	
---------	----------	------	--

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

Otkrivanje operativnog sistema: nmap -O 10.94.1.3,14,147

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-20 21:40 EDT

Stats: 0:00:27 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan

Ping Scan Timing: About 100.00% done; ETC: 21:41 (0:00:00 remaining)

Nmap scan report for dusan.wurth.yu (10.94.1.147)

Host is up (0.34s latency).

Device type: general purpose

Running: Microsoft Windows 7|2012|XP

OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012

cpe:/o:microsoft:windows_xp::sp3

OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3

Nmap scan report for dc1.wurth.yu (10.94.1.3)

Host is up (0.30s latency).

²⁸ Zbog vremena skeniranja i obimnih rezultata ovu fazu testa ćemo sprovoditi na 15 računara od kojih su većina serveri i nekoliko radnih stanica

Not shown: 974 closed ports
Device type: general purpose
Running: Microsoft Windows 7|2012|XP
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3
Nmap scan report for 10.94.1.14
Host is up (0.061s latency).
Device type: WAP|general purpose|storage-misc
Running (JUST GUESSING): Actiontec Linux (99%), Linux 2.4.X|3.X (98%),
Microsoft Windows 7|2012|XP (96%), BlueArc embedded (91%)
OS CPE: cpe:/o:actiontec:linux_kernel cpe:/o:linux:linux_kernel:2.4
cpe:/o:linux:linux_kernel:3 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_xp::sp3
cpe:/h:bluearc:titan_2100
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (99%), DD-WRT
v24-sp2 (Linux 2.4.37) (98%), Linux 3.2 (98%), Microsoft Windows 7 or
Windows Server 2012 (96%), Microsoft Windows XP SP3 (96%), BlueArc Titan
2100 NAS device (91%)
No exact OS matches for host (test conditions non-ideal).

3. Različiti formati izveštaja o skeniranju:

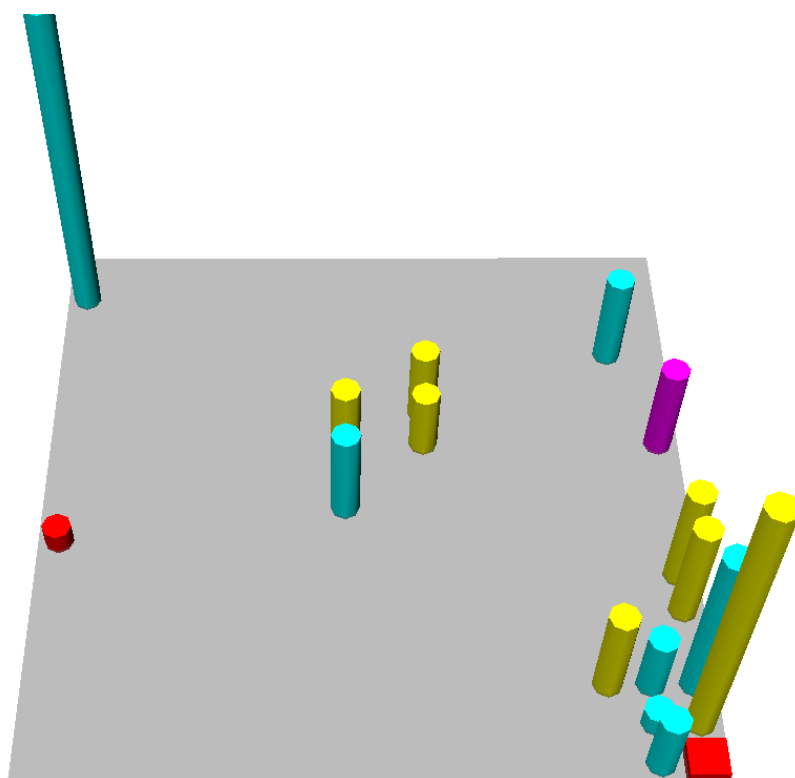
- a. **Sirovi prikaz** predstavlja rezultate NMAP skeniranja koje dobijemo u terminalu, npr:

```

Nmap scan report for 10.94.1.14
Host is up (0.061s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
514/tcp   filtered shell
3306/tcp  open  mysql

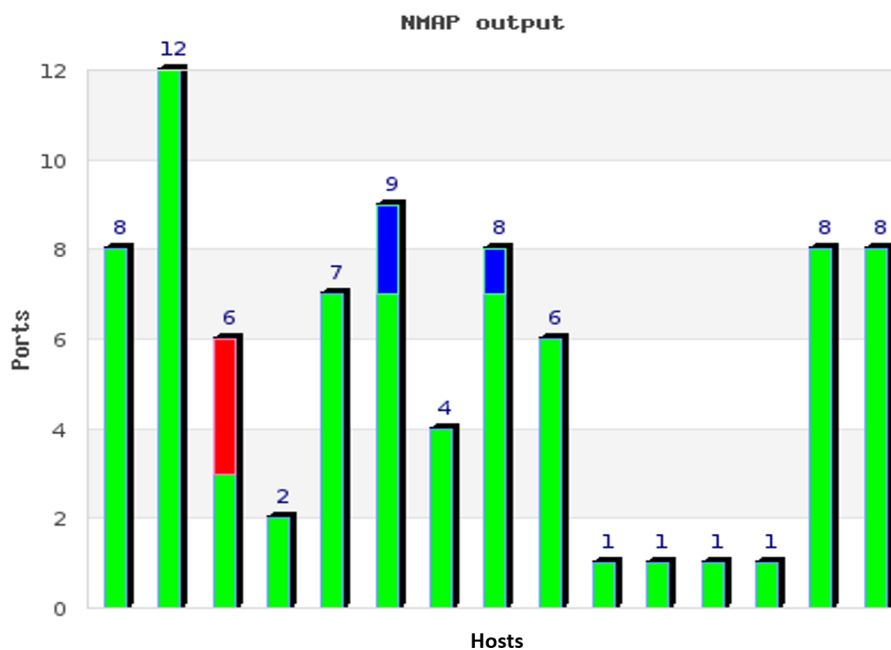
```

- b. **3D prikaz[23]:** Svaka radna stanica je postavljena redom po IP adresi, počevši od malog kvadrata koji predstavlja subnet mreže. Prelaskom miša preko ovog kvadrata dobijamo podatke o mreži i subnetu. Svaka radna stanica ove podmreže predstavljena je kao cilindar. Visina cilindra predstavlja informacije u brojkama o svakoj radnoj stanici, uglavnom predstavlja broj otvorenih portova radne stanice. Prikaz skeniranih računara nalazi se na slici 18.



Slika 18 - 3D prikaz dela skenirane mreže

c. **2D grafik:** Svaka linija predstavlja jednu radnu stanicu. Zelene linije predstavljaju otvorene portove radnih stanica, dok se crvene odnose na zatvorene. Plave linije su filtrirani portovi.



Slika 19 - 2D prikaz dela skenirane mreže

d. HTML format

Nmap Scan Report - Scanned at Wed Oct 21 08:34:44 2015

Scan Summary | **dusan.wurth.yu (10.94.1.147)**

Scan Summary

Nmap 6.49BETA4 was initiated at Wed Oct 21 08:34:44 2015 with these arguments:

```
nmap -T4 -A -p 1-80 -oX proba.xml --stylesheet=nmap.xsl 10.94.1.147
```

Verbosity: 0; Debug level 0

Nmap done at Wed Oct 21 08:35:10 2015; 1 IP address (1 host up) scanned in 26.65 seconds

10.94.1.147 / dusan.wurth.yu

Address

- 10.94.1.147 (IPv4)

Hostnames

- dusan.wurth.yu (PTR)

Ports

The 79 ports scanned but not shown below are in state: **closed**

- 79 ports replied with: **resets**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	Microsoft IIS httpd	7.5
	http-methods	Potentially risky methods: TRACE See http://nmap.org/nsedoc/scripts/http-methods.html				
	http-server-header	Microsoft-IIS/7.5				
	http-title	IIS7				

Slika 20 - HTML format NMAP izveštaja

U ovoj fazi testiranja pored standardnog korišćenja NMAP skenera takođe ćemo videti i kako loše konfigurisan uređaj na mreži može da se pronađe. U našem slučaju skeniramo server kojem je dodeljena IP adresa 10.94.1.12 i između ostalih posmatramo Apache i IIS servise i tražimo njihove ranjivosti. Na ovom serveru je pokrenut značajan broj različitih servisa koji nisu mnogo bitni za funkcionisanje kompanije, a neki servisi se više uopšte i ne koriste, ali nisu ugašeni. Pre same procene ranjivosti radimo pripremna skeniranja da bismo dobili sve potrebne podatke o otvorenim portovima i servisima koji su aktivni na njima.

Procena ranjivosti korišćenjem NSE skripti NMAP modula:

1. Prvo inicijalno skeniramo ciljani server koristeći komandu `nmap 10.94.1.12` gde dobijamo ime servera, spisak otvorenih portova i aktivne servise:

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-22 19:10 EDT
Nmap scan report for ex-konan.wurth.yu (10.94.1.12)

Host is up (0.89s latency).

Not shown: 979 closed ports

PORT STATE SERVICE

80/tcp	open	http
81/tcp	open	hosts2-ns
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft-ds
514/tcp	filtered	shell
900/tcp	open	omginitialrefs
1027/tcp	open	IIS
1031/tcp	open	iad2
1147/tcp	open	capioverlan
1311/tcp	open	rxmon
1433/tcp	open	ms-sql-s
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server
5800/tcp	open	vnc-http
5900/tcp	open	vnc
8000/tcp	open	http-alt
8009/tcp	open	ajp13
50000/tcp	open	ibm-db2
65000/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 45.63 seconds

2. Zatim komandom `nmap -sV 10.94.1.12` dobijamo i tačne nazive servisa koji su aktivni na našem serveru.

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-10-22 19:16 EDT

Nmap scan report for ex-konan.wurth.yu (10.94.1.12)

Host is up (1.6s latency).

Not shown: 979 closed ports

PORT STATE SERVICE VERSION

80/tcp	open	http	Microsoft IIS httpd 6.0
81/tcp	open	http	Apache httpd 2.4.10 ((Win32) OpenSSL/1.0.1h PHP/5.4.31)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
443/tcp	open	ssl/http	Apache httpd 2.4.10 ((Win32) OpenSSL/1.0.1h PHP/5.4.31)
445/tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
514/tcp	filtered	shell	
900/tcp	open	http	Microsoft IIS httpd 6.0
1027/tcp	open	msrpc	Microsoft Windows RPC
1031/tcp	open	iad2?	
1147/tcp	open	capioverlan?	
1311/tcp	open	ssl/rxmon?	
1433/tcp	open	ms-sql-s	Microsoft SQL Server 2000 8.00.760; SP3

```

3306/tcp open  mysql      MySQL (unauthorized)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
5800/tcp open  http-proxy  sslstrip
5900/tcp open  vnc         VNC (protocol 3.3)
8000/tcp open  http-alt?
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
50000/tcp open drda        IBM DB2 Database Server (QDB2/NT)
65000/tcp open  http        Microsoft IIS httpd 6.0
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_server_2003

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 74.25 seconds

3. Sada koristeći NSE skripte NMAP skenera, možemo da proverimo koji od pokrenutih servisa sadrže potencijalne propuste koje zlonamerni korisnici mogu iskoristiti da bi kompromitovali mrežu. Pokazaćemo na dva različita načina kako NSE skriptama testirati mrežu:

a. Skripte koje se nalaze u podrazumevanoj grupi skeniraju naš računar komandom `nmap -T4 -A -v -sC 10.94.1.12`. Kao rezultat vidimo sve potencijalne ranjivosti koje je NMAP skener pronašao, kao i adrese veb sajtova koji bliže opisuju pronađene ranjivosti, način kako ih rešiti i način kako proveriti da li je to zaista mrežni propust. problematični portovi koje je NMAP skener pronašao su 80, 81, 443, 900, 8009 i 65000. Na svim ovim portovima aktivni su Microsoft IIS ili Apache web servisi. Na svim ovim portovima nalazi se intranet stranica preduzće u nekoj od prvih faza razvoja koja je vremenom zaboravljena. Na portu 81 je instaliran Wordpress koji nije zaživeo kao rešenje u kompaniji, ali je i dalje aktivan i može mu se pristupiti, a nove zakrše nisu instalirane više od godinu dana. Na ostalim portovima na kojima je aktivan IIS servis nalaze se još starije verzije u raznim fazama razvoja, od kojih neke datiraju čak iz 1998. godine. Ovo je jedan veliki propust svih mrežnih administratora koji su radili u kompaniji.

Nmap scan report for ex-konan.wurth.yu (10.94.1.12)

Host is up (0.10s latency).

Not shown: 979 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 6.0

|_http-methods: OPTIONS TRACE GET HEAD POST

|_Potentially risky methods: TRACE

|_See <http://nmap.org/nsedoc/scripts/http-methods.html>

|_http-server-header: Microsoft-IIS/6.0

|_http-title: Under Construction

81/tcp open http Apache httpd 2.4.10 ((Win32) OpenSSL/1.0.1h PHP/5.4.31)

|_http-favicon: Unknown favicon MD5:

3BD2EC61324AD4D27CB7B0F484CD4289

|_http-methods: No Allow or Public header in OPTIONS response (status code

302)

|_http-server-header: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.31
|_http-title: Did not follow redirect to http://ex-konan.wurth.yu/xampp/
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn
443/tcp open ssl/http Apache httpd 2.4.10 ((Win32) OpenSSL/1.0.1h
PHP/5.4.31)
|_http-cisco-anyconnect:
|_ ERROR: Not a Cisco ASA or unsupported version
|_http-favicon: Unknown favicon MD5:
3BD2EC61324AD4D27CB7B0F484CD4289

|_http-methods: No Allow or Public header in OPTIONS response (status code
302)

|_http-server-header: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.31
|_http-title: Access forbidden!
|_Requested resource was https://ex-konan.wurth.yu/xampp/
|_ssl-cert: Subject: commonName=localhost
|_Issuer: commonName=localhost
|_Public Key type: rsa
|_Public Key bits: 1024
|_Signature Algorithm: sha1WithRSAEncryption
|_Not valid before: 2009-11-10T23:48:47
|_Not valid after: 2019-11-08T23:48:47
|_MD5: a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_ssl-date: TLS randomness does not represent time
445/tcp open microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
514/tcp filtered shell
900/tcp open http Microsoft IIS httpd 6.0
|_http-generator: Microsoft FrontPage 5.0
|_http-methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Wurth d.o.o Beograd - Intranet
1027/tcp open msrpc Microsoft Windows RPC
1031/tcp open iad2?
1147/tcp open ms-sql-s Microsoft SQL Server 2008 R2 10.50.1600.00; RTM
1311/tcp open ssl/rxmon?
|_ssl-date: 2015-10-22T23:39:12+00:00; -1s from scanner time.
1433/tcp open ms-sql-s Microsoft SQL Server 2000 8.00.760.00; SP3
3306/tcp open mysql MySQL (unauthorized)
3389/tcp open ms-wbt-server Microsoft Terminal Service
5800/tcp open http-proxy sslstrip
|_http-title: VNC desktop [ex-konan]
5900/tcp open vnc VNC (protocol 3.3)
|_vnc-info:
|_ ERROR: Your connection has been rejected.
8000/tcp open http-alt?
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

```
|_ajp-methods:
|_Supported methods: GET HEAD POST PUT DELETE OPTIONS
|_Potentially risky methods: PUT DELETE
|_See http://nmap.org/nsedoc/scripts/ajp-methods.html
50000/tcp open  drda      IBM DB2 Database Server (QDB2/NT)
|_drda-info:
|_DB2 Version: 9.07.0
|_Server Platform: QDB2/NT
|_Instance Name: DB2
|_External Name: DB2    db2sysc 0E241194%FED%Y00
65000/tcp open  http      Microsoft IIS httpd 6.0
|_http-methods: OPTIONS TRACE GET HEAD POST
|_Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
|_http-server-header: Microsoft-IIS/6.0
|_http-title: ex-konan.wurth.yu - /
```

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 86.74 seconds

Raw packets sent: 1240 (56.150KB) | Rcvd: 1220 (49.194KB)

b. Druga opcija skeniranja na mrežne propuste fokusiraće se samo na http ranjivosti, jer su nam tu najveće mogućnosti za potencijalne propuste koje zlonamerni napadači mogu iskoristiti. Sada koristimo komandu koja znato detaljnije skenira mrežne propuste, ali samo za http servise, kako vreme skeniranja ne bi bilo previše dugo. Komanda koju koristimo je: *nmap -vvv -script „vuln and http-“ 10.94.1.12*. Ovim skeniranjem dobijamo malo čudne rezultate. Servise koje je prethodnim skeniranjem NMAP prepoznao kao ranjive, ovaj način skeniranja nije, ali je pronašao novi propust na portu 8000. ono što je zanimljivo je da NMAP ne pronalazi nikakve propuste na starim HTML stranicama pravljenim u Frontpageu, već su dva glavna propusta u Wordpress instalaciji na portu 443 i u phpMyAdminu na portu 8000.

Nmap scan report for ex-konan.wurth.yu (10.94.1.12)
Host is up, received echo-reply ttl 128 (1.8s latency).
Scanned at 2015-10-22 20:41:01 EDT for 360s
Not shown: 979 closed ports
Reason: 979 resets

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack ttl 128

|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-fileupload-exploiter:
|_http-frontpage-login: false
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
81/tcp open hosts2-ns syn-ack ttl 128
135/tcp open msrpc syn-ack ttl 128
139/tcp open netbios-ssn syn-ack ttl 128
443/tcp open https syn-ack ttl 128
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /wordpress/: Blog
| /wordpress/wp-login.php: Wordpress login page.
| /icons/: Potentially interesting folder w/ directory listing
| /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (win32) openssl/1.0.1h php/5.4.31'
|_ /restricted/: Potentially interesting folder
|_http-fileupload-exploiter:
|_http-frontpage-login: false
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server might not be vulnerable
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
|Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750>
|_ <http://ha.ckers.org/slowloris/>
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-trace: TRACE is enabled
| Headers:
| Date: Fri, 23 Oct 2015 00:41:32 GMT
| Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.31
| Connection: close
| Transfer-Encoding: chunked
|_Content-Type: message/http
| http-vuln-cve2014-2126:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2127:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2128:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2129:
|_ ERROR: Not a Cisco ASA or unsupported version

```

|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't
find wp-login.php
445/tcp open  microsoft-ds syn-ack ttl 128
514/tcp filtered shell no-response
900/tcp open  omginitialrefs syn-ack ttl 128
1027/tcp open  IIS syn-ack ttl 128
1031/tcp open  iad2 syn-ack ttl 128
1147/tcp open  capioverlan syn-ack ttl 128
1311/tcp open  rxmon syn-ack ttl 128
1433/tcp open  ms-sql-s syn-ack ttl 128
3306/tcp open  mysql syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
| http-vuln-cve2014-2126:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2127:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2128:
|_ ERROR: Not a Cisco ASA or unsupported version
| http-vuln-cve2014-2129:
|_ ERROR: Not a Cisco ASA or unsupported version
5800/tcp open  vnc-http syn-ack ttl 128
|_http-frontpage-login: false
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
|_http-litespeed-sourcecode-download: Page: /index.php was not found. Try with an
existing file.
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't
find wp-login.php
5900/tcp open  vnc syn-ack ttl 128
8000/tcp open  http-alt syn-ack ttl 128
|_http-frontpage-login: false
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
| http-phpmyadmin-dir-traversal:
| VULNERABLE:
| phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File
Inclusion
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2005-3299
| PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4
and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect
parameter, possibly involving the subform array.
|
| Disclosure date: 2005-10-nil
| Extra information:
| ../../../../etc/passwd :
|
| References:
| http://www.exploit-db.com/exploits/1244/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
| http-vuln-cve2011-3368:
|_ ERROR: Got no answers from pipelined queries

```

```

|_http-vuln-wnr1000-creds: ERROR: Script execution failed (use -d to debug)
|_http-wordpress-users: [Error] Wordpress installation was not found. We couldn't
find wp-login.php
8009/tcp open  ajp13      syn-ack ttl 128
50000/tcp open  ibm-db2     syn-ack ttl 128
65000/tcp open  unknown    syn-ack ttl 128

```

```

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 20:47
Completed NSE at 20:47, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 364.66 seconds
Raw packets sent: 1130 (49.696KB) | Rcvd: 1133 (45.511KB)

```

c. Skeniranje može biti izvedeno tako da se određenom skriptom dobije više podataka o nekoj mrežnoj ranjivosti. Ova komanda: `nmap -script =http-methods.nse -script-args http-methods.retest=1 10.94.1.12` ne pokazuje samo mrežne ranjivosti, već nam ukazuje i na tačan propust u konfiguraciji http servisa na portu 80. I rezultat koji dobijamo ovim skeniranjem nam govori da imamo propust samo na portu 80. Nakon svih ovih rezultata potrebno je detaljnije analizirati izveštaje i proveriti sve potencijalne mane ili jednostavno ugasiti servise koji se više ne koriste.

```

Nmap scan report for ex-konan.wurth.yu (10.94.1.12)
Host is up (1.5s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
80/tcp    open  http
| http-methods: OPTIONS TRACE GET HEAD POST
| Potentially risky methods: TRACE
| See http://nmap.org/nsedoc/scripts/http-methods.html
| OPTIONS / -> HTTP/1.1 200 OK
|
| TRACE / -> HTTP/1.1 501 Not Implemented
|
| GET / -> HTTP/1.1 200 OK
|
| HEAD / -> HTTP/1.1 200 OK
|
|_POST / -> HTTP/1.1 405 Method Not Allowed
81/tcp    open  hosts2-ns
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
|_http-methods: No Allow or Public header in OPTIONS response
(status code 302)
445/tcp   open  microsoft-ds
514/tcp   filtered shell
900/tcp   open  omginitialrefs

```

```

1027/tcp open  IIS
1031/tcp open  iad2
1147/tcp open  capioverlan
1311/tcp open  rxmon
1433/tcp open  ms-sql-s
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5800/tcp open  vnc-http
5900/tcp open  vnc
8000/tcp open  http-alt
8009/tcp open  ajp13
50000/tcp open  ibm-db2
65000/tcp open  unknown

```

Nmap done: 1 IP address (1 host up) scanned in 13.79 seconds

Nakon skeniranja našeg servera već ugrađenim skriptama, da bi dobili dodatne rezultate i detaljniju analizu, pokušali smo i sa dodatkom *Vulscan* dodatkom NMAPu. Međutim, koristeći komandu *nmap -sV --script=vulscan 10.94.1.12* dobijamo jako detaljan izveštaj koji nam govori kako je naš server potpuno zaštićen i kako nema ni jednog jedinog mrežnog propusta.

Ukoliko je potencijalni napadač u stanju da iskoristi bilo koji propust i uspostavi konstantan pristup mreži, on tu vezu i održava kroz pomenuti ranjivi port. Nakon toga je u mogućnosti da mnogo lakše skenira celu mrežu u potrazi za podacima koji su mu potrebni i novim ranjivim uređajima koji će mu omogućiti još više privilegija.

4.2.2.2 Faza 2

U fazi dva skeniraćemo jedan mrežni Access Point sa otvorenim SNMP protokolom i pokušati da otkrijemo njegovu lozinku koristeći brute force napad. Glavna namena ovog uređaja je da gostima firme i zaposlenima koji koriste mobilne telefone omogući da imaju internet na bilo kom mestu u zgradi. Uređaju je dodeljena IP adresa 10.94.1.56.

1. Skeniranje portova i identifikacija svih pokrenutih servisa: Pošto je ovo identičan postupak kao u fazi jedan, nećemo ponavljati korake, već ćemo u tabeli 7 prikazati kombinovani rezultat.

2. Procena ranjivosti: da bi skratili dužinu napada, za lozinku sam koristio samo pet slova – naziv kompanije. NMAP skeneru je trebalo nekoliko minuta da otkrije administratorsku šifru uređaja. Komanda koja je korišćena za SNMP napad je najprostija verzija ovog napada *nmap -sU --script snmp-brute 10.94.1.56*. Nakon dobijanja administratorske lozinke za mrežni uređaj korisnik može preduzeti dalje mere za kompromitovanje mreže. Prva stvar koju može da uradi je da proveri DHCP tabelu odakle vidi sve priključene bežične uređaje koje može da napadne. U ovo spadaju i privatni mobilni telefoni na kojima se mogu nalaziti poruke osetljive sadržine kao što su PIN brojevi kreditnih kartica ili neki drugi osetljivi podaci.

Tabela 8 - Otkrivanje lozinke napadom na SNMP protokol

Provera uređaja	<i>Starting Nmap 6.49BETA4 (https://nmap.org) at 2015-10-24 20:43 EDT</i> <i>Nmap scan report for magacin6.wurth.yu (10.94.1.56)</i> <i>Host is up (0.0017s latency).</i> <i>Not shown: 995 filtered ports</i> <i>PORT STATE SERVICE VERSION</i> <i>161/udp open snmp Cisco router</i> <i>MAC Address: 28:C6:8E:BB:74:C7 (Linksys)</i> <i>Service detection performed. Please report any incorrect results at https://nmap.org/submit/.</i> <i>Nmap done: 1 IP address (1 host up) scanned in 8.46 seconds</i>
SNMP brute-force napad	<i>Starting Nmap 6.49BETA4 (https://nmap.org) at 2015-10-24 20:43 EDT</i> <i>Nmap scan report for magacin6.wurth.yu (10.94.1.56)</i> <i>Host is up (0.0017s latency).</i> <i>Not shown: 995 filtered ports</i> <i>PORT STATE SERVICE</i> <i>161/udp open snmp</i> <i> snmp-brute:</i> <i> wurth – valid credentials</i> <i>MAC Address: 28:C6:8E:BB:74:C7 (Linksys)</i> <i>Nmap done: 1 IP address (1 host up) scanned in 264.46 seconds</i>

4.3 Treći test: OpenVAS modul

Cilj ovog testa: Ovde ćemo skenirati mrežu posebno sa OpenVAS skenerom, a i sa mrežnim skenerom koji smo dobili integracijom NMAP i OpenVAS softvera. Cilj testa je da pokažemo da će integrisani NMAP skener doprineti znatnom smanjenju vremena potrebnom za skeniranje mreže. Ovo je prilično bitno kod velikog broja računara u mreži. Kao što je već pomenuto skeniranje samo sa OpenVAS skenerom traje prilično dugo i u ovom testu ćemo pokazati kako da efikasno smanjimo vreme skeniranja velikog broja računara.

4.3.1 Opis testnog okruženja

U kompniji postoji nešto više od 100 računara koji su povezani na 5 svičeva sa oko 20 radnih stanica na svakom te je tako napravljeno 5 grupa koje su testirane posebno i njihova vremena su prikazana u tabeli 8. Prvu grupu čine računari sa prvog sviča u rack ormaru, drugu računari sa prva dva sviča itd. Poslednju grupu čine svi računari na svih 5 svičeva.

4.3.2 Plan testiranja

Faza 1: Testiranje samo jedne radne stanica sa OpenVAS i OpenVAS+NMAP skenerom da bi ustanovili da oba programa rade korektno.

Faza 2: kada ustanovimo da je sve instalirano i konfigurisano kako treba, skeniraćemo svaku grupu posebno. Svaka grupa računara je testirana koristeći opciju „Full and Fast“ i sa OpenVAS i sa OpenVAS+NMAP softverom. Podešavanja programa su podrazumevana za tu opciju skeniranja i tu ništa nije menjano. Vreme skeniranja svake grupe je zabeleženo.

4.3.2.1 Faza 1: testiranje samo jedne radne stanice sa oba skenera

Koristeći OpenVAS skener za IP adresu 10.94.1.13 dobijamo rezultate prikazane na slici 21.



Slika 21 - OpenVAS izveštaj za 10.94.1.13

Zatim isti test radimo sa integrisanim NMAP skenerom u OpenVAS:

```
High Risk Issues:      2
Medium Risk Issues:   3
Low Risk Issues:       2
False Positives:       0
Logs:                  27
```

Slika 22 - OpenVAS+NMAP izveštaj za 10.94.1.13

4.3.2.2 Faza 2: Skeniranje kompletne računarske mreže

Svaku od pet grupa koja je napravljena skenirane su sa oba skenera vreme skeniranja za svaku grupu je prikazano u tabeli 8. iz ovog testa možemo zaključiti da što više povećavamo broj računara vreme skeniranja se smanjuje za integrisani skener.

Tabela 9 - vreme skeniranja različitog broja računara

Grupa	OpenVAS vreme skeniranja	Vreme skeniranja integrisanog skenera	razlika u sekundama
1	0:11:59	0:11:11	48
2	0:33:16	0:31:40	96
3	0:37:48	0:35:26	142
4	1:02:56	0:34:02	1735
5	1:12:31	0:38:14	2074

4.4 Četvrti test: OpenVAS izveštaj skeniranja određenih radnih stanica

Cilj testiranja: Ovim testom smo obuhvatili ključne servere, nekoliko računara sa administratorskim pravima i nekoliko računara koji još uvek rade na XP operativnom sistemu. Cilj testa je proveriti koliko propusta može da se nađe na operativnim sistemima na kojima se zakrpe ne instaliraju često.

Opis testnog okruženja: U ovom slučaju korišćen je Greenbone veb aplikacija koja je deo OpenVAS skenera za testiranje ciljanih računara. Na slikama 23 i 24 prikazani su prvi rezultati koji ne pokazuju ni malo lepu sliku, naročito ako se uzme u obzir to da većinu ovih računara čine serveri.

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
deep (Automatically generated by wizard)	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.13	Done	1 (1)	Oct 17 2015	9.3 (High)		     
Immediate scan of IP 10.94.1.13	Done	1 (1)	Oct 17 2015	9.3 (High)		     
Immediate scan of IP 10.94.1.134	Done	1 (1)	Oct 17 2015	9.3 (High)		     
Immediate scan of IP 10.94.1.138	Done	1 (1)	Oct 17 2015	5.0 (Medium)		     
Immediate scan of IP 10.94.1.14	Done	1 (1)	Oct 17 2015	5.8 (Medium)		     
Immediate scan of IP 10.94.1.140	Done	1 (1)	Oct 17 2015	5.0 (Medium)		     
Immediate scan of IP 10.94.1.145	Done	1 (1)	Oct 17 2015	6.4 (Medium)		     
Immediate scan of IP 10.94.1.147	Done	1 (1)	Oct 17 2015	5.0 (Medium)		     
Immediate scan of IP 10.94.1.189	Done	1 (1)	Oct 17 2015	6.4 (Medium)		     
Apply to page contents						
(Applied filter: first=1 rows=10 apply_overrides=1 sort=name)						
1 - 10 of 19 (total: 19)						

Slika 23 - OpenVAS izveštaj

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 10.94.1.216	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.219	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.3	Done	1 (1)	Oct 17 2015	9.3 (High)		     
Immediate scan of IP 10.94.1.4	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.5	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.6	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.6	Done	1 (1)	Oct 17 2015	10.0 (High)		     
Immediate scan of IP 10.94.1.8	Done	1 (1)	Oct 17 2015	6.4 (Medium)		     
Immediate scan of IP 10.94.1.94	Done	1 (1)	Oct 17 2015	5.0 (Medium)		     
Apply to page contents						
(Applied filter: first=11 rows=10 apply_overrides=1 sort=name)						
11 - 19 of 19 (total: 19)						

Slika 24 - OpenVAS izveštaj

Kada pogledamo izveštaj skeniranja za domen kontroler na adresi 10.94.13 koji je prikazan na slici 25, vidimo da postoji jedan kritičan propust, 19 srednje opasnih propusta i jedan manje opasan propust.

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	9.3 (High)	75%	10.94.1.3	3389/tcp	 
Microsoft RDP Server Private Key Information Disclosure Vulnerability	6.4 (Medium)	75%	10.94.1.3	3389/tcp	 
DCE Services Enumeration	5.0 (Medium)	75%	10.94.1.3	135/tcp	 
DCE Services Enumeration	5.0 (Medium)	75%	10.94.1.3	135/tcp	 
LDAP allows null bases	5.0 (Medium)	75%	10.94.1.3	389/tcp	 
Use LDAP search request to retrieve information from NT Directory Services	5.0 (Medium)	75%	10.94.1.3	389/tcp	 
Use LDAP search request to retrieve information from NT Directory Services	5.0 (Medium)	75%	10.94.1.3	3268/tcp	 
VNC security types	5.0 (Medium)	75%	10.94.1.3	5900/tcp	 
SSL Certification Expired	5.0 (Medium)	75%	10.94.1.3	6547/tcp	 
Check for SSL Weak Ciphers	4.3 (Medium)	75%	10.94.1.3	1311/tcp	 
Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	99%	10.94.1.3	1311/tcp	 
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	75%	10.94.1.3	1311/tcp	 
OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (FREAK)	4.3 (Medium)	80%	10.94.1.3	1311/tcp	 
Check for SSL Weak Ciphers	4.3 (Medium)	75%	10.94.1.3	2161/tcp	 
Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	99%	10.94.1.3	2161/tcp	 
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	75%	10.94.1.3	2161/tcp	 
Check for SSL Weak Ciphers	4.3 (Medium)	75%	10.94.1.3	6547/tcp	 
Web Server Cross Site Scripting	4.3 (Medium)	75%	10.94.1.3	6547/tcp	 
Deprecated SSLv2 and SSLv3 Protocol Detection	4.3 (Medium)	99%	10.94.1.3	6547/tcp	 
POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	4.3 (Medium)	75%	10.94.1.3	6547/tcp	 
TCP timestamps	2.6 (Low)	75%	10.94.1.3	general/tcp	 

Slika 25 - Izveštaj skeniranja domen kontrolera

Svi ovi propusti su jako zabrinjavajući na prvi pogled, međutim kada detaljnije pogledamo i analiziramo svaki od ovih propusta, možemo videti da rešenje za taj problem već postoji u vidu nove zakrpe za operativni sistem. Ono što OpenVAS skener odlikuje je detaljna analiza svakog propusta koji pronade uz njegov opis, link ka rešenju problema i linkovima ka još detaljnijoj analizi propusta i načinima napada na taj vid propusta – slika 26.

Međutim, ono što zabrinjava u ovom izveštaju je politika firme da se Microsoft ažuriranja isključuju i na serverima, a većinom i na radnim stanicama, jer nove softverske verzije mogu doneti probleme.

Drugi veliki problem je što u sistemu postoji određen broj radnih stanica sa XP operativnim sistemom za koji je podrška prestala da postoji u aprilu 2014. godine i od tada nije bilo novih ažuriranja. Dodatni problem tih radnih stanica je što se na njima nalaze specifične namenske aplikacije koje i mogu da rade isključivo na XP računarima i koje se takođe godinama nisu ažurirale. Problem sa njima je što ni mrežni skeneri ne mogu da ih analiziraju i da nam ukažu na eventualne propuste u izradi tih aplikacija.

Result Details

Task: Immediate scan of IP 10.94.1.3
ID: c967f110-66cb-4701-b53f-bf38d07b0fe6

Vulnerability	Severity	QoD	Host	Location	Actions
Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387)	9.3 (High)	75%	10.94.1.3	3389/tcp	

Summary
This host is missing a critical security update according to Microsoft Bulletin MS12-020.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation could allow remote attackers to execute arbitrary code as the logged-on user or cause a denial of service condition. Impact Level: System/Application

Solution
Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link, <http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

Affected Software/OS
Microsoft Windows 7 Service Pack 1 and prior Microsoft Windows XP Service Pack 3 and prior Microsoft Windows 2K3 Service Pack 2 and prior Microsoft Windows Vista Service Pack 2 and prior Microsoft Windows Server 2008 Service Pack 2 and prior

Vulnerability Insight
The flaws are due to the way Remote Desktop Protocol accesses an object in memory that has been improperly initialized or has been deleted and the way RDP service processes the packets.

Vulnerability Detection Method
Details: [Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities \(2671387\)](#) (OID: 1.3.6.1.4.1.25623.1.0.902818)
Version used: \$Revision: 174 \$

References
CVE: [CVE-2012-0002](#), [CVE-2012-0152](#)
BID: [52353](#), [52354](#)
CERT: [DFN-CERT-2012-0477](#)
Other: <http://blog.binaryninja.org/?p=58>
<http://secunia.com/advisories/48395>
<http://support.microsoft.com/kb/2671387>
<http://www.securitytracker.com/id/1026790>
<http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

Slika 26 - Analiza propusta u operativnom sistemu sa predloženim rešenjem

4.4.1 Zaključak ovog testa

Sa OpenVAS skenerom skenirano je 17 servera i radnih stanica koji su pokazali veliki broj propusta. Zabrinjavajuće je što je skener mnogo veći broj propusta otkrio na ključnim serverima za funkcionisanje sistema nego na radnim stanicama.

Na tih 17 servera i radnih stanica ukupno je pronađeno 28 mrežnih propusta vidokog rizika, čak 157 srednje opasnih propusta i 10 manje opasnih propusta.

Na sreću većina ovih propusta može da se reši samo instaliranjem WSUS aplikacije za redovno ažuriranje svih radnih stanica u mreži uz malo više obraćanja pažnje na serverske zakrpe koje dolaze. Takođe redovno ažuriranje firmvera servera, rutera, štampača je takođe poželjno.

5 Zaključna razmatranja

Svedoci smo da se svakodnevno pojavljuju nove ranjivosti u aplikacijama koje se najviše koriste i čiji proizvođači su se nametnuli kao skoro jedini izbor pri izboru tog tipa softvera (operativni sistem, aplikacije za svakodnevno poslovanje). Mrežni skener koji je korišćen i opisan u ovom radu uspeo je da pronade i upozori na dosta mrežnih propusta, kao i da pokaže da propusti postoje i na mestima koja smo zanemarivali i gde ih nismo očekivali. Mrežni skener je veb aplikacija, koja ima dva važna aspekta mrežne sigurnosti – skeniranje mreže i procena ranjivosti radnih stanica.

U skeniranje mreže spada identifikacija svih aktivnih članova mreže, otkrivanje koji operativni sistem koriste i koji servisi su aktivni na njima. Tokom procene ranjivosti baza podataka sa spiskom svih ranjivosti se upoređuje sa podacima prikupljenih tokom mrežnog skeniranja i kreira se izveštaj sa spiskom svih propusta koji se nalaze u skeniranoj mreži. Mrežni skener takođe proverava da li pronađeni mrežni propust može biti zloupotrebljen ili ne i kolika je stvarna opasnost od njega.

Korišćene su sve funkcije OpenVAS i NMAP skenera i to se pokazalo kao najbolja opcija da bi dobili sveobuhvatan rezultat. Kada se NMAP integriše u OpenVAS dobijamo dodatna poboljšanja, veb aplikaciju koja je laka za upotrebu i što je nama najvažnije, otvorenog je koda. Skeniranje sa ovim skenerom se može odvijati ručno kada mi to želimo, na računarima koje izaberemo ili se može podesiti raspored skeniranja u budućnosti koji će se periodično ponavljati po nekim procedurama koje uspostavimo. Dobijeni rezultati su prikazani na različite načine u različitim tipovima izveštaja radi lakše preglednosti i lakše razumljivosti, jer ti izveštaji treba da se predstava i upravljačkom kadru kompanije kako bi imali osnova da se traže sredstva za unapređenje bezbednosti mreže. Ovaj projekat je jedan odličan primer kako može da se implementira i sporvede testiranje mrežne bezbednosti softverom otvorenog koda, ali takođe ima i dosta izazova u sprovođenju i konfigurisanju.

Pored toga, postoji i dosta ograničenja ovog alata i potrebno je instalirati dodatne programe za unapređenje i poboljšanje funkcionisanja. Neka od ograničenja mrežnog skenera su:

1. Za 3D izveštaje potrebno je instalirati VRML plugin;
2. **Autentifikacija:** mrežni skener može da detektuje samo one ranjivosti koje se nalaze u bazi podataka OpenVAS skenera;
3. **Nemogućnost skenera da radi sa namenskim i neserijskim aplikacijama:** baza podataka ranjivosti se odnosi na poznate i raširene aplikacije i operativne sisteme koje su samo jedan deo od svih zlonamernih napada. A činjenica je i da svaka veća kompanija često ima potrebu za pravljenjem specifičnih i samo njima namenjenih aplikacija, a za takve aplikacije ne postoji mogućnost da budu proverene mrežnim skenerima jer za njih nema podataka.
4. **Mrežni skeneri ne mogu da predvide kompleksne napade:** mrežni skeneri su u stanju da detaljno analiziraju svaki mrežni uređaj, da ažuriraju svoju bazu podataka na dnevnom nivou i da nam detaljno opišu svaki pojedinačni problem na koji naiđu i njegovo rešenje. Međutim problem nastaje nakon inicijalnog neželjenog ulaska u mrežu, jer skeneri ne mogu da analiziraju moguće ponašanje i podatke koje napadač može da prikupi

krećući se od računara do računara kada već uspe da se probije u mrežu i koje nove potencijalne propuste napadač može da iskoristi.

5. Mrežni skeneri su u stanju da mnogo olakšaju praćenje mrežne bezbednosti i da olakšaju rad IT menadžerima koji nisu specijalizovani za ovu granu IT industrije, ali mrežni skeneri ne mogu zameniti visoko kvalifikovane stručnjake koji sprovode ovakve testove. Skeneri takođe mogu da pošalju i lažne pozitivne propuste gde će prikazati slabosti mreže tamo gde one ne postoje i lažne negativne rezultate, gde će prevideti sigurnosne propuste. Kvalifikovani stručnjaci treba pažljivo da analiziraju sve podatke koje dobiju od skenera koje koriste da bi pronašli i eliminisali i pogrešne rezultate.
6. Skeniranje mrežnih propusta znatno opterećuje mrežu, koristeći prilično resursa, vremena i potencijalno usporava kompletnu mrežu. A skeneri se ne mogu koristiti noću, jer mrežu treba da analiziraju u realnim uslovima rada.

Ovaj projekat procene mrežne bezbednosti predstavlja samo vrh ledenog brega. Budući projekti imaju mnogo prostora za napredovanje i razvijanje. U sigurnosnu proveru se može uključiti i socijalni inženjering, jer je poznato da je ljudski faktor uglavnom najslabija karika bezbednosti sistema. Zatim, moguća je integracija sa raznim dodatnim programima kako bi se dobilo sveobuhvatno rešenje. Mogući napredak NMAP skenera je da se u njegovu bazu uključi znatno više NSE skripti za testiranje ranjivosti. Takođe i integracija SNORT softvera zajedno sa OpenVAS i NMAP skenerom je moguća. Još jedno moguće proširenje OpenVAS softvera je da se podesi da „čeka“ pogodan momenat kada skenira radne stanice, ukoliko je njihov procesor zauzet preko određenog procenta, jer se dešava da može jako da uspori mašinu ili lak dovede do iznenadnog restarta.

Dodatak 1

NMAP komande

Usage	nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:	
Can pass hostnames, IP addresses, networks, etc. Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254	
-iL <inputfilename>	Input from list of hosts/networks
-iR <num hosts>	Choose random targets
--exclude <host1[,host2][,host3],...>	Exclude hosts/networks
--excludefile <exclude_file>	Exclude list from file
HOST DISCOVERY:	
-sL	List Scan - simply list targets to scan
-sP	Ping Scan - go no further than determining if host is online
-PN	Treat all hosts as online -- skip host discovery
-PS/PA/PU [portlist]	TCP SYN/ACK or UDP discovery to given ports
-PE/PP/PM	ICMP echo, timestamp, and netmask request discovery probes
-PO [protocol list]	IP Protocol Ping
-n/-R	Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>	Specify custom DNS servers
--system-dns	Use OS's DNS resolver

SCAN TECHNIQUES:	
-sS/sT/sA/sW/sM	TCP SYN/ Connect()/ ACK/ Window/ Maimon scans
-sU	UDP Scan
-sN/sF/sX	TCP Null, FIN, and Xmas scans
--scanflags <flags>	Customize TCP scan flags
-sl <zombie host[:probeport]>	Idle scan
-sO	IP protocol scan
-b <FTP relay host>	FTP bounce scan
--traceroute	Trace hop path to each host
--reason	Display the reason a port is in a particular state

PORT SPECIFICATION AND SCAN ORDER:	
-p <port ranges>: Only scan specified ports Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080	
-F	Fast mode - Scan fewer ports than the default scan
-r	Scan ports consecutively - don't randomize
--top-ports <number>	Scan <number> most common ports
--port-ratio <ratio>	Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:	
-sV	Probe open ports to determine service/version info
--version-intensity <level>	Set from 0 (light) to 9 (try all probes)
--version-light	Limit to most likely probes (intensity 2)
--version-all	Try every single probe (intensity 9)
--version-trace	Show detailed version scan activity (for debugging)

SCRIPT SCAN:	
-sC	equivalent to --script=default
--script=<Lua scripts>	<Lua scripts> is a comma separated list of directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...]>	Provide arguments to scripts
--script-trace	Show all data sent and received
--script-updatedb	Update the script database.

OS DETECTION:	
-O	Enable OS detection
--osscan-limit	Limit OS detection to promising targets
--osscan-guess	Guess OS more aggressively

TIMING AND PERFORMANCE:	
Options which take <time> are in milliseconds, unless you append 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).	
-T[0-5]	Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>	Parallel host scan group sizes
--min-parallelism/max-parallelism <time>	Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	Specifies probe round trip time.
--max-retries <tries>	Caps number of port scan probe retransmissions.
--host-timeout <time>	Give up on target after this long
--scan-delay/--max-scan-delay <time>	Adjust delay between probes
--min-rate <number>	Send packets no slower than <number> per second
--max-rate <number>	Send packets no faster than <number> per second

OUTPUT:	
-v	Increase verbosity level (use twice or more for greater effect)
-d[level]	Set or increase debugging level (Up to 9 is meaningful)
--open	Only show open (or possibly open) ports
--packet-trace	Show all packets sent and received
--iflist	Print host interfaces and routes (for debugging)

MISC:	
-6	Enable IPv6 scanning
-A	Enables OS detection and Version detection, Script scanning and Traceroute
--datadir <dirname>	Specify custom Nmap data file location
--send-eth/--send-ip	Send using raw ethernet frames or IP packets
--privileged	Assume that the user is fully privileged
--unprivileged	Assume the user lacks raw socket privileges
-V	Print version number
-h	Print this help summary page.

EXAMPLES:	
nmap -v -A scanme.nmap.org	
nmap -v -sP 192.168.0.0/16 10.0.0.0/8	
nmap -v -iR 10000 -PN -p 80	

Literatura

- [1] Alexey Polyakov, Head of the Global Emergency Response Team, *Corporate Incidents: Lessons Learned, Common and Avoidable Security Policy Mistakes for IT Management*, Kaspersky Lab International Press Tour, Malaga, 16-19 June, 2011
- [2] G. Murali M. Pranavi Y. Navateja K. Bhargavi, *NETWORK SECURITY SCANNER*, M Pranavi et al, Int. J. Comp. Tech. Appl.
- [3] Gordon Lyon, *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*, Insecure Press, ISBN-10:0979958717
- [4] Kavita S. Kumavat, Ranjana P. Dahake, Dr M. U. Kharat, *Overview of vulnerability analysis*, International Journal of Emerging Technology and Advanced Engineering
- [5] *Motion Computing LE1600 Supplementary Manual*, Customer Whitepaper: Motion Tablet PC Security Basics, Rev A03
- [6] Nick Hutton, *Understanding, Commissioning, & Maximising Value from Penetration Testing*, Three Sixty Information Security Ltd
- [7] Patrick Toomey and Greg Ose, *Scanning Reality: Limits of Automated Vulnerability Scanners, Strategy: Limits of Automated Vulnerability Scanners*, Oct 2010
- [8] Shakeel Ali, Tedi Heriyanto, *Backtrack 4, Security by Penetration testing*
- [9] Steven Drew, *Vulnerability Assessments Versus Penetration Tests*, EVP of Client Services, SecureWorks
- [10] VeriSign White Paper, *An Introduction to Network Vulnerability Testing*

Internet izvori:

- [11] About OpenVAS, dostupno na stranici: <http://www.openvas.org/about.html> - posećeno septembra 2015. godine
- [12] About OpenVAS Software, dostupno na stranici: <http://openvas.org/software> – posećeno septembra 2015. godine
- [13] Derrick Cramer, *Corporate network vulnerability explained*, dostupno na stranici: <http://hackertarget.com/nessus-openvas-nexpose-vs-metasploitable> – posećeno septembra 2015. godine
- [14] Jim Orrill, *What Is the Difference Between Active & Passive Vulnerability Scanners?*, Demand Media, dostupno na stranici: <http://smallbusiness.chron.com/difference-between-active-passive-vulnerability-scanners-34805.html>, posećeno oktobra 2015. godine
- [15] Kinney Williams, *Vulnerability list, VISTA Penetration Study Internet and internal network security testing*, Dostupno na stranici: http://www.internetbankingaudits.com/list_of_vulnerabilities.htm, posećeno septembra 2015. godine

- [16] *Limitations of Penetration Testing, Tutorials on Penetration testing tools*, Dostupno na stranici: <http://www.pen-tests.com/limitations-of-penetration-testing.html>, posećeno oktobra 2015. godine
- [17] *OpenVAS Compendium*, dostupno na stranici : <http://www.openvas.org/compendium/openvas-compendium.html>, posećeno oktobra 2015. godine.
- [18] Sudhanshu Chauhan, InfoSec Institute, *Windows Vulnerability Assessment*, Dostupno na stranici: <http://resources.infosecinstitute.com/windows-vulnerability-assessment/> - posećeno septembra 2015. godine
- [19] *Vulnerability Categories*, Dostupno na stranici: https://qualysguard.qualys.com/qwebhelp/fo_help/knowledgebase/vulnerability_categories.htm, posećeno septembra 2015. godine
- [20] <http://elastic-security.com/2013/07/18/automation-of-vulnerability-assessments-with-openvas/> - posećeno oktobra 2015. godine
- [21] <http://sectools.org/tag/vuln-scanners/> - posećeno septembra 2015. godine