Skeniranje mreže i mrežne ranjivosti

Marek, Ana

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA

I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni studij

SKENIRANJE MREŽE I MREŽNE RANJIVOSTI

Završni rad

Ana Marek

Osijek, 2022.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

Obrazac Z1P - Obrazac za ocjenu završnog rada na preddiplomskom sveučilišnom studiju

Osijek, 16.09.2021.

Odboru za završne i diplomske ispite

Prijedlog ocjene završnog rada na preddiplomskom sveučilišnom studiju

Ime i prezime Pristupnika:	Ana Marek
Studij, smjer:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. Pristupnika, godina upisa:	R4093, 28.07.2017.
OIB Pristupnika:	30569684552
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	,
Sumentor iz tvrtke:	
Naslov završnog rada:	Skeniranje mreže i mrežne ranjivosti
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rad:	Skeniranje ranjivosti je postupak detekcije potencijalnih točaka eksploatacije i sigurnosnih propusta na računalu ili mreži. U radu je potrebno pomoću programa za otkrivanje ranjivosti analizirati računala u lokalnoj mreži, te predvidjeti moguće učinkovite protumjere.
Prijedlog ocjene završnog rada:	Vrlo dobar (4)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 2 razina
Datum prijedloga ocjene od strane mentora:	16.09.2021.
Datum potvrde ocjene od strane Odbora:	22.09.2021.

Potvrda mentora o predaji konačne verzije rada:	Mentor elektronički potpisao predaju konačne verzije.
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 25.04.2022.

Ime i prezime studenta:	Ana Marek
Studij:	Preddiplomski sveučilišni studij Računarstvo
Mat. br. studenta, godina upisa:	R4093, 28.07.2017.
Turnitin podudaranje [%]:	3%

Ovom izjavom izjavljujem da je rad pod nazivom**: Skeniranje mreže i mrežne ranjivosti**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora ,

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

1. UVOD

U modernom svijetu teško je zamisliti život bez računala jer ih ljudi koriste gotovo svakodnevno. Kako je primjena i korištenje računala uvelike zastupljena u različitim dijelovima današnjice, potrebno je prepoznati opasnosti koje donosi i kako se zaštiti od istih. Ključno je paziti na privatnost osobnih podataka i voditi brigu o tome s kim ih dijelimo. Internet bankarstvo, kupovina online, komunikacija uz razmjenu raznovrsnih datoteka učestala je pojava. No treba biti svjestan mogućih rizika i na koji način sigurno obaviti te radnje. Računalna sigurnost, ukoliko je jasno shvaćena, nudi izgradnju sveobuhvatne i uspješne zaštite same opreme ili podataka sadržanih na računalu. Sigurnost uz dobro razvijenu strategiju omogućava učinkovito pronalaženje i rješavanje propusta.

Računalne mreže temelj su informacijskih sustava. Povezivanje informacijskih sustava na Internet jedna od najvažnijih uloga računalnih mreža. Osnovni dijelovi računalne mreže su komunikacijske veze i mrežni uređaji, a različiti protokoli čine rad mreže učinkovitim. Raznovrsne mane i propusti računalnih protokola ugrožavaju sigurnost mreže i cjelokupnog informacijskog sustava.

Rad je koncipiran tako da je prvo opisan pojam računalnih mreža te kako upravljati i održavati računalne mreže. Zatim je objašnjeno što je mrežna ranjivost, definirani su načini na koje sustav može biti ugrožen te potencijalni ciljevi napada. Nakon toga slijede ključni principi sigurnosti računalnih mreža. To su koraci uspostavljanja sigurnosti sustava i strategije upravljanja rizikom ukoliko dođe do propusta.

Nadalje, odrađen je proces skeniranja mreže koji za cilj ima nalaženje pravog rješenja ukoliko dođe do propusta, odnosno napada. Skeniranje je obavljeno u Nmap, tj Zenmap grafičom korisničkom sučelju gdje su skenirani portovi i Nessus programu koji je korišten za otkrivanje sigurnosne ranjivosti.

1.1. Zadatak završnog rada

Skeniranje ranjivosti je postupak detekcije potencijalnih točaka eksploatacije i sigurnosnih propusta na računalu ili mreži. U radu je potrebno pomoću programa za otkrivanje ranjivosti analizirati računala u lokalnoj mreži, te predvidjeti moguće učinkovite protumjere.

2. RAČUNALNE MREŽE

Računalna mreža, uz pomoć komunikacijskih kanala, povezuje računala s ciljem olakšane komunikacije i razmjene podataka između korisnika. Sačinjena je od nekoliko (barem dva) međusobno povezanih računala koja posjeduju pojedine zajedničke resurse poput sklopovlja, programa i podataka. Ukoliko računala mogu razmjenjivati informacije smatraju se povezanima. Postoji nekoliko mogućnosti povezivanja na mrežu; dvije glavne kategorije uspostave veza su: žične i bežične.

2.1. Uspostavljanje i rukovanje računalnim mrežama

Uspostavljanje računalnih mreža zahtijeva ispravnu konfiguraciju, povezivanje te praćenje dijelova mreže. Rukovanje mrežama označava cjelokupno upravljanje komunikacijskom mrežom, spojenim sistemima, aplikacijama i procesima koji su pokrenuti te evidenciju korisnika i njihovih podataka. Uspostavljanje i rukovanje računalnim mrežama provodi administrator mreže [1].

Na nižim razinama modela, mrežna komunikacijska oprema ne zahtjeva konfiguraciju jer postaje funkcionalna već prilikom spajanja u mrežu. Aktivna mrežna oprema sastoji se od svih elektroničkih uređaja koji dohvaćaju i isporučuju promet u računalnim mrežama. Povezivanje aktivne opreme omogućava žični sustav koji tvori pasivnu mrežnu opremu. Pod pasivnu opremu ubrajaju se kabeli, konektori, razvodni paneli, komunikacijski ormari i sustavi za napajanje električnom energijom.

Jednoznačno određene adrese čine razliku između uređaja mreže. Internet kao jedna svjetska računalna mreža, zasnovana na TCP/IP skupu protokola, adresiranje uređaja koji su povezani na tu mrežu ostvaruje primjenom numeričkih IP adresa i naziva.

Na višim razinama modela, upravljanje i održavanje oslanja se na ispravno konfiguriranje korisničkih i poslužiteljskih programa koji služe za određene mrežne usluge te kompatibilan rad tih programa s operacijskim sustavom instaliranim na računalu. Pretežito se po modelu klijent – poslužitelj zasnivaju mrežne usluge računalnih mreža. Poslužitelj, kao element koncepta, može biti: instaliran program na računalu kojemu je zadatak ispunjavati korisnikove zahtjeve, poseban hardverski uređaj osposobljen za obavljanje istih tih zahtjeva ili računalo korišteno u netipičnom smislu, odnosno za njegove potrebe instalirani su poslužiteljski softveri. Računarski koncept klijent – poslužitelj nemoguć je bez međusobne veze. Dakle, ovaj koncept definiran je klijentom koji zahtijeva resurse, podatke ili usluge i poslužiteljom koji te zahtjeve ostvaruje. Pojam klijent

je računalo i/ili program koji može postaviti poslužitelju zahtjev za podacima, primiti odgovor i u konačnici korisniku na zaslonu prikazati pristigle podatke.

Posredovanjem protokola prikladne usluge odvija se komunikacija klijenta i poslužitelja Protokol je definiran skupom pravila koja moraju poštovati obje strane radi uspješne komunikacije. Neke od poznatijih mrežnih usluga na Internetu, uz odgovarajuće protokole, ostvarene modelom klijent – poslužitelj su: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol 3), Telnet itd [1].

Rukovanje računalnim mrežama zahtjevna je i kompleksna zadaća zato što računala povezana na računalnu mrežu prestaju biti izolirani sustavi i postaju podložna interakciji s drugim računalima, korisnicima i mrežama. Obavljanje posla na jednom računalu, od strane mrežnog administratora, potencijalno utječe i na ostale sustave koji su povezani u mrežu.

3. MREŽNA RANJIVOST

Otvorenost ka ostalim mrežama i računalima, kao i moguć pristup informacijama neovisno o fizičkoj odvojenosti prednosti su spajanja u računalnu mrežu. Postoji mogućnost pristupa računalnoj opremi, koja ponekad nije pod nadzorom, s neke udaljene lokacije. Stoga je zahtjevnije zaštiti neki umreženi sustav od izoliranog, odnosno nepovezanog sustava. Glavna zadaća zaštite sustava je osiguranje konzistentnosti i funkcionalnosti sustava te pouzdanost i integritet podataka. Uvođenjem određenih zaštitnih mjera dolazi i do pojave dodatnih restrikcija, što nerijetko može dovesti do smanjenja dostupnosti ili kvalitete usluga. Kako bi zaštita sustava bila učinkovita potreban je kompromis između slobode pristupa uslugama sustava i težnji korisnika za zaštitom vlastitih podataka.

Strategija zaštite sustava definirana je ispitivanjem poznatih prijetnji te načina kako ih riješiti. Potrebno je štititi sustav od zlonamjernih pojedinaca. Isto tako treba štititi sustav od neobrazovanih i/ili nedovoljno upućenih pojedinaca čije greške mogu ugroziti rad sustava. Pod zaštitu sustava ubraja se zaštita mrežne opreme, poslužitelja, radnih stanica i podataka korisnika.

Osnova mrežnih usluga računalnih mreža uglavnom se bazira prema modelu klijent – poslužitelj što treba uzeti u obzir kod planiranja zaštite sustava. Kako su poslužitelji konstantno priključeni na mrežu i korisnicima nude usluge izvan ili na lokalnoj mreži; oni su glavna točka sustava koju treba štititi jer se većina podataka nalazi upravo na njima [2].

Potencijalni ciljevi napadača:

- neovlašten pristup sustavu ili podacima
- brisanje ili promjena podataka
- stvaranje netočnih podataka
- onemogućavanje usluge

Ukoliko smo upoznati s načinima i putevima na koje neki sustav može biti ugrožen, olakšan je plan stvaranja zaštite sustava. Zbog toga je načinjena sistematizacija potencijalnih prijetnji kroz nekoliko nivoa koji su usporedivi s modelom Interneta (TCP/IP) te ISO-OSI komunikacijskim modelom.

3.1. Zlonamjerni softveri

Zlonamjerni softver (eng. malware) je softver koji čini štetu korisniku. To je program pokrenut na računalu bez korisnikove suglasnosti. Cilj takvog programa je zlonamjeran utjecaj, kao što su oštećenja podataka i progama koji se nalaze na sustavu, otuđivanje informacija, nekontrolirano proslijeđivanje nepoželjne elektroničke pošte, neovlašten udaljen pristup na računala, širenje te uključivanje u napade na ostala računala koja su umrežena.

Crvi

Crvi su u početku napravljeni u znanstvene svrhe, korišteni za pronalazak slobodnih procesora, odnosno poboljšanje učinkovitosti mreže i optimizaciju distribuiranog procesa.

Danas služe kako bi iskorištavali propuste u sigurnosti prilikom prijenosa podatatka te imaju sposobnost samoumnožavanja. Koriste mrežne resurse kako bi bez ikakve intervencije stvorili kopije koje zatim šalju mrežom. Pri napadima u potpunosti blokiraju ostali promet mreže i tako utječu na sveobuhvatnu mrežu. Uobičajeno ih povezujemo uz napade na poslovne mreže.

Virusi

Računalni programi koji svojom izvedbom nastoje zaraziti računala nazivaju se virusi. Bez znanja ili dopuštenja samog korisnika računala, kopiraju se u memoriju ili datotečni sustav odabranog računalnog sustava. Jednom pokrenut, virus pretražuje ostale datoteke na računalu s ciljem inficiranja datoteka i konačnim proširivanjem na druga računala. Inficirana datoteka je ona legitimna datoteka u koju je virus uklopio vlastiti programski kod. Virus će se pokrenuti učitavanjem zaražene datoteke u memoriju računala, primjerice otvaranjem dokumenata ili pokretanjem programa. Virusi kao i crvi imaju sposobnost samoumnožavanja. Šire se pokretanjem zaraženih datoteka na drugim računalima, a prenose se putem pohrane na prijenosnim medijima, dijeljenjem direktorija u lokalnoj mreži, elektroničkom poštom, sustavima za razmjenu datoteka i slično.

Trojanski konj

Štetan softver koji služi za inficiranje odabranog računalnog sistema i uzrokuje zlonamjerne aktivnosti naziva se trojanski konj. Takvi programi uobičajeno služe za ometanje performasi računala, otuđivanje osobnih informacija ili razvijanje nekih drugih štetnih vrsta. Hakeri ih koriste za stvaranje štete, neovlašteni udaljen pristup izloženom računalu i zarazu datoteka. Čim trojanski konj dospije u računalo, počinje se sakrivati od svoje žrtve. Trojanski konj je vrlo sličan računalnim virusima te ga je zato teško otkriti, ali za razliku od virusa ne može se sam replicirati. Učinkovitost i štetnost takvih softvera ovisi o namjerama njihova autora i o postupcima žrtve.

Prema načinu na koji napadaju i šteti koji uzrokuju dijele se na:

- trojanski konj koji šalje informacije
- trojanski konj koji omogućava udaljeni pristup
- trojanski konj koji uništava resurse i datoteke računala
- FTP (File Transfer Protocol) trojanci
- proxy trojanci
- trojanski konj koji uskraćivanjem usluge omogućuje napade
- trojanski konj koji onemogućava rad sigurnosnih programa
- trojanski konj koji otvara pojedine Web-stranice

Logičke i vremenske bombe su posebne vrste trojanaca. Logičke bombe se aktiviraju poklapanjem niza okolnosti na ugroženom računalu. Dok je aktivacija u zadano vrijeme ili dan karakteristika vremenskih bombi [3].

Špijunski softveri

Zloćudan softver kojemu je cilj preuzimanje kontrole nad računalom, prikupljanjem podataka o korisniku i njegovom korištenju računala, naziva se špijunski softver. Obično se ne replicira, a korisnik ne zna za njegovu prisutnost.

Oglašivački softveri

Prikazivanje oglasa čak i kada korisnik nije priključen na Internet odlika je oglašivačkog softvera (eng. adware). On poput špijunskog softvera, također narušava privatnost korisnika. Najčešće je prisutan u besplatnim aplikacija, ali se može nalaziti i u ograničeno djeljivim aplikacijama.

Keylogger

Keylogger je zlonamjeran program koji prati korisnikov unos preko tipkovnice. Pojedinci ga svjesno instaliraju na tuđa računala kako bi mogli tajno pratiti aktivnosti te osobe. Keylogger može uzeti snimak ekrana i tako vidjeti što korisnik trenutno radi, s kojim programima ili gdje surfa na Internetu. Informacije koje prikupi većinom dolaze do zlonamjernih osoba.

Lažni antivirusni softveri

Softveri koji se korisniku lažno prikazuju kao pravi nazivaju se lažni antivirusni softveri. Oni pokušavaju navesti korisnika na kupnju programa. Simuliraju pregled računala i pokušavaju zastrašiti korisnika porukom da je pronađen nepostojeći štetni softver koji je moguće ukloniti samo ako korisnik kupi taj antivirusni program. Također, mogu preuzimati prave štetne softvere.

4. KLJUČNI PRINCIPI SIGURNOSTI

Kako bi uvidjeli gdje je sustav najranjiviji potrebno je razumijevanje sigurnosti sustava. Važno je poznavanje ocjenjivanja sigurnosti, principa sigurnosti i dobra praksa kako bi se osigurao pregled ranjivosti sustava. [4][5].

4.1. Ostvariti jednostavnu sigurnost

Ukoliko je sigurnost kompliciranа, otežava se osiguravanje sustava i smanjuje se učinkovitost. Cilj je napraviti sigurnost što jednostavnijom, a to se postiže podjelom u diskretne dijelove:

1. Držanje pokrenutih servisa i informacija podalje od napadača
2. Dopuštanje korisnicima pristupanju određenim informacijama
3. Zaštita svakoga sloja obrane kao da je posljednji
4. Evidencija svakog pokušaja pristupanja osjetljivim informacijama
5. Odvajanje sredstava u skupine i što veća izolacija
6. Izbjegavanje pogrešaka koje svi čine
7. Ne dopušanje da prethodno spomenuti dijelovi budu preskupi

Držanje pokrenutih servisa i informacija podalje od napadača

Prilikom početka izgradnje sigurnosnog sustava važno je zabraniti pristup svima, a zatim na odgovarajući način dizajnirati sisteme i aplikacije. Dakle, podrazumijevano pravilo ove odredbe je zabrana pristupa.

Dopuštanje korisnicima pristupanju određenim informacijama

Obzirom da je podrazumijevano zabranjen pristup svima, neophodno je odrediti što može vidjeti koji korisnik. Administratorima i korisnicima treba dozvoliti pristupanje informacijama koje žele, ali samo do one razine do koje ih trebaju, sve iznad toga stvara nepotreban rizik. Ovakav princip pristupa, u sigurnosnom vokabularu, naziva se najmanja privilegija. Nalik tome, servisi i aplikacije trebaju raditi pod najmanjim privilegijama koje su nužne za rad.

Zaštita svakoga sloja obrane kao da je posljednji

Evolucijom računalnih mreža iz izoliranih mreža do spojenih mreža diljem svijeta, sigurnost je postala kompleksnija. Pouzdanje u samo jedan sloj zaštite loša je i pogubna ideja. Svi slojevi trebaju biti osigurani kao da su zadnji slojevi zaštite između informacija i napadača.

Evidencija svakog pokušaja pristupanja osjetljivim informacijama

Često se dešava da administratori računalnih mreža prilikom početka rada misle o tome koja će ispitivanja trebati tek nakon što dođe do uspješnog napada. Određivanje koje događaje treba pratiti složen je posao. U obzir se treba uzeti nekoliko čimbenika poput veličine loga te djelovanja na izvođenje. Aktiviranje ispitivanja jednostavan je korak, no obrađivanje logova složeniji je posao. Odvajanje bezazlenih logova od onih koji su potencijalno mogli uzrokovati napad iziskuje predznanje i praksu u čitanju log datoteka.

Odvajanje sredstava u skupine i što veća izolacija

Razdvajanje sredstava u skupine onemogućava određenom propustu u nekoj skupini da kompromitira preostale skupina, odnosno cijeli sustav.

Primjenom sljedećih tehnika jača se sigurnost mreža:

1. Pojednostavljenje mrežne arhitekture – lakše je rukovati manjim mrežama, a segregacijom mreža u infrastukturne komponente, velike mreže dijele se u manje. Stvaranjem odjeljaka smanjuju se smetnje prijelaza mrežnih komunikacija.
2. Izrada choke pointa – ovakvo kreiranje omogućava nezavisno odvajanje, tj. isključivanje dijelova mreže ukoliko su oni ugroženi. Trenutačno odvajanje mala je cijena u usporedbi s cijenom moguće štete i gubitaka.
3. Izolacija zona prema razinama povjerenja – jedna od glavnih prednosti podjele u odjeljke je ta da se prema različitim razinama povjerenja mogu segmentirati i izolirati radne stanice i poslužitelji.

Izbjegavanje pogrešaka koje svi čine

Treba biti upoznat s pogreškama koje čine drugi te ih izbjegavati. Informiranje o računalnom kriminalu i sigurnosnim incidentima doprinosi raspoznavanju takvih pogrešaka.

Ne dopušanje da prethodno spomenuti dijelovi budu preskupi

Prilikom izgradnje sigurnosti radi se o rukovanju rizikom, a glavni dio rukovanja je crpljenje vlastitih resursa koje treba djelotvorno rasporediti. Ukoliko se od početka razvija adekvatno i učinkovito, moguće je umanjiti troškove osiguravanja mreža i aplikacija.

4.2. Upravljanje rizikom

U pravilu niti jedna mreža nije posve sigurna. Važno je procijeniti vrijednost imovine jer je više resursa potrebno izdvojiti za osiguravanje bitnije imovine.

Neki od loših primjera rukovanjem prijetnjama su:

- nepotrebno osiguravanje sve imovine na najvišem stupnju, bez obira na upravljivost ili korisnost
- adresiranje prijetnje, ali u ad hoc stilu
- ignoriranje prijetnje i nepoduzimanje ničega da bi se ta prijetnja spriječila

Ako se upravljanje rizikom odvija na neorganiziran i loše isplaniran način može postati vrlo zahtjevno i složeno. Općenito, izgradnja ocjenjivanja rizika uključuje mnogo ljudi iz različitih dijelova tvrtke i može trajati mjesecima.

Moguće je koristiti sljedeće procese za ocjenjivanje i upravljanje rizikom:

1. Postavljanje dosega
2. Identifikacija imovine i određivanje njene vrijednosti
3. Modeliranje prijetnji
4. Dokumentiranje sigurnosnih rizika
5. Određivanje strategije upravljanja rizikom
6. Nadzor imovine
7. Praćenje promjena

Postavljanje dosega

Ocjenivanje i upravljanje sveokupnim sigurnosnim rizicima u nekoj organizaciji dovodi do propusta kritičnih detalja. Najprije treba odrediti doseg projekta ocjenjivanja rizika. To rezultira poboljšanom procjenjivanju troškova i vremena potrebnog za ocjenjivanje sigurnosnih rizika te olakšano praćenje rezultata i dokumentiranje.

Identifikacija imovine i određivanje njene vrijednosti

Nakon ocjenjivanja rizika slijedi identifikacija imovine, a potom određivanje njene vrijednosti. Prilikom određivanja vrijednosti imovine treba uzeti u obzir sljedeće čimbenike:

- Vrijednost imovine hakerima
- Financijski učinak
- Nefinancijski učinak

Pri definiranju do koje mjere će se izgraditi zaštita imovine, vrijednost imovine treba uzeti kao glavni parametar. Ako se neadekvatno procijeni koliko je važna, može doći do situacije gdje se početni izbornik štiti jednako kao i tajne poslovne datoteke.

Financijski utjecaj gubitka ili kompromitiranja imovine, zbog vremena proteklog kada je servis ugašen, obuhvaća dohodak i izgubljenu produktivnost, troškove vezane uz nadoknadu servisa i izravne gubitke opreme.

Nefinancijski utjecaj gubitka ili kompromitiranja imovine obuhvaća resurse potrebne za oblikovanje javne percepcije sigurnosnog incidenta poput reklamnih kampanja i rukovanje gubitkom javnog povjerenja.

Modeliranje prijetnji

Modeliranje prijetnji je proces predviđanja ranjivosti i prijetnji nad imovinom. To je inžinjerska tehnika korištena za identifikaciju opasnosti, napada, ugroženosti i pripadnih zaštitnih mjera te pomaže pri definiranju sigurnosnih ciljeva. Modeliranje prijetnji temelji se na ideji da svi sustavi imaju resurse koje je nužno štititi zbog njihove važnosti. Resursi posjeduju nekoliko različitih ranjivih točaka koje pojedine unutarnje ili vanjske opasnosti mogu upotrijebiti kao način

pristupa s ciljem štetnih radnji. Modeliranje prijetnji nudi strukturirani pristup znatno jeftiniji i učinkovitiji od nasumične primjene svojstava sigurnosti, uz nedovoljnog poznavanje koje opasnosti određeno svojstvo tumači.

Postoji nekoliko pristupa modeliranju prijetnji:

- Pristup usmjeren na resurs – kreće od resursa povjerenih sustavu, kao što su osjetljivi osobnih podaci
- Pristup usmjeren na obranu – vrši procjenu slabosti u sigurnosnom nadzoru
- Pristup usmjeren na programsko rješenje – polazi od dizajna samog sustava i prolazi kroz
  model sustava tražeći napade na svaki element modela
- Pristup usmjeren na napadača – kreće od napadača, procjenjuje njegove namjere i načine na koji ih želi realizirati. Dakle, polazi od napadačevih resursa ili ulaznih točaka u sustav

Dokumentiranje sigurnosnih rizika

Nakon modeliranja prijetnji slijedi dokumentacija sigurnosnih rizika kako bi prijetnje mogle biti pregledane, a mi upoznati s njima. Ključni elementi koje treba obraditi su opis opasnosti i meta opasnosti. Pojam protumjere neophodan je za adresiranje prijetnji, dok pojam napadačke tehnike naglašava iskorištenu ranjivost. Tijekom ove faze obilježja rizika ostaju nepopunjena te se unose prilikom završnog stadija modeliranja prijetnji. Tijekom dokumentacije važno je rangirati rizike kvalitativno ili kvantitativno.

Kvalitativno rangiranje služi se sustavom za ocjenjivanje relativnih utjecaja određenih rizika. Dok se za kvantitativno rangiranje koriste realni i procjenjeni podaci o imovini kako bi se ocjenjila ozbiljnost rizika.

Kvalitativno rangiranje iziskuje tehničke vještine, a kvantitativno uvjetuje računovodstvene vještine. No nijedno od ova dva rangiranja nije nadmoćno nad drugim, već su komplementarni.

Određivanje strategije upravljanja rizikom

Kada je završeno rangiranje rizika, dolazi do određivanja opće strategije upravljanja rizicima te odabira sigurnosnih mjera koje će se primjeniti kako bi podržale takvu strategiju. Ovaj korak rezultira potpunim planom upravljana rizikom. Plan bi u pravilu morao obuhvaćati rizike, prijetnje i potencijalne utjecaje, strategiju upravljanja rizicima te popis sigurnosnih mjera koje će biti poduzete.

Nadzor imovine

Nazdor imovine važan je korak zbog potencijalnog sigurnosnog propusta. Ukoliko dođe do sigurnosnog incidenta potrebno je pokrenuti sve radnje sadržane u planu nepredviđenih situacija te započeti istraživanje kako bi se što prije reducirala načinjena šteta.

Praćenje promjena

Kroz vrijeme, bilo kakve promjene sofvera, hardvera, osoblja ili poslovnih procesa dodati će ili eliminirati sigurnosne rizike. Time će nastati nove ranjivosti i prijetnje. Stoga je važno pratiti sve promjene i redovito obnavljati sigurnosne mjere i plan upravljama rizicima.

4.2.2. Strategije upravljanja rizikom

Postoje četiri opće skupine strategije upravljanja rizikom:

1. Ublažavanje
2. Prijenos
3. Izbjegavanje
4. Prihvaćanje

Ublažavanje

Ublažavanje sigurnosnih rizika najzastupljenija je metoda zaštite računala i mreža. Poduzimaju se proaktivne mjere kako bi se ublažio sigurnosni rizik i smanjila izloženost imovine opasnostima. Instalacija antivirusnog programa najopćenitiji je primjer ublažavanja sigurnosnih rizika. Antivirusnim programi smanjuju izloženost zloćudnim softverima, ali ne mogu u potpunosti eliminirati mogućnost zaraze računala. Prilikom ublažavanja rizika potrebno je razraditi plan nepredvidivih situacija.

Prijenos

Prijenos rizika postoje sve učestalija metoda rukovanjem sigurnosnim rizicma time što se dio prenosi nekom drugom. Razlog prijenosa može biti bolja iskorištenost ekonomskih razmjera ili korištenje usluga i stručnosti drugih tvrtki. Dobar primjer iskorištenosti ekonomije razmjera je osiguranje koje se plaća relativno malo kao naknada za smanjenje financijskih gubitaka ili oporavak kada bi došlo do sigurnosnog rizika. Ugovaranje web hostinga primjer je iskorištenosti usluga i stručnosti drugih tvrtki gdje je ostvarena napredna web sigurnosna usluga uz visoko educirano osoblje, a mi za takvo osoblje nemamo dovoljno resursa za zapošljavanje.

Izbjegavanje

Kako bi se izbjegao rizik, nužno je eliminirati izvor prijetnji i izloženost prijetnjama. Ako postoji mala vjerojatnost ublažavanja i prijenosa te prihvaćanje rizika donosi više štete od koristi, primjenjuje se izbjegavanje rizika.

Prihvaćanje

Prihvaćanje rizika krajnja je reakcija na prijetnju koja prihvaća, bez poduzimanja proaktivnih mjera, cjelovitu izloženost i posljedice koje donose sigurnosne prijetnje. Ako ne postoji drugo rješenje ili su ublažavanje ili prijenos rizika preskupi, rizik se prihvaća kao zadnja mjera. Prilikom prihvaćanja rizika treba napraviti plan nepredvidivih situacija. Plan treba detaljno određivati raspon radnji koje se poduzimanju kada se rizik ostvari. Primjenom plana smanjuje se utjecaj gubitka ili kompromitiranja imovine.

4.3. Načini osiguranja računalne mreže

Potreba zaštite podataka postoji oduvijek, ali neke metode koje su bile prejednostavne nisu omogućavale dovoljnu zaštitu i time narušavale tajnost i sigurnost. Razvojem kriptografije utemeljeni su dobri načini zaštite i kriptiranja dokumenata, no zaštita ne može ovisiti samo o jednoj tehnologiji. Kombinacija sigurnosnih mehanizama, poput antivirusnih programa, sigurnosnih protokola mreža računala (npr. IPSec), kontrole pristupa, kriptiranja i vodenih žigova čini učinkovitu zaštitu.

Antivirusna zaštita

Posebna skupina programa čija je glavna namjena identificiranje, neutraliziranje i eliminiranje crva, virusa, trojanaca i ostalih štetnih programa su antivirusni programi. Ukoliko je računalo zaraženo, zadatak antivirusnog programa je izolacija i uklanjanje opasnosti. U osnovi, svaki virus je računalni program koji je definiran određenom sekvencom okteta, odnosno znakovnih kodova. Antivirusni program nakon detektiranja virusne sekvence u nekoj datoteci će:

- brisanjem virusa pokušati popraviti datoteku
- izolirati datoteku tako da više nijedan program nema pristup toj datoteci i time zaustaviti širenje virusa
- obrisati zaraženu datoteku

Virusi se stalno razvijaju, stoga treba stalno osvježavati bazu definicija i kodova virusa. Ukoliko se baze ne osvježavaju, antivirusni program neće moći prepoznati nove viruse. Programeri virusa sve češće stvaraju takozvane metamorfne viruse kako bi izbjegli mehanizme detekcije virusa. Takvi virusi mijenjaju programski kod kako bi ostali neopaženi.

Još jedan način rada antivirusa je nadzor svih programa i ponašanja. Ukoliko neki program pokuša pristupiti mreži, slati podatke na neki port ili u izvršni kod nekog programa upisivati podatke, antivirusni program će to detektirati i obavijestiti korisnika. Takav pristup proširuje zaštitu i na dosad nepoznate viruse. Zbog ovakvog pristupa, jedini nedostatak je što će antivirusni program ponekad označiti sumnjivim i neke akcije koje su legitimne. Učestalo slanje obavijesti korisnicima, može dovesti do oglušavanja na takve situacije i kada dođe do problema koji iziskuje intervenciju.

Kriptiranje

Enkripcija je važan dio zaštite podataka. To je relativno jednostavan postupak kojim je moguće zaštiti povjerljive podatke u slučaju napada putem fizičkog pristupa računalu. Današnji operacijski sustavi u većini sadrže ugrađene mehanizme kriptiranja pohranjenih podataka. Kriptiranje je postupak preoblikovanja otvorenog teksta u tekst razumljiv, odnosno čitljiv samo onima koji posjeduju poseban ključ za dekriptiranje. Kriptosustavi se dijele na simetrične i asimetrične.

Simetrični kriptosustav sastoji se od jednakog ključa za kriptiranje i dekriptiranje. Komunikacija se sastoji od pošiljatelja i primatelja poruke., a kako bi poruka bila ispravno interpretirana mora se obaviti razmjena tajnoga ključa. Diffie – Hellmanov protokol je uobičajen protokol razmjene tajnog ključa.

Asimetrični kriptosustav definiran je određenim svojstvima brojeva. Sastoji se od javnog i privatnog ključa. Prednost asimetričnog sustava je otklonjen problem distribucije ključa. Ovisno o algoritmu za kriptiranje i duljini kriptografskih ključeva određena je sigurnost kriptiranih dokumenata.

IPSec protokol

Danas većina računalnih mreža kao standard za mrežnu komunikaciju prihvaća TCP/IP skup protokola. Taj skup se bazira na IPv4 (četvrta inačica IP protokola) protokolu. Jedna od mana TCP/IP skupa protokola u standardnom obliku je odsustvo mehanizama koji osiguravaju zaštitu i integritet podataka prilikom prijenosa te mehanizama za izvršavanje autentikacije.

Skup proširenja IPv4 protokola je IPSec. Tim proširenjem jamče se glavni sigurnosni elementi, a to su integritet, autentikacija, tajnost i neporecivost. Usluga komunikacije od kraja do kraja omogućena je IP protokolom. Korištenjem IPSec protokola omogućena je zaštita kanala na istoj razini neovisno o nižim slojevima. Prilikom komunikacije komunikacijski uređaji ne moraju podupirati IPSec. Bez obzira na sloj prijenosa podataka i na način implementacije fizičkog sloja omogućeno je korištenje IPSec protokola. S druge strane, uporaba IPSec protokola je transparentna obzirom na više slojeve ako dva entiteta podržavaju IPSec.

Dakle. IPSec protokol pruža sigurni komunikacijski kanal bez obzira na protokole implementirane u transportnom sloju i njihovu funkcionalnost [6].

4.4. Nepromjenjivi zakoni

Zakoni sigurnosnih ograničenja:

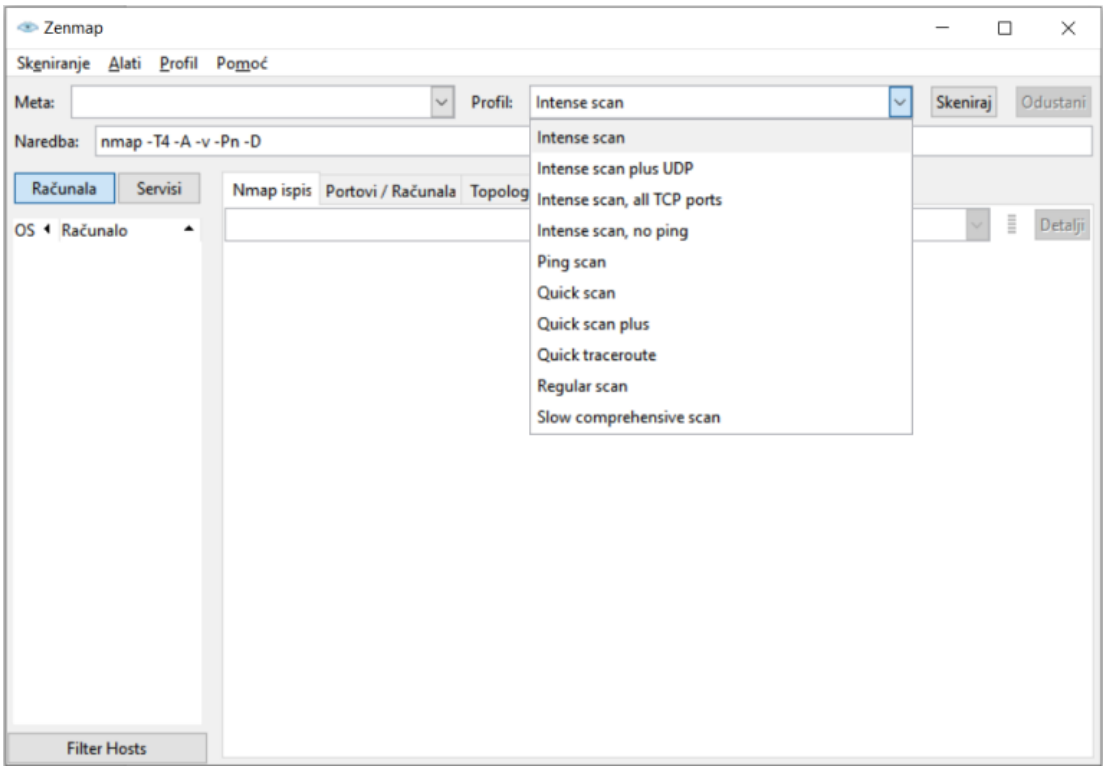
1. Ukoliko napadač uvjeri nekoga da na svom računalu pokrene njegov program – računalo je ugroženo
2. Ukoliko napadač može praviti izmjene operacijskog sustava računala – računalo je ugroženo
3. Ukoliko napadač ima omogućen fizički pristup računalu – računalo je ugroženo
4. Ukoliko je napadaču dopušteno postavljanje svog programa na web stranicu – web stranica je ugrožena
5. Ukoliko je administrator pouzdan – računalo i mreža su sigurni
6. Ukoliko je poznat dekriptirajući ključ, enkriptirani podaci nisu sigurni
7. Apsolutna anonimnost je nepraktična jednako kao i u stvarnom životu
8. Neažurirani antivirusni program malo je bolje rješenje od neposjedovanja antivirusa uopće
9. Snažne lozinke odraz su snažne sigurnosti

5. SKENIRANJE MREŽE

5.1. Nmap/Zenmap

Nmap je program koji služi za skeniranje poslužitelja i sigurnosnu reviziju. Pomoću IP paketa utvrđuje dostupne domaćine na mreži, operacijski sustav na kojem rade, koji se vatrozid i filtri paketa koriste i slično. Zbog svoje učinkovitosti jedan je od najraširenijih korištenih mrežnih skenera, a dizajniran je za brzo skeniranje velikih mreža [7].

Zenmap je grafičko korisničko sučelje Nmap-a. Osim Nmap-ovih svojstava sadrži i neka dodatna, poput grafičke reprezentacije skena, odnosno topologije. Kako bi podaci bili pregledniji u nastavku je korišten Zenmap.

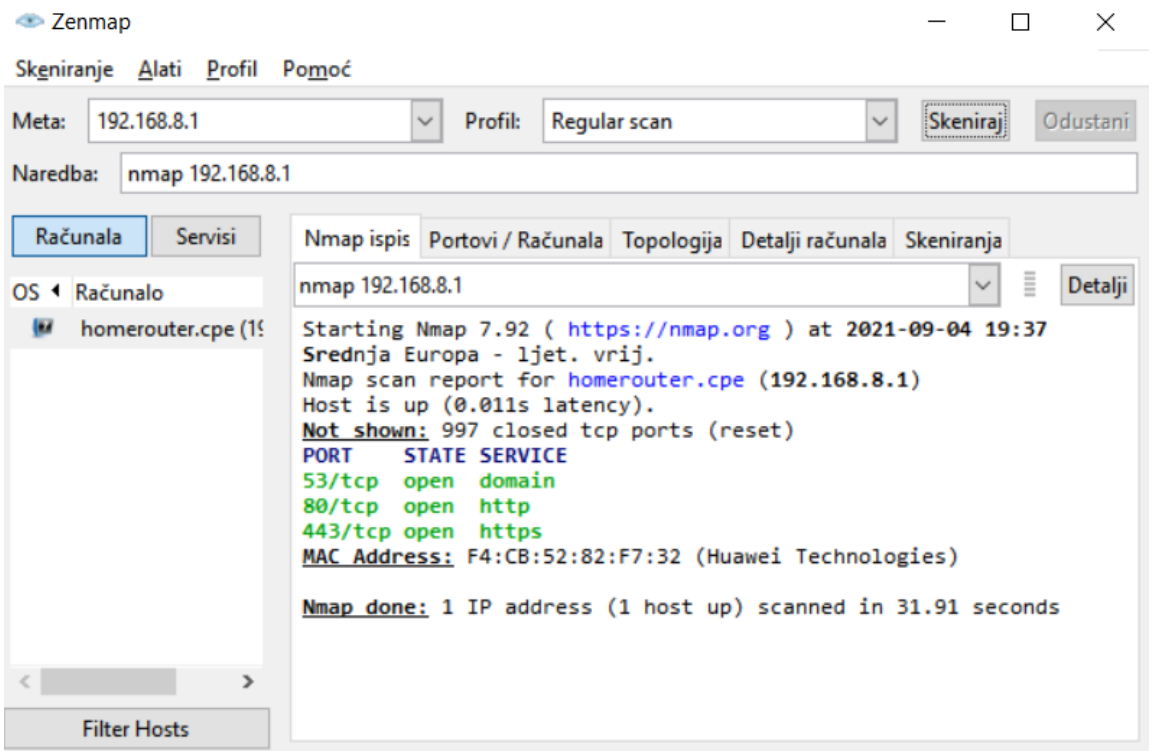


Sl. 5.1 *Zenmap GUI i izbornik s vrstama skeniranja*

U sekciju *Meta* upisuje se ime poslužitelja ili mreže koju želimo skenirati. To može biti raspon IP adresa ili IP adresa u CIDR (engl. Classless Inter-Domain Routing) formatu. Zatim se u sekciji *Profil* odabire vrsta skeniranja. Različite opcije moguće je odabrati pri uređivanju profila označavanjem na pojedine zastavice ili direktnim upisivanjem u sekciju *Naredba* (Slika 5.1). Preporučljivo je prije skeniranja zatražiti dozvolu za skeniranje.

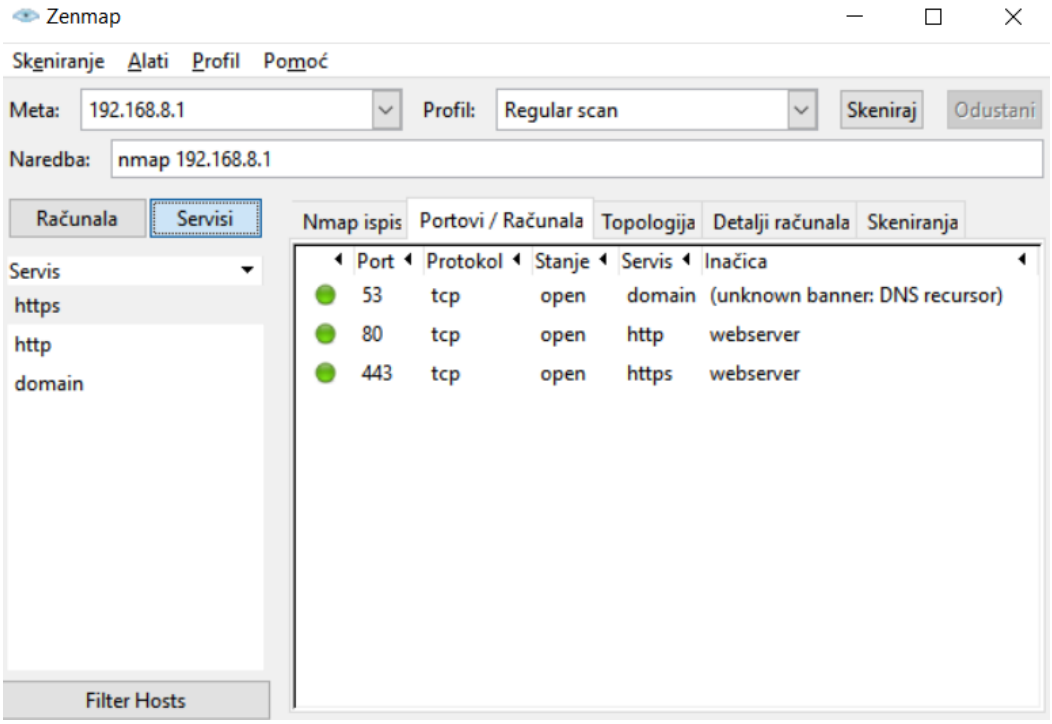
Opcija *-A* omogućuje agresivno skeniranje. Agresivno skeniranje koristi opciju -O za detekciju operacijskog sustava, -sV za detekciju verzije, -sC za skeniranje skripti te traceroute opciju.

Nadalje, opcija *-Pn* služi kako Nmap/Zenmap ne bi prvo pingao sve IP adrese u rasponu mreže te zbog ove opcije skeniranje traje duže. Kada ne bismo koristili ovu opciju program bi pingao samo dohvatljive i žive poslužitelje.

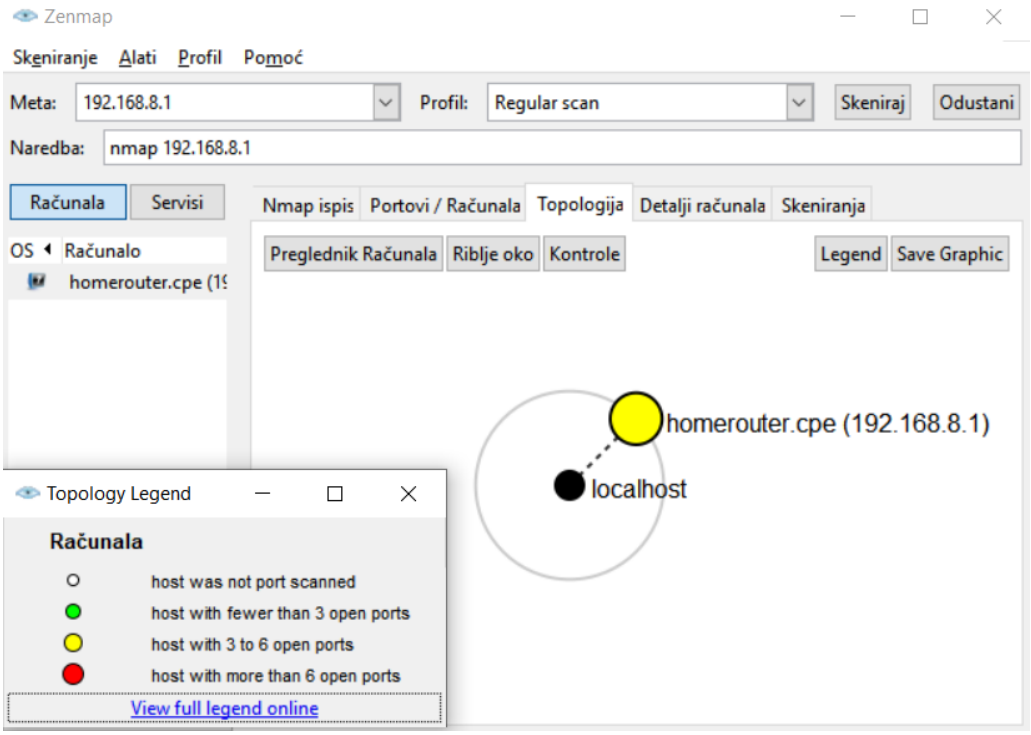


Sl. 5.2 *Rezultat skeniranja*

Kartica Portovi/Računala daje pregled otvorenih portova s detaljima poput vrste protokola, servisa i inačica (Slika 5.3).

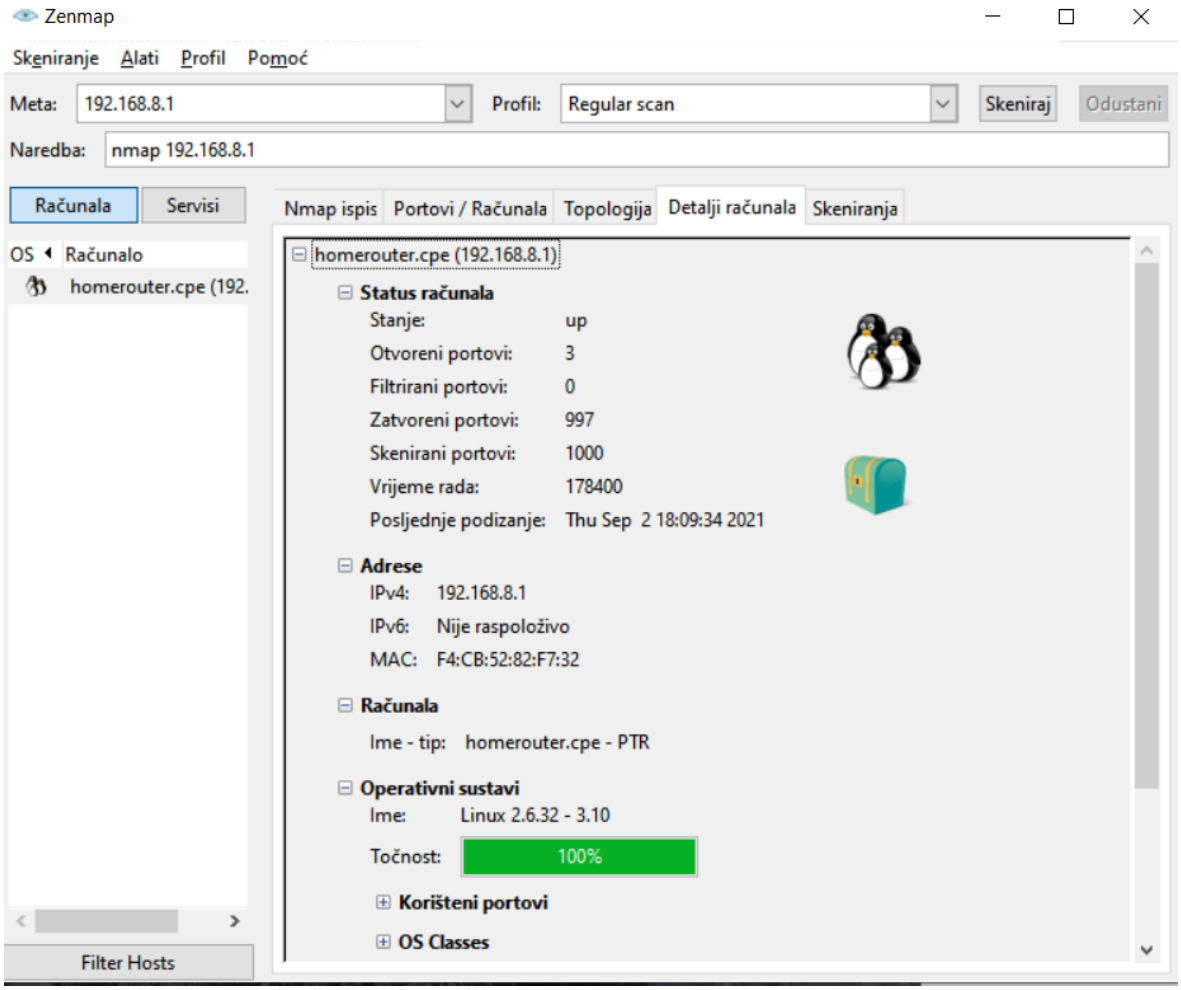


Sl. 5.3 *Kartica Portovi/Računala*



Sl. 5.4 *Grafički prikaz skena*

Kartica *Detalji računala* pruža uvid u pojedinosti računala, a to su status računala, adrese, ime i tip računala te operacijski sustavi.



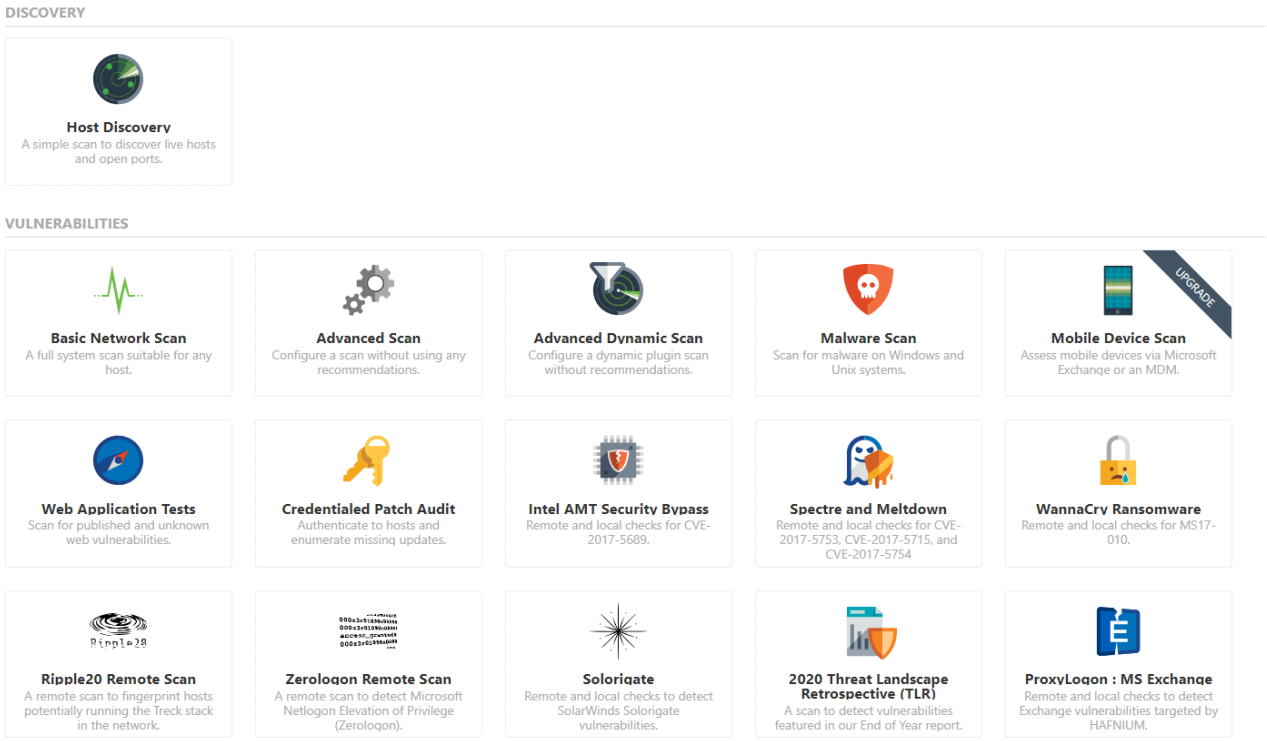
Sl. 5.5 *Detalji računala*

5.2. Nessus

Nessus je jedan od najpoznatijih besplatnih programa za skeniranje ranjivosti. Tenable Network Security je proizvodač i autor Nessusa. Nudi velik broj raznovrsnih sigurnosnih skeniranja, a pojedini dodaci se naplaćuju (Slika 5.6).

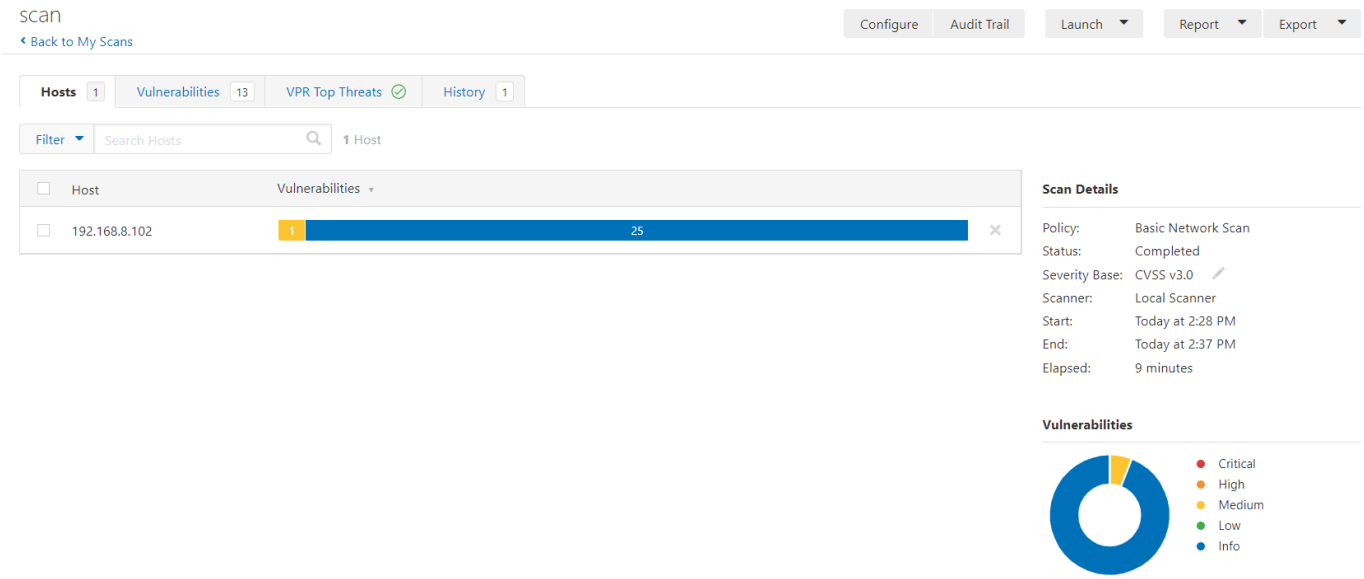
Program je definiran klijent - poslužitelj arhitekturom. Cjelokupna mrežna komunikacija između servera i klijenta je zaštićena, a pri komunikaciji upotrebljava se TLS (engl. Transport Layer Security) protokol.

Nessus klijent podešava skeniranje, dodatke, način i cilj skeniranja te u konačnici osigurava izvještaj o rezultatima skeniranja. Nessus poslužitelj realizira sva odabrana sigurnosna skeniranja. Dodaci za skeniranje napisani su u NASL (engl. Nessus Attack Scripting Language) jeziku [8].



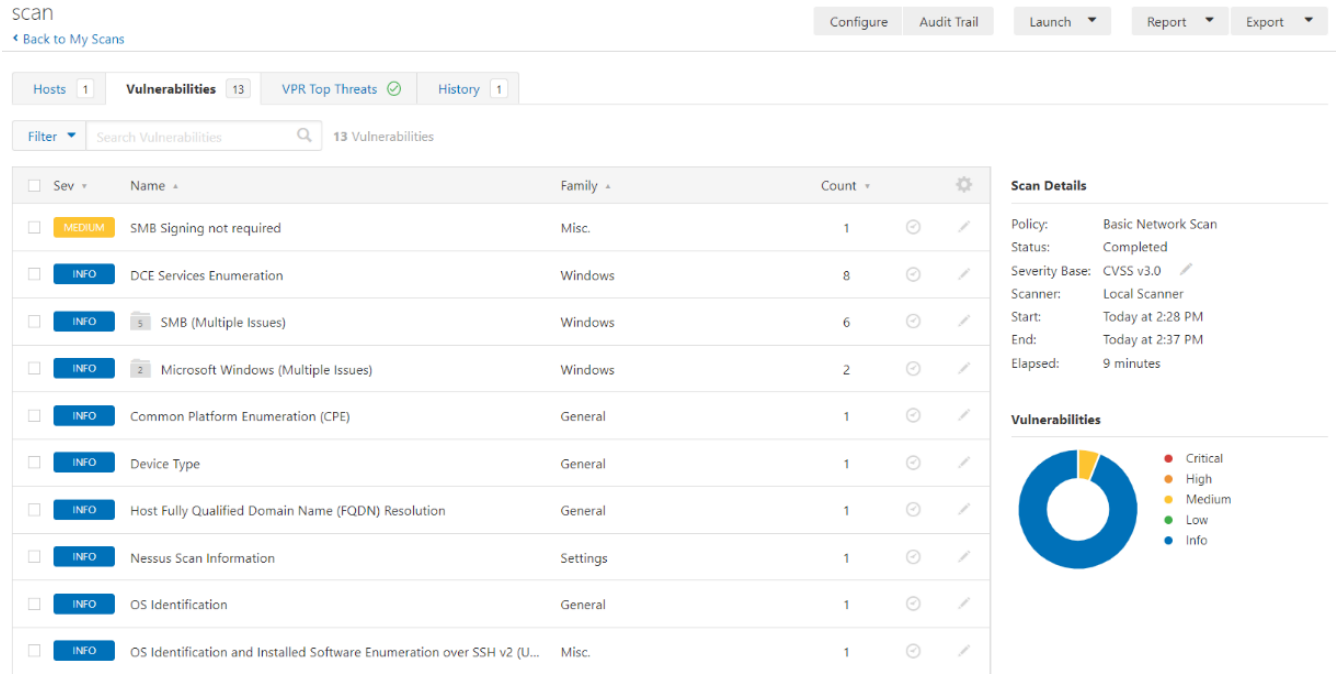
Sl. 5.6 *Vrste skeniranja*

Nakon odabira vrste skeniranja, potrebno je odrediti metu skeniranja. Kada je skeniranje završeno prikazani su rezultati broja skeniranih podataka, detalji skeniranja (status skeniranja, početak i kraj te proteklo vrijeme za odabrano skeniranje) i razina opasnosti, odnosno ranjivosti mete (Slika 5.7).

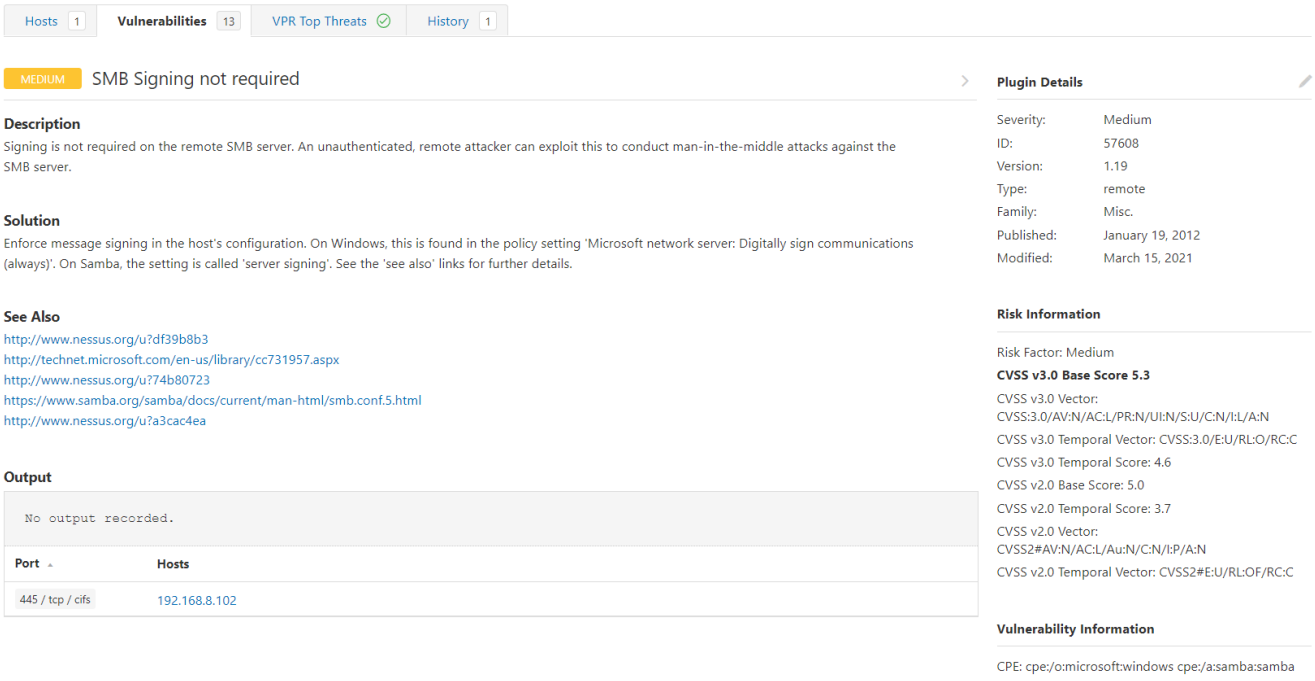


Sl. 5.7 *Rezultat skeniranja*

Kartica *Vulnerabilities* prikazuje popis svih skeniranih ranjivosti (Slika 5.8). Odabirom pojedine ranjivosti, dobiva se detaljniji uvid u situaciju; o kojem se portu radi, opis problema, prijedlog rješenja kao i korisne poveznice (Slika 5.9).



Sl. 5.8 *Popis skeniranih ranjivosti*



Sl. 5.9 *Detalji pojedine ranjivosti*

6. ZAKLJUČAK

Obzirom da su u današnje vrijeme ljudi diljem svijeta sve više međusobno povezani, računalna sigurnost postaje sve važnija tema. Računalne mreže moraju biti ispravno postavljene i održavane od strane pouzdanog administratora. Nužno je zaštititi osobne podatake, poslovne informacije, novčane transakcije i ostale vrlo važne informacije. Korisnici trebaju biti upoznati s pojmom mrežne ranjivosti, osnovnim strategijama uspostavljanja sigurnosne računalne mreže, potencijalnim ciljevima napada te zlonamjernim softverima pomoću kojih se napadač želi približiti. Plan izgradnje sigurnosne zaštite sustava olakšan je ako smo upoznati s načinima i putevima koji mogu ugroziti sustav. Crvi, virusi, trojanci, špijunski softveri, oglašivački softveri, keylogger te lažni antivirusni programi samo su neki od zlonamjernih softvera. Kako bi se zaštitili od štetnih softvera nužno je kritički sagledati i odnositi se prema svemu s čime dolazimo u kontakt na mrežnom sustavu. Postoji nekoliko važnih sigurnosnih načela kojih se treba pridržavati. Važno je izgraditi jednostavan, odnosno razumljiv sigurnosni sustav kako bi osiguravanje sustava bilo olakšano. Izgradnja takvog sustava sastoji se od držanja pokrenutih servisa i informacija podalje od zlonamjernih pojedinaca, korisnicima dopuštanja pristupanju samo odabranim podacima, zaštite svih slojeva obrane kao da su posljednji, evidencije svih pokušaja pristupanja rizičnim podacima, odvajanje sredstava u skupine i izolaciju, izbjegavanje čestih pogrešaka i ne dopuštanje da sigurnosni koraci budu preskupi. Ukoliko dođe do propusta, tj. napada nužno je znati upravljati rizikom. Nijedna mreža ne može biti posve sigurna, stoga postoje procesi za ocjenjivanje i upravljanje rizikom koje je moguće koristiti. Procesi su slijedeći: postavljanje dosega, identifikacija imovine i određivanje njene vrijednosti, modeliranje prijetnji, dokumentiranje sigurnosnih rizika, određivanje strategije upravljanja rizikom, nadzor imovine i praćenje promjena. Ako je računalo ili mreža ugrožena postoje četiri strategije upravljanja rizikom, a to su ublažavanje, prijenos, izbjegavanje i prihvaćanje. Kako do rizičnih situacija ne bi došlo nude se antivirusna zaštita, kriptiranje te IPSec protokol kao potencijalna rješenja. Dakle, anonimnost je nepraktična i gotovo nemoguća stoga je važno oprezno postupati s nepoznatim informacijama, komunicirati s poznatim i pouzdanim osobama, koristiti snažne lozinke te redovito ažurirati sustav i antivirusne programe. Skeniranje mreže i mrežne ranjivosti služi za sigurnosnu analizu i jasnije shvaćanje zaštite mreže, kao i utvrđivanje mogućih točaka eksploatacije.

LITERATURA

[1] Turk, S. Računarske mreže. Zagreb, Školska knjiga, 1991.

[2] Bača, Miroslav, Uvod u računalnu sigurnost, Zagreb; Narodne novine, 2004.

[3] T. Šoštarić: Sigurnost i zaštita računalnih mreža, završni rad, Fakultet prometnih znanosti, Zagreb, 2016.

[4] Saadat Malik: Network Security Principles and Practices. Cisco Systems, 2004

[5] V. Franković: Sigurnost računalnih mreža te pregled alata za poboljšanje sigurnosti, seminar, Fakultet elektrotehnike i računarstva, Zagreb, 2014.

[6] Steve Manzuik, Ken Pfeil, Andrew Gold: Network Security Assessment: From Vulnerability to Patch. Syngress, 2006

[7] www.nmap.org/download

[8] www.tenable.com/products/nessus

SAŽETAK

Naslov: Skeniranje mreže i mrežne ranjivosti

Završni rad podijeljen je na pet cjelina. U prvoj cjelini definirane su računalne mreže, kako upravljati računalnim mrežama i održavati ih. Druga cjelina definira što je mrežna ranjivosti, koji su ciljevi potencijalnih napada i opis zlonamjernih softvera. Treća cjelina sadrži ključne principe sigurnosti, smjernice kako uspostaviti računalnu sigurnost te prijedloge rukovanja propustima. U četvrtoj cjelini prikazani su programi za skeniranje računalne mreže i skeniranje ranjivosti. U zaključku su istaknute neke smjernice za bolje razumijevanje sigurnosti mreže i time povećanje razine zaštite sustava.

Ključne riječi: Računalne mreže, Mrežna ranjivost, Ključni principi sigurnosti, Skeniranje mreže, Skeniranje ranjivosti

ABSTRACT

Title: Network and network vulnerability scanning

The final paper is divided into five parts. In the first part, computer networks are defined, how to manage and maintain computer networks. The second unit defines what network vulnerabilities are, what the targets of potential attacks are, and the description of malware. The third section contains key security principles, guidelines on how to establish computer security, and suggestions for handling vulnerabilities. The fourth part presents programs for computer network scanning and vulnerability scanning. In conclusion, there are listed some guidelines for better understanding of network security and thus increading the level of system preotection.

Key words: Computer network, Network vulnerability, Key security principles, Network scanning, Vulnerability scanning

ŽIVOTOPIS

Ana Marek rođena je 24. rujna 1998. godine u Virovitici. Pohađala je Osnovnu školu Suhopolje. Po završetku osnovne škole, u Virovitici upisuje Gimnaziju Petra Preradovića, prirodoslovno - matematički smjer. Nakon položene državne mature 2017. godine, obrazovanje nastavlja na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku, preddiplomskog sveučilišnog studija računarstva.