Analiza programskih alata za sigurnost računalnih mreža

Miškulin, Ivan

Undergraduate thesis / Završni rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:472624

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-19**

Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Ivan Miškulin

ANALIZA PROGRAMSKIH ALATA ZA SIGURNOST RAČUNALNIH MREŽA

ZAVRŠNI RAD

Zagreb, 2016.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

ANALIZA PROGRAMSKIH ALATA ZA SIGURNOST RAČUNALNIH MREŽA

ANALYSIS OF SOFTWARE TOOLS FOR COMPUTER NETWORKS SECURITY

Mentor: doc. dr. sc. Ivan Grgurević

Student: Ivan Miškulin, 0135228486

Zagreb, kolovoz 2016.

ANALIZA PROGRAMSKIH ALATA ZA SIGURNOST RAČUNALNIH MREŽA

SAŽETAK:Upotreba računalnih mreža je sve veća te dobiva sve veći značaj. Jedan od bitnih aspekata računalnih mreža je njihova sigurnost. U radu će se obraditi značajke računalnih mreža, mehanizmi zaštite te opasnosti u računalnim mrežama. Za detekciju opasnosti u mreži se koriste programski alati: Network Mapper, Nessus i Nexpose. Iz dobivenih rezultata napravila se usporedna analiza programskih alata te se ukazalo na njihove prednosti i nedostatke.

KLJUČNE RIJEČI:Računalne mreže, sigurnost računalnih mreža, mehanizmi zaštite računalnih mreža

SUMMARY:The use of computer networks is increasing and becoming ever more important. One of most important aspects of computer networks is their safety. This paper will cover features of computer networks, security mechanisms and dangers in computer networks. Software tools: Network Mapper, Nessus and Nexpose are used for vulnerability detection. Comparative analysis is based on the results of scan and points out advantages and deficiencies of software tools.

KEYWORDS:Computer networks, computer network security, mechanisms for computer network protection

Sadržaj

1. Uvod 1
2. Značajke računalnih mreža 3
2.1 Vrste topologija računalnih mreža 3
2.1.1 Topologija sabirnice 4
2.1.2 Topologija prstena 5
2.1.3 Topologija zvijezde 6
2.1.4 Stablasta topologija 6
2.1.5 Isprepletena topologija 7
2.1.6 Kombinacija više vrsta topologija 8
2.2Računalne mreže prema veličini 9
2.2.1 Local Area Networks 9
2.2.2 Metropolitan Area Network 9
2.2.3 WAN 10
2.3 Podjela računalnih mreža prema načinu korištenja usluga 11
3. Sigurnost računalnih mreža 13
3.1 Opasnosti za računalnu mrežu 13
3.1.1 Računalni virusi i crvi 13
3.1.2 Računalni trojanski konj 14
3.1.3 Adware i spyware 15
3.1.4 Phishing 15
3.2 Mehanizmi zaštite u računalnim mrežama 15
3.2.1 Kriptografija 16
3.2.2 Digitalni potpis 18
3.2.3 Autentikacijski protokoli 18
4. Primjeri sigurnosti prema mrežnim slojevima 19
4.1 Aplikacijski, prezentacijski i sesijski sloj 19
4.2 Transportni sloj 19
4.3 Mrežni sloj 20
4.4Sloj podatkovne veze 20
5.Programski alati u funkciji sigurnosti računalnih mreža 22
5.1 Network Mapper 22

5.1.1 Grafičko sučelje Zenmap....22
5.1.2 Opcije skeniranja koristeći Network Mapper....23
5.1.3 Primjer korištenja Network Mapper-a....26
5.2 Nessus....33
5.3 Nexpose Community Edition....40
6. Usporedna analiza programskih alata Network Mapper, Nessus i Nexpose....46
6.1 Network Mapper....46
6.2 Nessus....50
6.3 Nexpose....54
6.4 Usporedba alata....57
7. Zaključak....60
Literatura....61
Popis kratica....64
Popis slika....67
Popis tablica....68

1. Uvod

Razvoj i unaprjeđenje računala i tehnologija za posljedicu ima sve veće korištenje tih uređaja i tehnologija u privatne i poslovne svrhe. Bitne informacije se prenose u digitalni oblik te je potrebno zaštiti uređaje od napada te spriječiti prisluškivanje komunikacije kako bi se zaštitili korisnici tehnologija. U ovome radu će se obraditi tema o sigurnosti računalnih mreža te primjena programskih alata za sigurnost računalnih mreža.

Motiv za istraživanje teme završnog rada je upoznavanje i funkcionalno korištenje programskih alata za potrebe analize sigurnosti računalnih mreža. Cilj završnog rada je analiza programskih alata za sigurnost računalnih mreža.

Svrha rada je predočiti različite napade na računalne mreže i upoznavanje s osnovnim mehanizmima zaštite računalnih mreža upotrebom programskih alata.Rad je podijeljen u sedam cjelina:

1. Uvod
2. Značajke računalnih mreža
3. Sigurnost računalnih mreža
4. Primjeri sigurnosti prema mrežnim slojevima
5. Programski alati u funkciji sigurnosti računalnih mreža
6. Usporedna analiza programskih alata Network Mapper, Nessus i Nexpose
7. Zaključak

Uvodno poglavlje daje osnovnu sliku o radu te definira cilj i strukturu rada.

U drugome pogavlju će se obraditi osnovne značajke računalnih mreža poput topologije, podjele računalnih mreža prema veličini i prema načinu korištenja usluga.

U trećem poglavlju će se navesti i ukratko objasniti opasnosti za računalne mreže kao što su: računalni virusi, crvi i računalni trojanski konj. U drugome dijelu

poglavlja će se obraditi mehanizmi zaštite u računalnim mrežama poput: kriptografije, upotreba digitalnog potpisa te autentikacijski protokoli.

Primjeri upotrebe mehanizama zaštite po slojevima OSI referentnog modela objasniti će se u četvrtom poglavlju.

Kroz peto poglavlje prikazati će se upotreba programskih alata od odabira vrste skeniranja, pronalaženja računala u mreži i skeniranja računala.

U šestome pogavlju će se napraviti usporedna analiza sva tri programska alata. Alati će biti upotrebljeni na jednoj meti te će se usporediti razlike, nedostaci i prednosti pojedinih alata i njegovih rezultata skeniranja.

U poglavlju Zaključak će se obraditi tema o potrebi upotrebe programskih alata i drugih mehanizama u svrsi zaštite računalnih mreža.

2. Značajke računalnih mreža

Računalne mreže su napravljene da zadovolje potrebe za bržom obradom podataka te distribucija tih istih podataka na više različitih lokacija.Računalnu mrežu čine dva ili više međusobno povezana računala. Povezuju se iz razloga dijeljenja podataka i informacija te kasnije s razvojem mreža dolazi do dijeljenja resursa poput printera, skenera i slično.

Prva računala su imala mogućnost obrade podataka,ali ne i distribuciju tih podataka. Kako bi se ubrzao postupak distribucije podataka s jednog mjesta na više lokacija uzeli su se primjeri iz tadašnjih telekomunikacija. Telekomunikacijska mreža je tada omogućavala prijenos govora te telegrafiju, ali potrebno je bilo osmisliti novu tehnologiju za prijenos podataka primjerenim za računala u obliku električnog signala na veće udaljenosti. Iz telekomunikacijskih mreža mogli preuzeti primjeri fizičkog spajanja mreže te dijeljenje resursa mreže.[1]

Kroz sljedeća potpoglavlja objasniti će se neke od najbitnijih značajki računalnih mreža.

2.1 Vrste topologija računalnih mreža

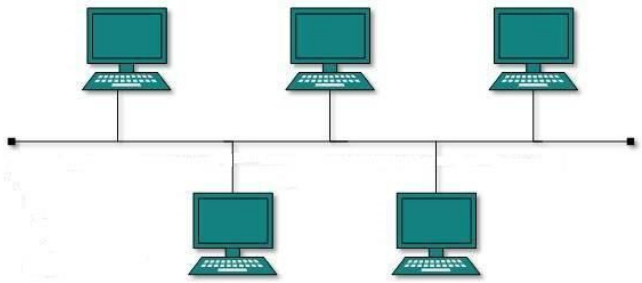
U računalnim mrežama topologija predstavlja prikaz na koji način su računala povezana u mreži. Topologija se ne odnosi na fizički raspored računala i raspored njihovih veza u stvarnosti.

Vrste topologije se dijele na:

- Topologija sabirnice,
- Topologija prstena,
- Topologija zvijezde,
- Stablasta topologija,
- Isprepletena topologija,
- Kombinacija više vrsta topologija[1]

2.1.1 Topologija sabirnice

Topologija sabirnice je vrsta mreže gdje računala koriste zajednički medij za prijenos podataka u mreži. U ovakvoj mreži nema središnjeg čvora te upravljanje mrežom može biti distribuirano. Na dijeljenom mediju dolazi do „sudara“ poruka odnosno signala te u tom slučaju računalo čeka da prođe neko slučajno odabrano vrijeme prije nego što ponovno pokuša poslati poruku. Računalo šalje podatke putem medija, na kojeg su spojena sva računala u mreži kao što je vidljivo iz primjera u slici 1. Poruka je vidljiva svim računalima na mreži, ali poruku prima i obrađuje samo odredišno računalo za određenu poruku.

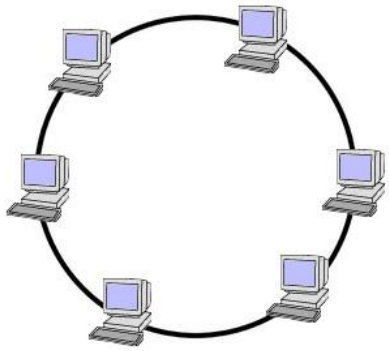


Slika 1 Shematski prikaz mreže s topologijom sabirnice [2]

Prekid rada jednog računala ne utječe na ostatak mreže, ali kvar na mediju može uzrokovati prestanak rada cijele mreže. Na oba kraja dijeljenog medija je terminator mreže. Podaci odnosno signal se šalju iz jednog čvora prema jednom kraju mreže. Odredišno računalo zaprimi i obradi podatke. Signal nastavlja dalje do kraja mreže odnosno do terminatora mreže. Terminator prima signal i uklanja ga iz mreže time oslobađajući medij za slanje novih poruka.[2]

2.1.2 Topologija prstena

U topologiji prstena svako računalo ima dva susjedna računala kao što je vidljivo na slici 2. Računala u prstenu su povezana s dva susjedna računala i tako sve dok se ne spoje u krug. Poruke se u mreži kreću u smjeru kazaljke na satu ili suprotno. Sa slanjem poruka u istom smjeru dolazi do uklanjanja vjerojatnosti kolizije poruka na kanalu. U slučaju prekida veze na jednom kanalu ili računalu moguće je slati poruke suprotnim smjerom u mreži. Time poruka mora proći kroz više čvorova u mreži čime se gubi na performansama mreže. Iz tog razloga se u mrežama s topologijom prstena koriste primarni i sekundarni prsten.



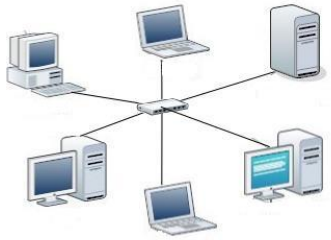
Slika 2 Prikaz topologije prstena [3]

Za slanje i primanje podataka koristi se TOKEN. TOKEN se šalje zajedno s korisnim podacima iz izvorišnog računala. Sljedeće računalo zaprimi signal te provjeravaju je li signal odnosno podaci namjenjeni njemu. U slučaju da nisu, signal se s TOKEN-om šalje dalje i postupak se ponavlja dok signal ne dođe do odredišta. Odredišno računalo primi signal te proslijedi dalje prazan TOKEN[1]. Računala s TOKEN-om jedina smiju slati podatke.[4]

[1]Primitak praznog TOKEN-a znači da čvor smije slati podatke u mrežu

2.1.3 Topologija zvijezde

Sva računala su spojena na centralni čvor preko kojega se odvija sav promet u mreži. Topologija zvijezde omogućuje jednostavno upravljanje prometom, no kvar centralnog čvora znači prekid komunikacije na cijeloj mreži.[1]

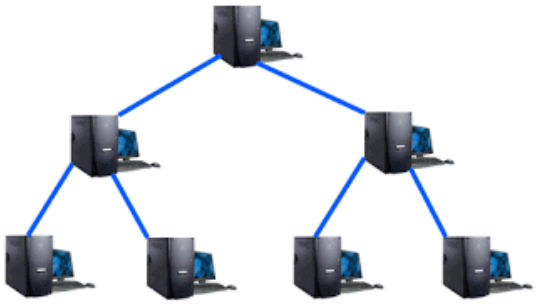


Slika 3 Prikaz topologije zvijezde [5]

Centralni čvor kroz kojega prolazi sav promet mreže može biti računalo, hub ili switch kao što je prikazano na primjeru u slici 3.[6]

2.1.4 Stablasta topologija

Stablasta topologija je nadograđena verzija topologije zvijezde. Predstavlja više mreža sa topologijom zvijezde spojene u hijerarhijsku strukturu kao što je vidljivo na slici 4.

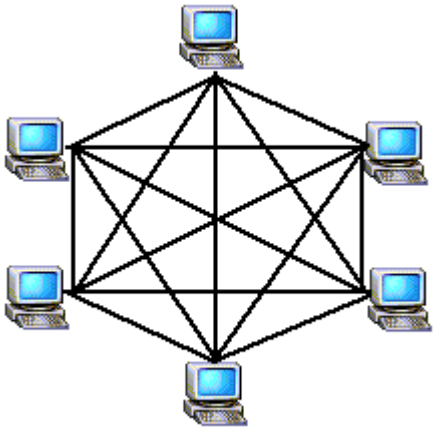


Slika 4 Prikaz stablaste topologije [7]

Računalo može komunicirati unutar vlastite podmreže odnosno mreže s topologijom zvijezde. Za komunikaciju sa računalima u drugim podmrežama koristi se čvor s više hijerarhijske razine. Kvar na računalu u podmreži ne utječe na mrežu dok kvar na centralnom čvoru neke podmreže prekida komunikaciju svih računala u toj mreži međusobno i prema ostatku mreže. Kvar na čvoru više hijerarhijske razine prekida komunikaciju između podmreža, ali ne i komunikaciju u podmreži. Iz tog razloga se čvorovi više hijerarhijske razine u većim mreža sa stablastom topologijom dodatno međusobno povezuju. Dodatno povezivanje omogućuje zamjenske kanale za slanje podataka u slučaju kvara. Na slici 4. prikazana je mreža gdje su dvije podmreže s topologijom zvijezde koje su povezane preko čvora više hijerarhijske razine.[2]

2.1.5 Isprepletena topologija

Mreža u kojoj su sva računala međusobno povezana naziva se mreža s isprepletenom topologijom. Prikaz isprepletene topologije vidljiv je u slici 5.



Slika 5 Prikaz mreže s isprepletenom topologijom [7]

Podaci mogu doći do odredišta putem više različitih puteva koji su omogućeni međusobnom povezanošću računala u mreži. Takva mreža je vrlo otporna na kvarove čvorova u mreži, ali zbog velikog broja kanala je također i najskuplja te najteža

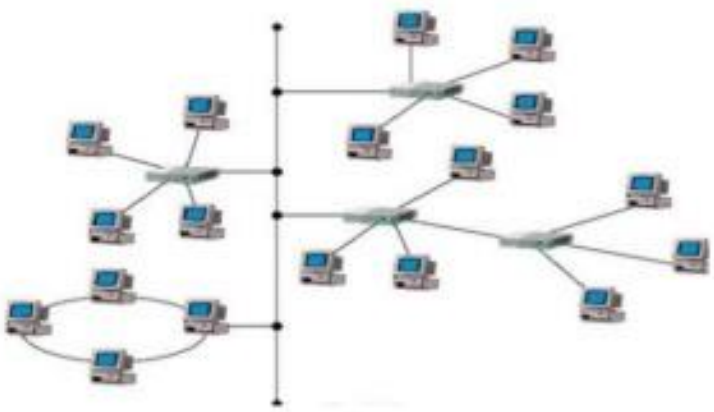
zaizgraditi te održavati.Broj veza između računala u mreži s n računala računa se po formuli:

Broj linkova = n(n+1)/2 [7]

Ukoliko se uzme da ima n računala u mreži. Svako računalo mora imati n-1 port-ova za komunikaciju što u mrežama s većim brojem računala predstavlja problem. U nastavku je opisana kombinacija više vrsta topologija.

2.1.6 Kombinacija više vrsta topologija

Kombinirana mreža sadrži više različitih topologija. Ovisno o potrebama i zahtjevima se kombinacijom prethodno navedenih topologija povezuju mreže koje onda čime kombiniranu mrežu.[1]



Slika 6 Prikaz mreže sa kombinacijom više vrsta mreže [8]

Na slici 6. prikazana je mreža koja sadrži podmreže s topologijama prstena, zvijezde i sabirnice. Različite topologije moguće je kombinirati na takav način da se

iskoriste prednosti pojedine topologije. Nedostatak ovakve mreže je kompleksnost dizajniranja mreže, visoka cijena hub-ova koji povezuju dvije mreže s različitim topologijama.[9]

2.2Računalne mreže prema veličini

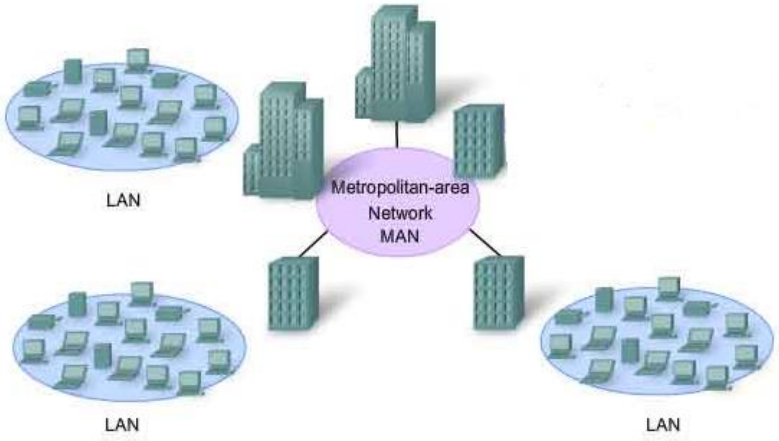
Računalne mreže mogu obuhvaćati mala područja poput jedne zgrade ili više zgrada, preko mreža koje pokrivaju područja cijeloga grada do računalnih mreža koje obuhvaćaju cijele regije te na kraju i cijeli planet. Različiti su zahtjevi ovisno o veličini mreže. Lokalne mreže odnosno LAN(engl. *Local Area Network,* LAN) zahtjevaju manja kašnjenja i veće brzine dok se kod većih MAN mreža(engl. *Metropoian Area Network*, MAN) i mreža koje pokrivaju veće regijeodnosno WAN (engl. *Wide Area Network*, WAN)dolazi do smanjenja osjetljivosti na kašnjenje te do smanjenja brzine prijenosa podataka.[1]

2.2.1 Local Area Networks

Lokalne mreže geografski pokrivaju manja područja poput zgrade ili kuće, ali unutar pokrivenog područja mogu posluživati razan broj korisnika odnosno računala. Od malog broja računala, npr. 2 ili 3 računala, pa do velikog broja računala i uređaja, npr. stotinu i više. Najčešće korištene LAN tehnologije su Ethernet i Wi-Fi (engl. *Wireless Fidelity,* Wi-Fi).[10]

2.2.2 Metropolitan Area Network

MAN-ovi su mreže koje geografski pokrivaju veće područje od lokalnih mreža te pritom zadržavaju neke od karakteristika lokalnih mreža. Jednu MAN mrežu čini više povezanih lokalnih mreža koje se povezuju optičkim kablovima.[11]



Slika 7Prikaz odnosa MAN i LAN mreža [12]

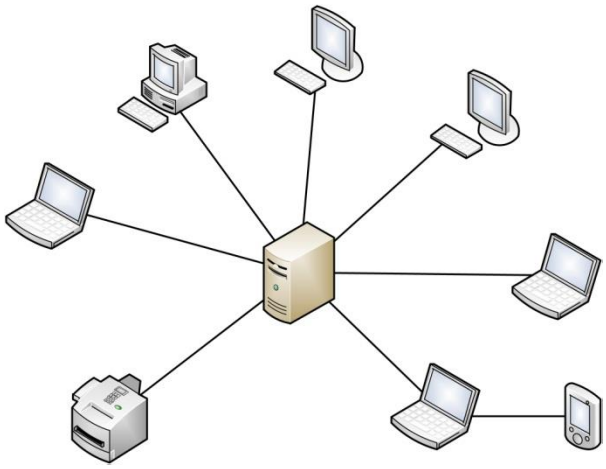
U slici 7. je prikazan primjer gdje lokalne mreže pokrivaju područje jedne zgrade. Lokalne mreže su međusobno udaljene i nalaze se na različitim lokacijama u gradu. Lokalne mreže se međusobno povezuju te tvore jednu MAN mrežu. MAN mreža na taj način obuhvaća znatno veće geografsko područje koje je u ovom slučaju područje grada.[1]

2.2.3 WAN

WAN mreža obuhvaća velika područja od države do cijelog kontinenta. Unutar obuhvaćenog područja prima podatke od više različitih mreža te ih šalje prema odredištu. Podaci dolaze u mrežu putem različitih kanala, koristeći različite protokole te na kraju i različitim brzinama. Primarna svrha WAN mreža je povezivanje korisnika odnosno njihovih računala i uređaja koji su spojeni na lokalnu mrežu.[11]

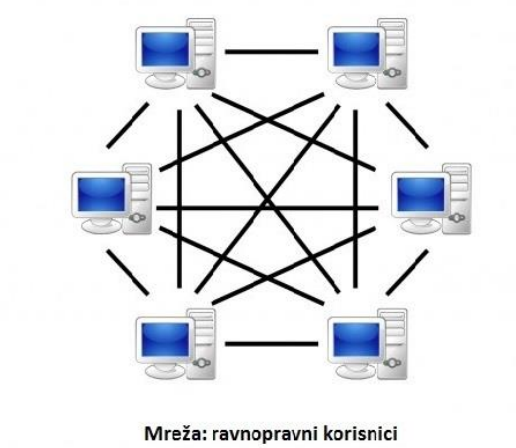
2.3 Podjela računalnih mreža prema načinu korištenja usluga

Elementi u računalnim mrežama mogu biti u ravnopravnom odnosu ili arhitektura mreže može biti slojevita. Mreže u kojoj su računala u ravnopravnom odnosu naziva se P2P (engl. *Peer-to-Peer,* P2P) mreža. Slojevita arhitektura odnosi se na mreže gdje imamo poslužitelje i korisnike u mreži.



Slika 8 Primjer mreže s poslužiteljem i korisnicima [13]

Na slici 8. prikazan je primjer mreže sa poslužiteljem u središtu te korisnicima koji su spojeni na poslužitelja. Poslužitelj je vrsta računala koja obrađuje zahtjeve korisnika te im pruža određenu uslugu. Karakteristike poslužitelja su velika memorija te brzo posluživanje većeg broja korisnika istovremeno.[13]



Slika 9 Primjer mreže s ravnopravnim korisnicima [14]

Mreža ravnopravnih korisnika sadrži računala koja imaju jednake ovlasti, mogućnosti i zadatke kao što je prikazano na slici 9. Svi korisnici međusobno komuniciraju te dijele resurse, što svako računalo čini poslužiteljem i korisnikom. Ovakva vrsta mreže je jednostavnija i glavna karakteristika mreže je decentralizacija.[15]

3. Sigurnost računalnih mreža

Sigurnost računalnih mreža odnosi se na sprječavanje svih štetnih aktivnosti u mreži. To se odnosi na aktivnosti poput: zaštite korištenja resursa mreže, pouzdanost mreže, te održavanje integriteta i zaštita podataka koji su pohranjeni i koji se šalju preko mreže. Različiti sigurnosni alati sprečavaju opasnosti da uđu u mrežu te se njome prošire.

3.1 Opasnosti za računalnu mrežu

Maliciozni programi su napravljeni tako da iskoriste određene slabosti s ciljem zaražavanja jednog računala u mreži.Zaraženo računalo služi kao izvor za daljnje širenje štetnog programa mrežom. Štetni programi se razlikuju ovisno o svrsi za koju su kreirani. Dio štetnih programa uništava softver računala pa tako i cijelo računalo. Određeni maliciozni programi su napravljeni za špijunažu te krađu podataka s računala.[16]

3.1.1 Računalni virusi i crvi

Računalni virusi su programi napravljeni da se šire po mreži od računala do računala te modificiraju ili uništavaju podatke na napadnutom računalu. Virusi se često šire kao dodaci putem elektroničke pošte ili instant poruka. Moguće ih je sakriti u slike, audio i video zapise. Računala se također često zaraze virusom putem preuzimanja datoteka s Interneta. Viruse je moguće sakriti unutar nekog softvera ili programa te se nakon preuzimanja uz softver pokreće i virus.

Računalni virusi mogu se podijeliti u grupe:

- File viruses
- Boot sector viruses
- Macro viruses
- Script viruses[17]

File viruses su vrsta virusa koji napadaju kodove računala, modificiraju kod tako da se kod virusa uvijek izvrši prije izvršavanja koda napadnutog računala odnosno njegovog programa. Ovo omogućuje da će se uvijek pokrenuti kod virusa prilikom pokretanja koda zaražene datoteke. Također zaražena datoteka predstavlja sredstvo širenja virusa na druga računala. [18]

Računalni crv je vrsta programa koja penetrira operativni sustav s ciljem širenja malicioznog programa. Na zaraženom računalu mogu brisati datoteke te slati dokumente putem elektroničke pošte. Moguće je da crv ima mogućnost da napravi *backdoor*[2] na računalu. Razlika između računalnog virusa i crva je u njihovom širenju mrežom. Računalni crvi šalju kopije malicioznog programa koristeći slabosti automatski, bez ljudskoga vođenja.[19]

3.1.2 Računalni trojanski konj

Računalni trojanski konj je maliciozna vrsta softvera koja je često zamaskirana u legitimni softver. Trojanskog konja koriste hakeri kako bi dobili pristup korisničkome računalu. Trojanski konj svojom aktivacijom na računalu daje pristup hakeru da špijunira aktivnosti korisnika te ukrade, modificira ili briše podatke. Za razliku od računalnih virusa i crva, trojanski konj se ne replicira i širi iz zaraženog računala.[20]

[2]Backdoor je metoda prisutupa računalu zaobilaženjem sigurnosnih mehanizama te predstavlja opasnost

3.1.3 Adware i spyware

Adware je odnosi na softver koji prikazuje neželjene reklame u softveru koji se koristi. *Adware* često dolazi u paketu sa softverom kojeg korisnik kupuje. *Adware* može biti napravljen kako bi prikupljao podatke o internetskim stranicama koje korisnik posjećuje. Podaci o stranicama koje su posjećene *adware* šalje kompaniji koja onda po tim informacijama prilagođava reklame koje se prikazuju.

Adware može sadržavati ili biti klasificiran kao *spyware*. *Spyware* je vrsta malicioznog softvera koji zadire u privatnost korisnika. *Spyware* može ukrasti korisničke informacije ili koruptirati korisničke sistemske datoteke. Postoje police o privatnosti kojih se moraju pridržavati kompanije koje kreiraju *Adware*, no korisnik ne može biti upotpunosti siguran da je njegova privatnost održana. Iz toga razloga današnji antivirusni softveri otkrivaju i uklanjaju i *adware* i *spyware*.[21]

3.1.4 Phishing

Phishing je vrsta napada čiji je cilj saznati korisničke podatke te ih upotrijebiti kako bi se na kraju došlo do novca korisnika. Na korisničko računalo može doći elektronička pošta koja korisniku može izgledati legitimno. Takve poruke su lažne i napadači se najčešće predstavljaju predstavnicima neke tvrtke. U poruci traže korisničke podatke kako bi napravili neku uslugu u ime tvrtke. Također može tražiti da korisnik na računalo instalira softver. Takav softver je maliciozan i služi za krađu podataka s korisnikovog računala.[22]

3.2 Mehanizmi zaštite u računalnim mrežama

Uloga mehanizama za zaštitu je da omoguće korisniku sigurnu komunikaciju preko mreže. Komunikacija treba biti zaštićena od prisluškivanja. Također treba se autenticirati korisnik odnosno računalo s kojim se komunicira. Potrebno je ustvrditi integritet poruka koje se izmjenjuju u komunikaciji odnosno da poruke nisu

nedozvoljeno promijenjene tijekom slanja kroz mrežu. Mehanizmi zaštite nisu samostalno dovoljni da osiguraju sigurnu komunikaciju. Iz toga razloga upotrebljavaju se zajedno kako bi se međusobno nadopunili i uklonili postojeće nedostatke. Mehanizmi za zaštitu se kombiniraju ovisno o zahtjevima aplikacije.[23]

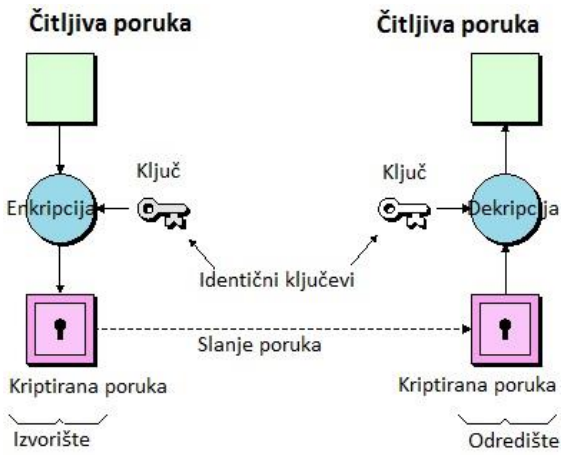
3.2.1 Kriptografija

Kriptografija predstavlja glavno sredstvo zaštite podataka u računalnim mrežama. Sadrži više dijelova koji samostalno nisu rješenja za zaštitu podataka odnosno komunikacije u računalnim mrežama. Zajedno ti dijelovi čine trenutno najbolje rješenje za zaštitu podataka u računalnim mrežema.

Poruke koji se kriptiraju nazivaju se *plaintext*[3]. Na tim porukama vrši se šifriranje odnosno enkripcija. Mogućnost dešifriranja odnosno dekripcije dostupna je samo odredišnom korisniku koji ima ključ za dešifriranje poruke. Enkripcija poruke dijeli se na enkripciju privatnim ključem i javnim ključem. Enkripcija privatnim ključem se naziva još i simetrična enkripcija jer izvorište i odredište koriste isti ključ za enkripciju i dekripciju podataka. Problem kod ovakve vrste enkripcije je distribucija ključa pošto se on koristi i za enkripciju i dekripciju. U ovome slučaju potrebno je prilikom distribucije ključa osigurati da ključ primi samo odredište.[24]

Za sigurnu komunikaciju koristeći simetričnu enkripciju potrebno je prethodno razmjeniti ključeve preko sigurne mreže ili koristeći druge metode za sigurnu razmjenu ključeva preko nesigurne mreže. Pojednostavljen primjer komunikacije koristeći simetričnu enkripciju prikazan je na slici 10.

[3]Plaintextpredstavljakorisničkepodatkekoji čitljiviodnosnopodatkekojinisukriptirani



Slika 10 Prikaz komunikacije koristeći simetrični ključ [25]

Asimetrična kriptografija se zasniva na privatnom i javnom kriptografskom ključu. Jedan od korisnika u komunikaciji ima i privatni i javni ključ. Javni ključ tog korisnika je javno objavljen. Korisnik koji želi s njime komunicirati uzima njegov javni ključ te koristeći njega šifrira tekst. Odredišni korisnik prima šifrirani tekst te preko pripadajućeg privatnog ključa dešifrira poruku. Prednost ovakvog načina je što nema distribucije ključeva. Svi ključevi se nalaze kod odredišnog računala s kojime se želi uspostaviti sigurna komunikacija. Dekripcija u ovoj vrsti enkripcije je moguća samo putem pripadajućeg privatnog ključa. Sama enkripcija koristeći javni ključ nije dovoljna za sigurnu komunikaciju jer ne može razlikovati ako se neki korisnik lažno predstavlja. Postoji više mogućnosti za rješenje toga problema kao što su: metoda tajnog sesijskog ključa ili digitalni potpis. Asimetrična enkripcija je sporija od simetrične te zahtijeva više procesne snage za enkripciju i dekripciju poruka.

Ekripcija simetričnim ključevima koristi se u većini slučajeva kriptiranja podataka dok se asimetrični ključevi koriste za autentikaciju i uspostavu tajnoga sesijskog ključa.[26]

3.2.2 Digitalni potpis

Digitalni potpis je matematička metoda kojom se potvrđuje autentičnost i integritet poruke, softvera ili digitalnog dokumenta. Digitalni potpis koristi asimetričnu kriptografiju i funkcije sažimanja. Korisnik priprema poruku za slanje tako što prvo napravi sažetak poruke kako bi se dobila *hash*[4] vrijednost. Nakon toga se dobivena *hash* vrijednost kriptira privatnim ključem izvorišnog korisnika i time se dobije digitalni potpis. Duljina *hash* vrijednosti može biti fiksirana na određenu duljinu, čime se štedi vrijeme jer se uzima duljina znatno manja od duljine poruke.

Na odredištu se prima poruka s digitalnim potpisom. Valja napomenuti kako poruka može biti kriptirana javnim ključem odredišta ili simetričnim ključem. Na odredištu digitalni potpis se dešifrira te se izračunava*hash* vrijednost. *Hash* vrijednost koja se uspoređuje sa *hash* vrijednosti dobivenom dešifriranjem digitalnog potpisa. Ukoliko su te dvije vrijednosti jednake može se zaključiti da je izvorište poruke autenticirano. Također se može zaključiti da na poruci nisu napravljene nikakve modifikacije jer bi one uzrokovale drukčiju vrijednost *hash* vrijednosti.[25]

3.2.3 Autentikacijski protokoli

Autentikacija predstavlja proces prilikom kojega se potvrđuje da je korisnik odnosno računalo s kojim se komunicira onaj pod kojim se predstavlja. Nakon autentikacije se može obaviti autorizacija te sama komunikacija u kojoj se onda koristi simetrična enkripcija. Asimetrična enkripcija se često koristi za autentikaciju te uspostavu sesijskog ključa. Slučajno generirani sesijski ključevi služe za smanjenje podataka koji se šalju koristeći privatni i javni ključ. Moguća šteta je značajno manja ukoliko sesijski ključ dospije u krive ruke jer se sesijski ključevi koriste samo za pojedinačnu sesiju i moguće ih je periodički mijenjati za vrijeme trajanja sesije.[11]

[4]Hashvrijednostjevrijednostdobivenasažimanjemporuke, nijemogućenapravitireverznufunkcijuteizhashvrijednostidobitiizvornuporuku

4. Primjeri sigurnosti prema mrežnim slojevima

Različiti mehanizmi zaštite koriste seovisno o mrežnom sloju OSI referentnog modela.Aplikacijski, prezentacijski i sesijski sloj su spojeni jer se odnose na mehanizme zaštite vezane koji su vezani za aplikaciju. Slojevi vezani za slanje podataka preko mreže su objašnjeni pojedinačno zbog njihovih razlika u primjeni unutar mreže.

4.1 Aplikacijski, prezentacijski i sesijski sloj

Mjere zaštite na aplikacijskom sloju su specifične za svaku aplikaciju. Protokol na aplikacijskom sloju koji bi koristio kriptografiju je vrlo teško za dizajnirati. Implementacija takvog protokola je također vrlo teška.[27]

Prezentacijski sloj obavlja zadatke poput: kompresije i dekompresije te enkripcije i dekripcije. Enkripcija podataka predstavlja jedinu metodu zaštite na ovome sloju.[28]

Ova dva sloja zajedno sa sesijskim slojem čine više slojeve OSI referentnog modela koji se bave problematikom aplikacija za razliku od nižih slojeva koji se bave problematikom slanja informacija preko mreže. Vatrozidi na aplikacijskom sloju imaju mogućnosti analizirati i blokirati maliciozne pakete, ali to ih čini skupljima te analizom prometa vatrozidi usporavaju komunikaciju.[29]

4.2 Transportni sloj

Protokoli na transportnom sloju mogu pomoći kod problema slanja podataka preko nesigurne mreže. Primjer nesigurne mreže je mreža kojoj svi mogu pristupiti te iskoristiti slabosti te mreže kako bi prisluškivali komunikaciju. Dva bitna protokola na ovoj razini za sigurnu komunikaciju su TLS (engl. *Transport Layer Security,* TLS) i SSL[5] (engl. *Secure Sockets Layer,* SSL). Oni omogućuju autentikaciju servera ili korisnika te korištenje ekripcije podataka nakon što je obavljena autetikacija. TLS i SSL omogućuju sigurnu HTTP (engl. *Hypertext Transfer Protocol,* HTTP) komunikaciju odnosno HTTPS(engl. *Hypertext Transfer Protocol Secure,* HTTPS) za elektroničke transkacije

[5]TLSiSSLsuprotokolikojiomogućujusigurnukomunikacijuizmeđuklijentaiposlužiteljaprekonesigurnemreže

između internetskih pretraživača i poslužitelja. Protokoli pružaju autentikaciju klijenta i servera, ekripciju podataka i integritet podataka preko nesigurnih mreža kao što su World Wide Web.

Nedostaci ovih protokola su povećanje opterećenja procesora i povećanje administracije. Povećanje opterećenja procesora dolazi od upotrebe kriptografije odnosno upotrebe javnih ključeva. Opterećenje varira i ovisi o učestalosti uspostavljanja konekcije i trajanju konekcija. Najveće opterećenje procesora je tijekom uspostave konekcije. Upotreba TLS i SSL protokola zahtijeva održavanje sustava. Administrator sustava mora konfigurirati sustav i upravljati certifikatima.[30]

4.3 Mrežni sloj

Mjere zaštite na ovome sloju primjenjive su za sve aplikacije. Sve mrežne komunikacije između dva računala ili dvije mreže moguće je zaštiti na ovome sloju bez potrebe za modifikacijom aplikacije.

IPsec[6] (engl. *Internet Protocol Security,* IPsec)koristi kriptografsku zaštitu za komunikacije u mrežama sa IP protokolom. IPsec podržava autentikaciju na mrežnome sloju, autentikaciju izvora podataka, integritet podataka i povjerljivost podataka.[31]

4.4Sloj podatkovne veze

Osnovni mehanizam zaštite u sloju podatkovne veze je filtriranje bazirano na MAC adresi (engl. *Media Access Control*, MAC) računala koje pokušava uspostaviti komunikaciju. Filtriranje bazirano na MAC adresama je moguće postaviti tako da se odredi početak i kraj MAC adresa kojima se ne dopušta uspostava komunikacije. Unutar sloja postoje dvije vrste autentikacije. Autentikacije otvorenog sistema i autentikacija

[6]IPsec koristi autentikaciju te kriptira sve IP pakete u komunikaciji

dijeljenog ključa. Autentikacija otvorenog sistema je manje sigurna te filtrira ovisno o identifikaciji računala. Autentikacija dijeljenog ključa koristi WEP (engl. *Wired Equivalent Privacy,* WEP) gdje se ključ distribuira svim računalim koja su autorizira za korištenje mreže. Također se unutar sloja podatkovne veze koristi enkripcija podataka.[32]

5.Programski alati u funkciji sigurnosti računalnih mreža

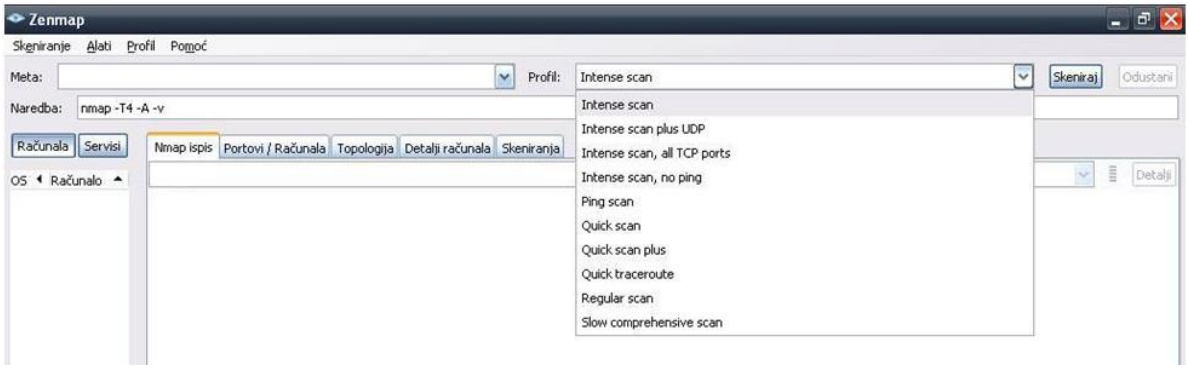
Funkcija programskih alata koji će biti upotrebljeni je detekcija slabosti unutar računalnih mreže. Detekcija slabosti predstavlja prvi korak u životnom ciklusu zaštite mreže. Kroz poglavlje objasniti će se priprema skeniranja, upotreba skeniranja te interpretacija dobivenih rezultata. Uklanjanje slabosti i održavanje sigurnosti mreže neće biti obrađeno u radu.

5.1 Network Mapper

Network Mapper je programski alat za otkrivanje čvorova u mreži te provjeru sigurnosti mreže te pojedinih dijelova mreže. Prvotno je napravljen za vrlo brzo skeniranje mreža s velikim brojem čvorova, ali je i iznimno koristan za otkrivanje podataka samo jednog čvora. Koristi IP pakete kako bi otkrio čvorove u mreži, usluge koje čvor pruža, operativne sustave koji se koriste, kakvi se vatrozidi koriste i njihova pravila i mnoge druge mogućnosti.[33]

5.1.1 Grafičko sučelje Zenmap

Grafičko sučelje Zenmap je napravljeno kako bi olakšalo upotrebu Network Mapper-a za početnike te za korištenje naprednih mogućnosti za iskusne korisnike. Vrste skeniranja koja se često koriste se mogu spremiti kao Profil kako bi im se lakše pristupalo. Polje s naredbama omogućuje jednostavno dodavanje ili uklanjanje naredbi. Rezultati spremljenih skeniranja moguće je međusobno usporediti kako bi se lakše istaknule razlike.[33]



Slika 11 Početno sučelje Network Mapper-a

Na slici 11. vidljivo prazno početno sučelje Zenmap. U područje Meta upisujemo IP adrese ili DNS adrese koje želimo skenirati. U području Profil moguće je odabrati kakvu vrstu profila skeniranja želimo napraviti. U području Naredba moguće je dodati ili ukloniti naredbe. Rezultati skeniranja se pojavljuju u prozorima ispod: Nmap ispis, Portovi/Računala, Topologija, Detalji računala i Skeniranja.[34]

5.1.2 Opcije skeniranja koristeći Network Mapper

Opcije predstavljaju naredbe koje se dodaju pri skeniranju kako bi se pokušalo doći do određenih informacija o čvoru. Naredbe se mogu podijeliti na naredbe za:

- Odabir meta za skeniranje,
- Pronalaženje čvorova u mreži,
- Tehnike skeniranja,
- Specifikacije port-ova i poredak skeniranja,
- Detekciju usluge i verzije,
- Skeniranja uz pomoć skripti,
- Detekciju operativnog sustava,
- Vrijeme odnosno brzinu skeniranja,
- Obilaženje i „*spoofing*“ vatrozida i *Intrusion Detection System-a*,
- Prikaz rezultata,
- Ostale razne naredbe[35]

Odabir mete za skeniranje može se obaviti na više načina. Upisom DNS-a (engl. *Domain Name System,* DNS) ili IP adrese, više IP adresa, spektar IP adresa, uvozom popisa meta iz vanjskih izvor. Upis DNS-a, IP adrese ili više adresa je vrlo jednostavan odabir meta za skeniranje dok su ostali kompliciraniji.

Spektar IP adresa je moguće upisati na više načina te jedan od najčešćih načina za unos je oblika: 192.168.1.0-255. Vrlo jednostavnim upisom odabrano je 256 IP adresa za skeniranje. Također je moguće napisati 192.168.0-255.0-255. čime se znatno povećao broj IP adresa za skeniranje. Valja napomenuti da su ovo samo primjeri i treba obratiti pozornost na broj meta koji je odabran za skeniranje zbog vremena koje je potrebno da se skeniranje izvrši. Također je potrebno obratiti pozornost na zakone jer nije dopušteno skenirati mreže i IP adrese za koje nije izdano dopuštenje.

Pronalaženje aktivnih čvorova na mreži moguće je izvršiti na više načina. Naredbom –sn koristi se Ping i onesposobljava se skeniranje port-ova što značajno ubrzava proces skeniranja, ali takva vrsta skeniranja daje vrlo malo rezultata zbog postavaka vatrozida koji odbacuju takve pakete te je zbog toga Network Mapper u nemogućnosti zaključiti stanje čvora. Naredba –Pn tretira sve čvorove kao „online“ i ona se koristi ukoliko je mišljenje da vatrozid sprječava odgovore čvora i time Network Mapper zaključuje da je čvor „offline“. Naredbe –PS, -PA, -PU i –PY koriste se za skeniranje port-ova tako da pokušavaju uspostaviti komunikaciju sa računalom koristeći TCP (engl. *Transfer Control Protocol,* TCP) SYN poruke, TCP ACK poruke te UDP (engl. *User Datagram Protocol,* UDP) i SCTP (engl. *Stream Control Transmission Protocol,* SCTP) poruke. Valja napomenuti da se uspostava komunikacije nikada ne izvrši do kraja kako bi računalo koje skenira mrežu ostalo sakriveno.[35]

Tehnike skeniranje variraju slično kao i pronalaženje čvorova. Razne naredbe koriste jedne od tehnika skeniranja koristeći: TCP SYN poruke, TCP ACK poruke, TCP prozore, TCP Null, TCP FIN poruke, TCP zastavice, UDP skeniranje, „Idle scan“, FTP „*bounce scan*“ i razne druge tehnike. Network Mapper za rezultate tehnike skeniranja u obzir uzima i vrstu poruke koja se šalje u tehnici skeniranja te odgovore skeniranog računala te i sam izostanak odgovora. Uspoređuju se odgovori računala sa standardima

u koja se uzimaju u obzir i sigornosne postavke kada računalo odnosno vatrozid filtrira dolaze poruke te time izostane odgovor računala.

Odabir portova za skeniranje može se izvršiti odabirom početka i kraja broja port-ova kao u naredbi –p1-65535 u kojoj se skeniraju svi portovi, počevši od jedan i završivši sa port-om 65535. Za brže i određenije skeniranje moguće je upisati broj port-ova kod kojih je najveća vjerojatnost da postoji usluga koja „sluša“ na tom port-u. Primjer takvoga odabira je naredba –p22,80,443 kojom se zadaje da skeniraju samo portovi 22, 80 i 443. Vatrozid i IDS-i vrlo vjerojatno će uočiti ukoliko se skenira veći broj port-ova na računalu te se koristi inkrementalni poredak. Zbog toga razloga se koristi slučajan odabir redoslijeda port-ova za skeniranje.

Detekcija usluge i verzije se može konfigurirati tako da se detekcija izvrši samo na otvorenim port-ovima, na port-ovima na kojim je najveća vjerojatnost za dobivanje informacija i na svim port-ovima.

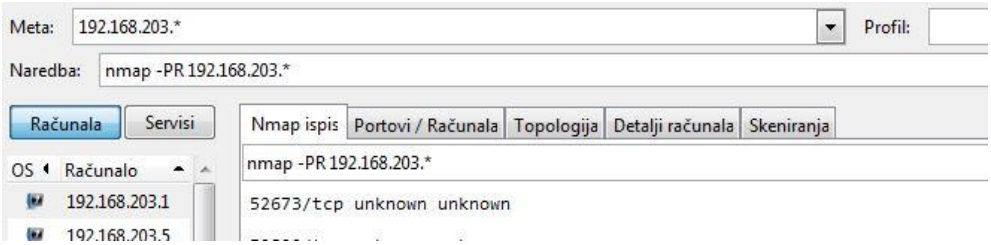
Detekcija operativnog sustava je slično postavljena. Postoje tri opcije: uključivanje detekcije operativnog sustava, ograničavanje na mete sa najvećom vjerojatnošću davanja informacija i agresivno prikupljanje podataka te davanje vjerojatnosti koji se operativni sustav koristi. Proces detekcije operativnog sustava prikuplja podatke iz otvorenih i zatvorenih port-ova. U slučaju ne postojanja jedne vrste port-a prelazi se na davanje vjerojatnosti najizglednijim vrstama operativnog sustava.[35]

Obilaženje vatrozida i IDS-a je vrlo bitno za testiranje sigurnosti. Raznim naredbama pokušava se prevariti vatrozid kako ne bi uočio skeniranje ili zabranio uslugama da putem port-ova daju informacije. Naredba –D zamaskirava skeniranje lažnim paketima, -S <IP adresa> pokušava doći do izvorišne adrese određenih podataka. Druge naredbe koriste lažne korisne podatke kako bi dobili odgovor u kojemu se nalaze razni podaci.

Zadnju grupu čine naredbe koje utječu na prikaz rezultata, format rezultat i ostale mogućnosti poput izlistavanja rezultat ili spremanja na internetsku stranicu te praćenja pogrešaka i slično.[35]

5.1.3 Primjer korištenja Network Mapper-a

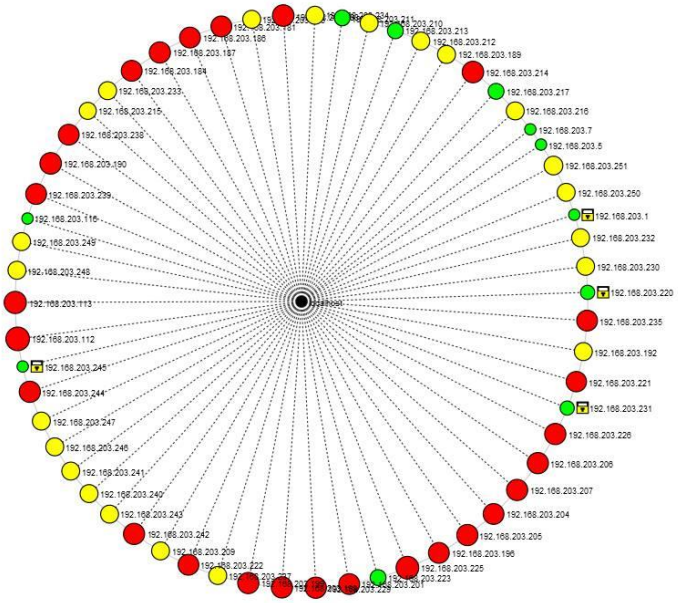
Prvi korak je pronalaženje svih meta u lokalnoj mreži koja su u tom trenutku spojena na mrežu. Za spektar IP adresa se odabralo područje u kojemu je *localhost.* Koristi se naredba –PR na mete 192.168.203.* što znači da su se skenirale sve IP adrese od 192.168.203.0 do 192. 168.203.255. Primjer korištenja ovih naredbi prikazan je na slici 12.



Slika 12 Unos naredbe za otkrivanje čvorova u mreži

Naredbom –PR se uključuje ARP (engl. *Address Resolution Protocol,* ARP) skeniranje kojime se omogućuje Network Mapper-u i njegovim algoritmima da upravlja ARP zahtjevima. Network Mapper šalje IP pakete poput ICMP (engl. *InternetControlMessageProtocol*, ICMP) echo request, te meta ukoliko je *online*, odgovara tražeći dodatne podatke kako bi mogla ispravno popuniti Ethernet paket. Sam odgovor odnosno zahtjev znači da je meta *online.*[36]

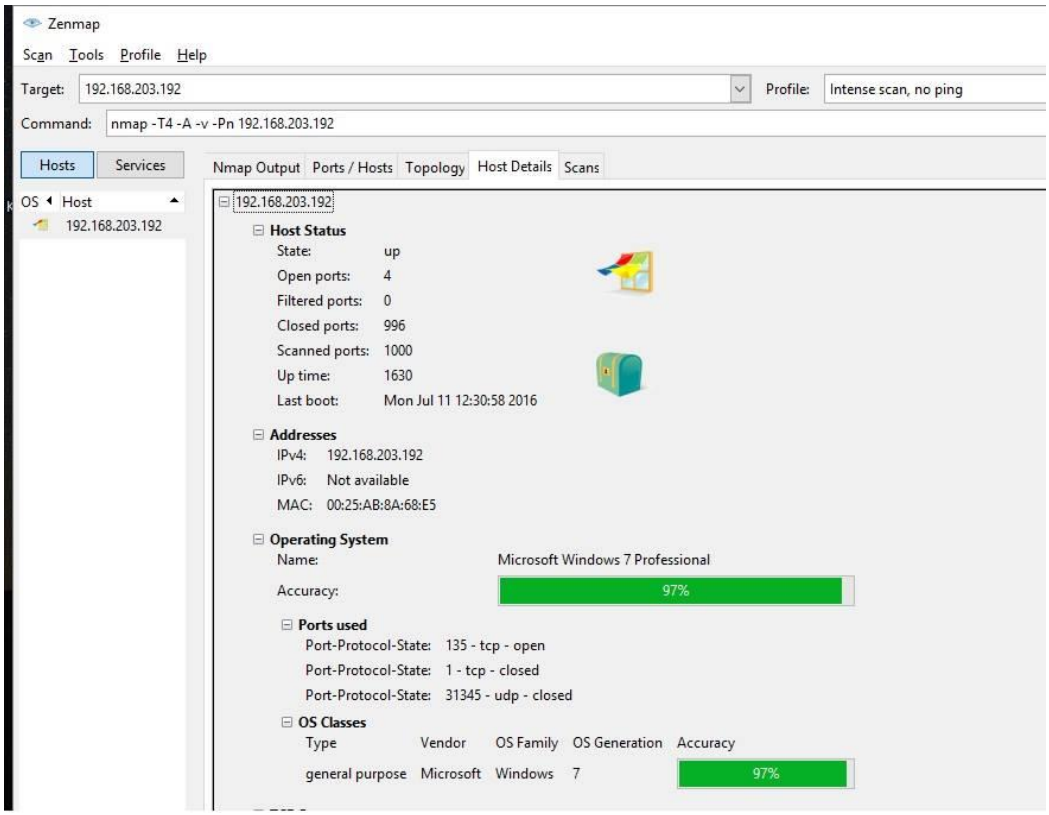
U spektru od 256 IP adresa otkriveno je 60 čvorova koji su u tome trenutku *online*.



Slika 13 Prikaz topologije

Nakon skeniranja u prozoru Topologija se prikazuje slika 13. Vidljivo je da su svi čvorovi udaljeni za jedan *skok* od *localhost-a*. Zelenom bojom označeni su čvorovi na kojima je manje od tri otvorena port-a. Ukoliko je broj otvorenih port-ova između tri i šest onda se koristi žuta boja, dok se za sve čvorove sa više od šest otvorenih port-ova koristi crvena boja za označavanje. Također što je veći broj otvorenih port-ova veći je i krug koji označava čvor.[37]

Sljedeći korak je odabir jedne od dobivenih IP adresa te korištenje profila skeniranja *Intense scan, no ping* kako bi se dobilo više podataka o meti.



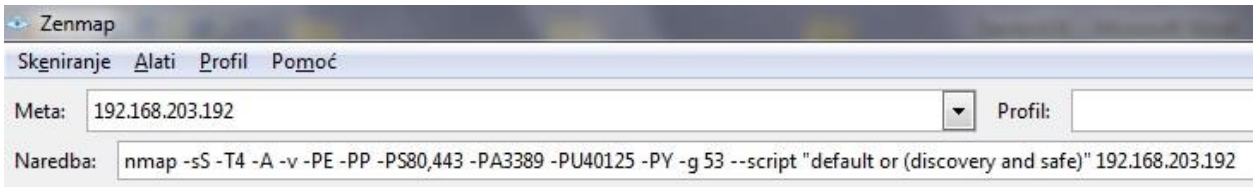
Slika 14 Detalji računala

Koristi se *Intense scan*, no ping jer je prethodnim skeniranjem utvrđeno da je čvor *online*. Jedan od najbitnijih detalja je operativni sustav jer je cilj pronaći osobno računalo na mreži te na njemu upotrijebiti *Slow comprehensive scan* jer unutar otkrivenih čvorova ima usmjerivača, poslužitelja i osobnih računala. Vidljivo je na slici 14. da se unutar profila *Intense scan,no ping* nalazi naredba –A. Naredbom se Network Mapper-u omogućuje detekcija operativnog sustava, usluga i verzija na meti. Također određuje put do mete i pokreće dodatne skripte kako bi saznali više informacija. Naredba –v zadaje da se u rezultatima Network Mapper-ovog skeniranja prikažu detaljnije podaci koji su dobiveni i na koji način se došlo do tih podatka.

Detekcija operativnog sustava se vrši preko otvorenih i zatvorenih port-ova na računalu. Na port-ove se šalju različiti paketi te se prate odgovori računala na te pakete. Odgovori se uspoređuju sa različitim RFC (engl. *Request For Comment*, RFC) dokumentima ili drugim standardima kako bi se došlo do zaključka koji se operativni

sustav koristi. Kao što je vidljivo na slici rezultati nisu upotpunosti sigurni već se daje vjerojatnost od 97% da se koristi Windows 7 Proffesional za metu sa IP adresom 192.168.203.192.

Za detaljnije podatke o meti koristi se profil skeniranja *Slow comprehensive scan*. Unutar profila nalazi se mnogo naredbi i skripti koje će biti upotrebljene na meti 192.168.203.192. Iz profila skeniranja maknuta je naredba –sU koja označava UDP skeniranje port-ova koja značajno usporava skeniranje. Primjer korištenih naredbi prikazan je na slici 15.

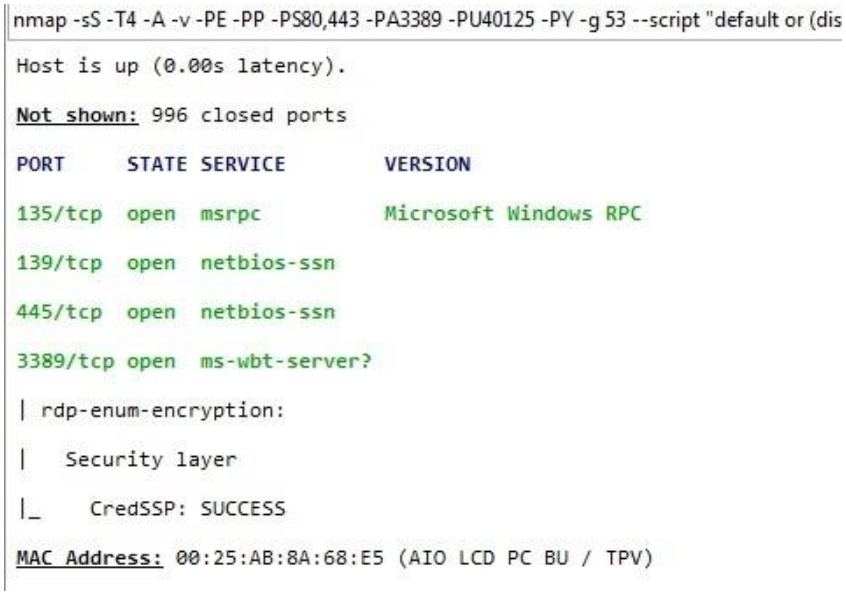


Slika 15 Naredbe korištene za detaljno skeniranje računala

Naredbama se određuje koje će vrste skeniranja biti uključene, koje će informacije biti tražene, koliko će detaljni biti rezultati, kojom brzinom će se odraditi skeniranje i druge mogućnosti vezane za skripte.

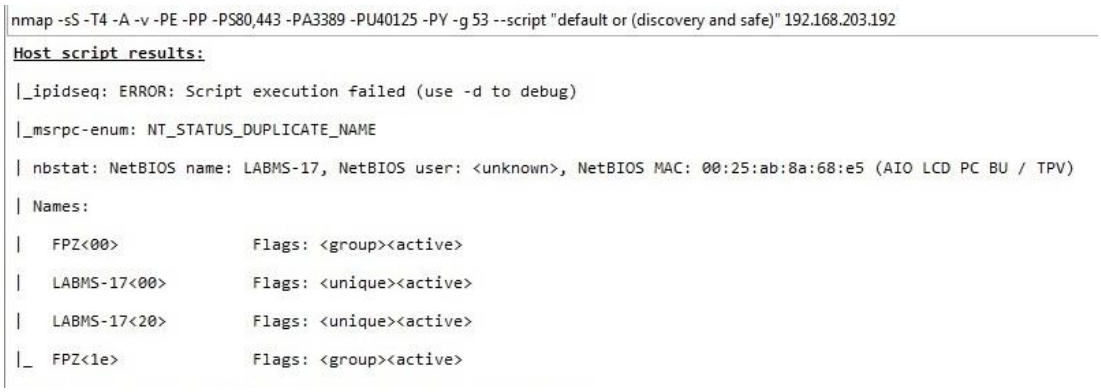
Naredba –T4 označava brzinu skeniranja gdje broj može biti od nula do pet gdje nula označava najsporije, a pet najbrže skeniranje. Povećanjem brzine se dobiva na vremenu, ali se istovremeno povećava mogućnost da skeniranje bude uočeno.

Naredbom –A omogućuje se agresivno prikupljanje informacija vezane za operativni sustav, usluge i verzije. Detaljniji rezultati se uključuju naredbom –v.[37]



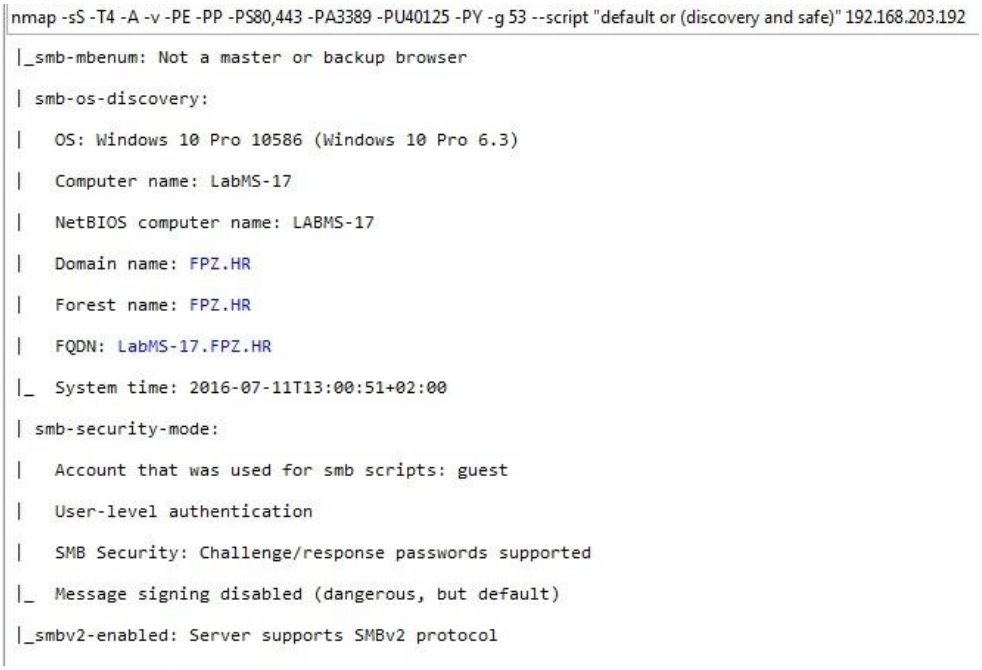
Slika 16 Rezultati skeniranja

Na slici 16. je vidljivo da je skenirano 1000 port-ova od kojih su četiri otvorena. Prikazane su usluge koje slušaju na tim port-ovima te na kraju i MAC adresa mete. Od četiri pronađena otvorena port-a, posebno je bitan port 3389. Sljedeće 3 linije otkrivaju da se radi o port-u putem kojega se radi udaljeni pristup računalu. Naredbom –PA3389 dolazi se do podataka da se koristi enkripcija za ovu uslugu te CredSSP (engl. *Credential Security Support Provider,* CredSSP) usluga koja se koristi za autentikaciju između klijenta i servera. Port 3389 predstavlja značajnu slabost koja se može eksploatirati daljnjim skeniranjima te na kraju i napadom na port.



Slika 17 Rezultati skripti - NetBIOS

U rezultatima skeniranja dolazimo do informacija dobivenih pokretanjem skritpti. Na slici 17. vidljiv je NetBIOS identifikator računala dok se nije uspjelo doći do naziva računa korisnika na računalu. Ispod se nalaze ostale informacije koje pokazuju da je računalo dio grupe FPZ koja je aktivna te kao jedinstveni identifikator koristi LABMS-17.[38]



Slika 18 Rezultati skripti - Domena

U prvoj liniji sa slike 18. vidljivo je da pomoću ovih skripti nije se moglo doći do informacija o Internet pretraživaču koji se koristi. Rezultati nastavljaju dalje sa otkrivanjem operativnog sustava koji se koristi. Vidljivo je iz slike da je na računalu pokrenut Windows 10 Pro verzije 6.3. Ponovo se pojavljuju podaci o NetBIOS imenu računala te se sada pojavlju i imena domene te pomoću njih i FQDN-a (engl. *Fully Qualified Domain Name*, FQDN) koji predstavlja potpuno ime računala na mreži.

Rezultatima dalje prelazimo smb-security-mode. U linijama ispod se saznaje da se koristi autentikacija koja zahtijeva korisničko ime i lozinku. Linijom *Challenge/response passwords supported* pokazuje da lozinke mogu biti u više vrsta: u nepromjenjenom obliku, LM (engl. *LAN Manager Hash,* LM), NTLM (engl. *Windows New Technology LAN Manager,* NTLM), LMv2 i NTLMv2. Sustav je slab na prisluškivanje ukoliko se koriste nepromijenjene lozinke dok su ostale verzije LM i NTLM slabe na određene vrste napada na lozinku te *man-in-the-middle* napade.[39]

Preostaje još samo zadnja linija vezana za digitalno potpisivanje poruka. U primjeru sa slike 18 je vidljivo da je digitalno potpisivanje isključeno te je to potencijalno opasno iako je standarno zadano da je digitalno potpisivanje poruka isključeno. Napadač je u mogućnosti izvesti *man-in-the-middle*[7]i SMB-relay (engl. *Server Message Block,* SMB) napad.

Među ostalim rezultatima koji nisu prikazani je TCP/IP „otisak prsta“ putem kojega se u ovome slučaju ne sazna ništa više od rezultata dobivenih drugim naredbama. Trajanje *Slow Comprehensive Scan* na samo jednoj meti, bez UDP skeniranja koje bi značajno produžilo trajanje skeniranja, je dvije minute. Meta je udaljena jedan skok od računala koje je izvršavalo skeniranje.[40]

[7]Man-in-the-middle napad se odnosi kada napdač presretne komunikaciju te sva komunikacija odvija u tajnosti preko napadača

5.2 Nessus

Nessus je dostupan kao besplatni programski alat za provjeru sigurnosnih slabosti računalnih mreža. Koristi sučelje kojemu se pristupa putem Internet preglednika i time omogućuje skeniranje mreže s udaljenje lokacije. Preko sučelja se pripremaju skeniranja, izvršavaju skeniranja te dobivaju rezultati skeniranja u odabranom obliku.

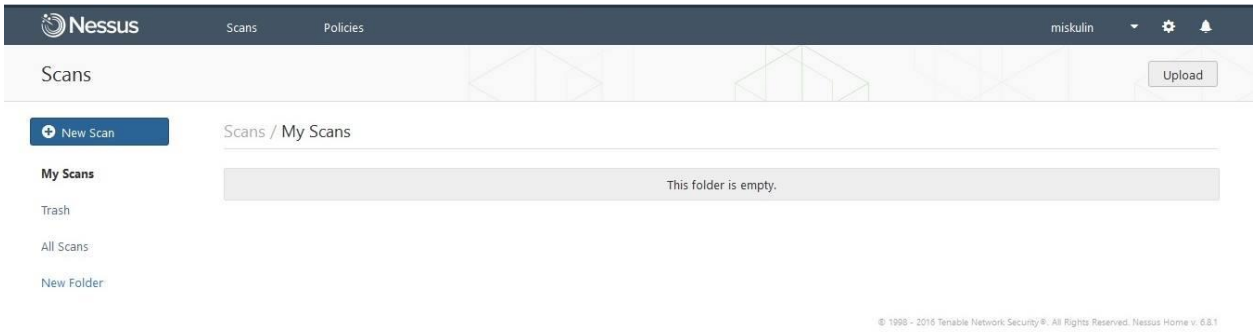
Glavne značajke ovog programskog alata: identifikacija slabosti mreže koja omogućuju napadaču pristup informacijama o sustavu računala u mreži i provjera dostupnih ažuriranja koja uklanjaju određene slabosti mreže. Programski alat također testira sigurnost računa u mreži koristeći zadane i često korištene lozinke, provodi analizu slabosti mreže te provjeru mobilnih uređaja u mreži.

Skeniranje je moguće izvršiti na jednom računalu, na spektru IP adresa ili na cijelim podmrežama. Postoje mnogi dodaci dostupni za preuzimanje pomoću kojih se detaljnije određuje kakve se slabosti traže u mreži. Nessus na često korištenim port-ovima ne pretpostavlja koje usluge koriste te port-ove već pokušava detektirati slabosti kako bi došao do više informacija.

Ažuriranje dodataka za Nessus je vrlo važno jer su oni napravljeni kako bi pojedinačno pronalazili slabosti u mreži ili računalnom sustavu. Mogu se napisati koristeći NASL [8] (engl. *Nessus Atack Scripting Language,* NASL). Opća podjela dodataka vrši se na dodatke koji pronalaze slabosti i dodaci koji iskorištavaju i napadaju slabosti. Dodaci su primarno napravljeni za poznate slabosti mreže i sustava, ali se mogu i napisati vlastiti dodaci sa specifičnim otkrivanjem slabosti ili dodaci za otkrivanje slabosti koje mogu doći sa jedinstvenom konfiguracijom vatrozida, mreže i drugih postavaka mreže.

Ažuriranje dodataka je bitno jer se kroz vrijeme otkrivaju nove slabosti odnosno ranjivosti mreže i sustava na nove viruse i ostale štetne programe.[41]

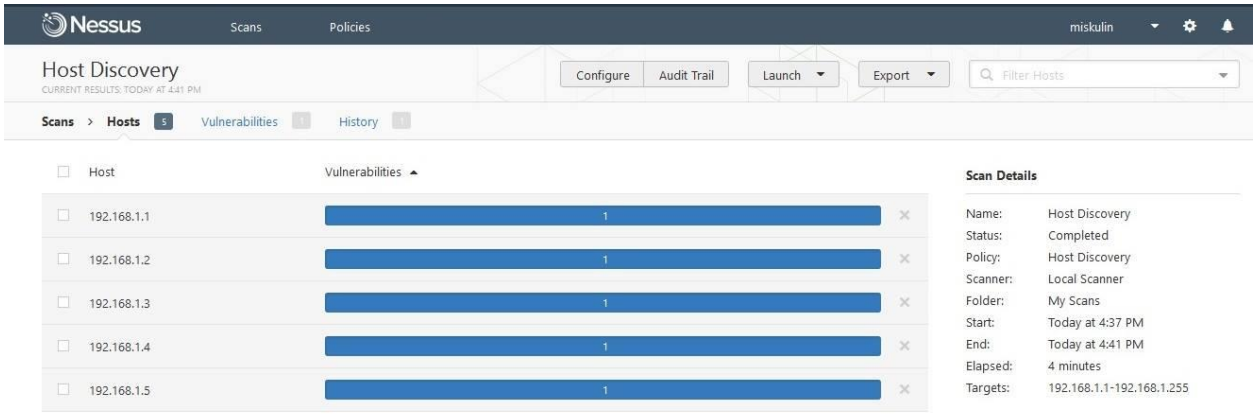
[8]NASL je skriptni jezik dizajniran za Nessus čija je svrha samostalno kreiranje skripti za detektiranje slabosti



Slika 19 Početno sučelje Nessus

Nessus se pokreče preko internet pretraživača i na slici 19. vidljivo je početno sučelje. Novo skeniranje se pokreče pritiskom na gumb New Scan. Nakon pritiska prelazi se u novi prozor gdje se odabire vrsta skeniranja. Predložene su standardne vrste skeniranja od otkrivanja računala na mreži, standardnog skeniranja primjerenog za sve vrste mreža, skeniranja za štetne programe do skeniranja kod kojih korisnik sam odabire detaljnije opcije skeniranja.

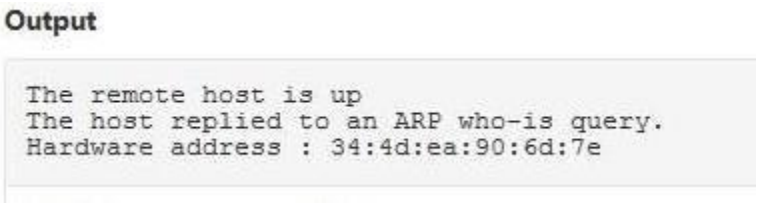
Za prvo skeniranje je odabran *Host Discovery* vrsta skeniranja. Za mete su odabrane IP adrese od 192.168.1.1 do 192.168.1.255



Slika 20 Otkrivanje uređaja na mreži koristeći Nessus

Na slici 20. vidljiv je rezultat skeniranja *Host Discovery*. U lokalnoj mreži pronađeno je pet uređaja koja su tome trenutku bili spojeni na mrežu. Ovo je vrlo

jednostavno skeniranje koje koristi ARP, ICMP, TCP i UDP ping kako bi ustanovio je li meta *online.* Pritiskom na određenu IP adresu ulazi se u detalje gdje je ispisano kako se došlo do rezultata.[42]

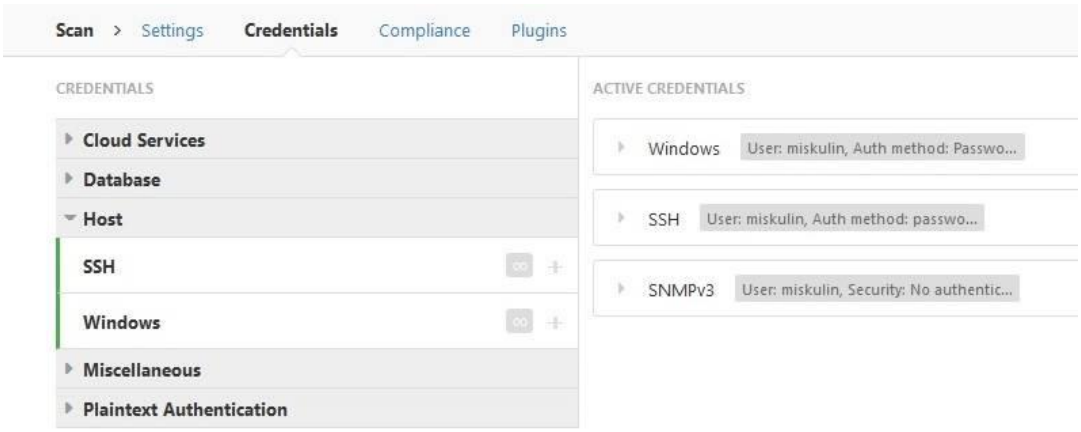


Slika 21 Odgovor na ARP ping

U slučaju sa slike 21. sve mete su odgovorile na ARP ping pakete iz čega se zaključuje da je meta *online*. Za sve mete je isti rezultat s razlikom fizičke odnosno MAC adrese.

Sljedeći korak je detaljnije skeniranje otkrivenih meta na mreži. Koristi se profil skeniranja *Advanced Scan* u kojemu se ručno odabiru opcije skeniranja. Unutar profila uključeno je slanje ARP, TCP i ICMP ping paketa, korištenje SSH, WMI (engl. *Windows Managment Instrumentation,* WMI) i SNMP enumeratora port-ova te slanje TCP SYN paketa ukoliko enumeratori ne uspiju doći do željenih informacija. TCP SYN paketima se ne uspostavlja potpuna konekcija. Od ostalih bitnijih postavki je detektiranje pokrenutih usluga. Detektiranje se vrši na svim port-ovima te se dodatno testira na svim port-ovima postojanje SSL i TLS usluge. Ukoliko se pronađu SSL i TLS usluge na njima se vrši detekcija šifranata koji se koriste.

Sljedeći korak je unošenje akreditacije. Za korištenje određenih opcija potrebna je akreditacija koja je vrlo korisna za administratore. Ovom metodom je moguće putem administratorovog korisničkog imena i lozinke detaljno skenirati računalo te detektirati greške koje ostali korisnici računala ne bi mogli detektirati.

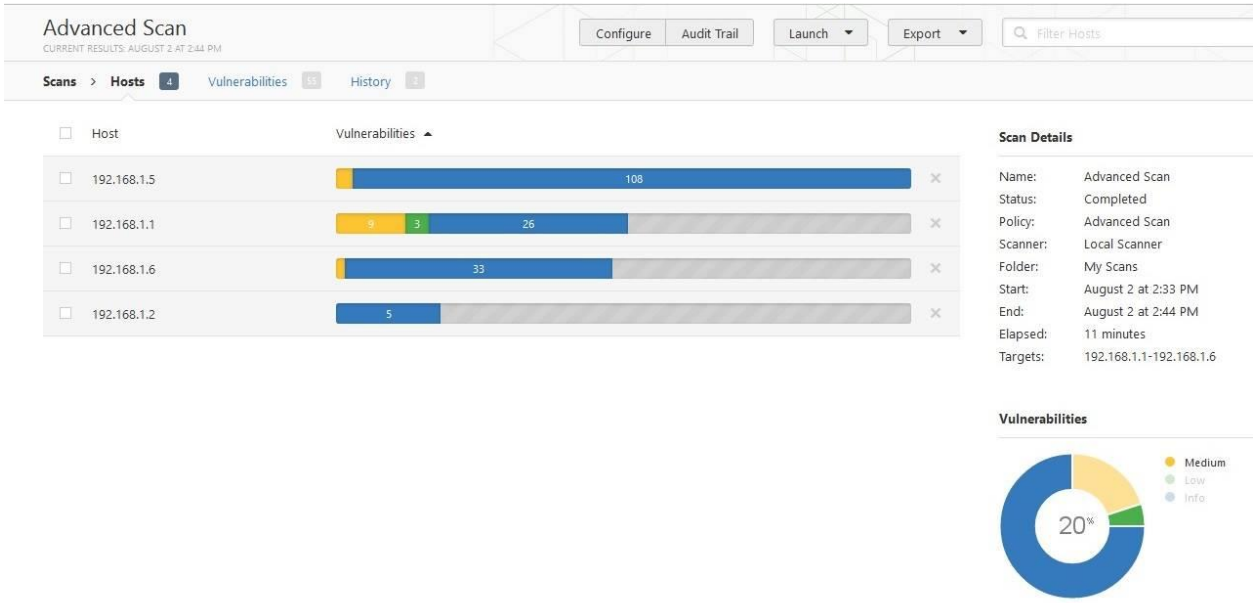


Slika 22 Akreditacije korištene u Advanced Scan

Na slici 22. vidljivo je da su aktivne tri akreditacije. Sve tri su dio Host akreditacija. Windows i SSH je moguće dodati neograničen broj puta te ih zasebno konfigurirati dok SNMPv3 (engl. *Simple Network Managment Protocol*, SNMP) je moguće dodati samo jednom. Windows akreditacijom moguće je koristiti korisničko ime i lozinku kao što jekorišteno u primjeru sa slike 22. Ostale mogućnosti su: Kerberos, LM Hash i NTLM Hash. Za korištenje Kerberosa potrebno je korisničko ime, lozinka te centar distribucijskih ključeva. Za korištenje LM Hash i NTLM Hash je potrebno korisničko ime i hash lozinke.[43]

Korištenjem SSH (engl. *Secure Shell,* SSH) akreditacije omogućuje da skeniranje bude detaljnije te brže izvršeno. Korištena je opcija korisničkog imena i lozinke koja je nesigurna, ali i najjednostavnija. Ostale mogućnosti su Kerberos, korištenje javnog enkripcijskog ključa i korištenje certifikata. U SNMPv3 opciji odabrana je akreditacija bez šifre i bez privatnosti. U toj opciji unosi se samo korisničko ime i broj port na kojemu će se izvršiti skeniranje. U ostalim opcijama je autentikacija bez privatnosti i autentikacija sa privatnosti. U autentikaciji bez privatnosti se koristi SHA1 (engl. *Secure Hash Algorithm 1,* SHA1) ili MD5 (engl. *Message Digest 5,* MD5) algoritam enkripcije šifre. U autentikaciji sa privatnosti se odabire AES (engl. *Advanced Encryption Standard,* AES) ili DES (engl. *Data Encryption Standard,* DES) algoritam za dodatnu privatnost uz koju se mora unesti i lozinka za privatnost.[43]

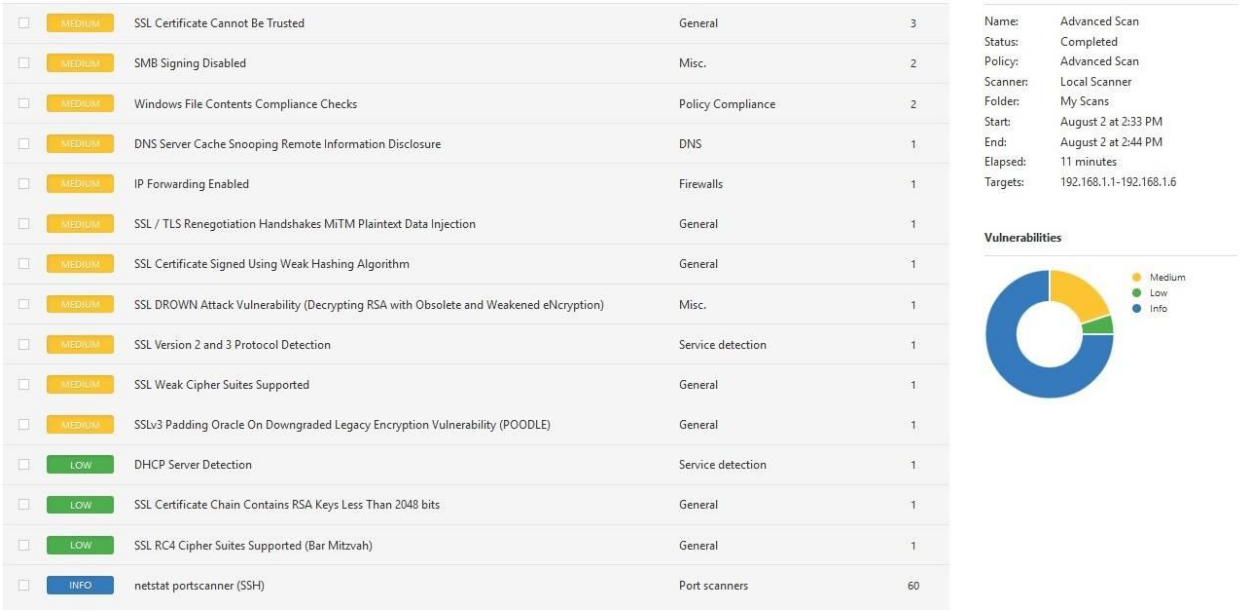
Završetkom skeniranja dobivenisu rezultati prikazani u slici 23. Rezultati prikazani u dvije vrste: po *Host-u* i ukupno. U sredini slike *Host-ovi* poredani po broju određenih slabosti detektiranih tijekom skeniranja te im je s lijeve strane prikazana IP adresa. U donjem desnom kutu vidljivi su ukupni rezultati skeniranja.



Slika 23 Rezultat skeniranja Advanced Scan

Bojama se označuju različite vrste slabosti ovisno o njihovoj vrsti te mogućoj šteti. U primjeru sa slike plavom su bojom označene informacije o *host-ovima*, zelenom bojom manje značajne slabosti putem kojih nije moguće napraviti veliku štetu te žuta boja koja označava srednje rangirane opasnosti. Postoje još opasnosti narančaste i crvene boje koje označavaju dvije najopasnije grupe slabosti.

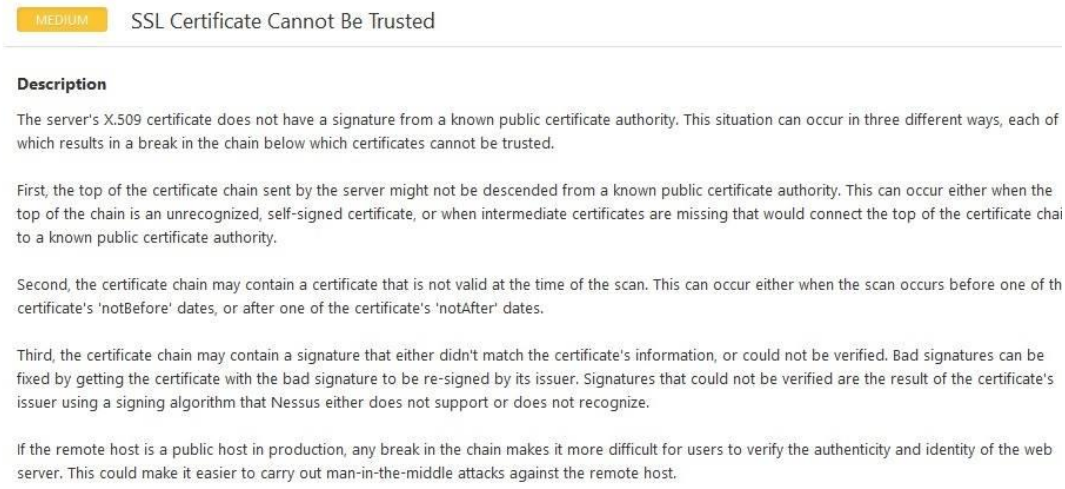
Od dobivenih rezultata 75% čine različite informacije, 5% nisko rangirane i 20% srednje rangirane slabosti. Primjer dobivenih informacija: naziv računala, MAC adresa, operativni sustav, otvoreni port-ovi te razloge zašto dio skeniranja nije uspio doći do ciljanih informacija.[43]



MEDIUM	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	SMB Signing Disabled	Misc.	2
MEDIUM	Windows File Contents Compliance Checks	Policy Compliance	2
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1
MEDIUM	IP Forwarding Enabled	Firewalls	1
MEDIUM	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
MEDIUM	SSL Weak Cipher Suites Supported	General	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	General	1
LOW	DHCP Server Detection	Service detection	1
LOW	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	General	1
LOW	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	General	1
INFO	netstat portscanner (SSH)	Port scanners	60

Slika 24 Popis detektiranih slabosti rangiranih po opasnosti

Na slici 24. prikazan je popis detektiranih slabosti na svim metama. Popis se nastavlja dalje s raznim informacijama kojima je dodan faktor opasnosti nula. Pritiskom na određenu slabost, ulazi se u detalje. Detalji se satoje od opisa slabosti, mogućeg rješenja, dodatne poveznice za više informacija i izvor slabosti.



MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the chain below which certificates cannot be trusted.

First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chai to a known public certificate authority.

Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of th certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Slika 25 Opis slabosti

Na primjeru iz slike 25. vidljiv je detaljan opis zašto pronađeni X.509 SSL certifikat nije siguran. Opisane su sve tri mogućnosti putem kojih se dolazi do nesigurnog certifikata. Prvi slučaj je da certifikat dolazi sa poslužitelja koji nije javno poznat i njegovo porijeklo nije potvrđeno kao sigurno. Druga mogućnost je da vrijeme u koje se upotrebaljava certifikat nije ispravno. Certifikat nije siguran ukoliko se upotrebljava prije ili nakon određenog vremenskog roka. Treća mogućnost da potpis ne odgovara informacijama na certifikatu ili nije moguće potvrditi potpis. Nadalje se napominje da u sva tri slučaja dolazi do prekida lanca s nesigurnim certifikatom te da nesigurni certifikati olakšavaju izvedbu *man-in-the-middle* napada.

Za rješenje je predložena kupnja ili generiranje ispravnog certifikata za uslugu. Sljedeći dio detalja je prikaz dobitka informacija sa mete.

Slika 26 Ispis izvora slabosti

Sa slike 26. je vidljiva dva primjera slabosti. U oba primjera sa slike se certifikat nalazi na vrhu lanca. Certifikat je dobiven sa udaljenog računala te je certifikat potpisan od nepoznatog tijela. Prvi je vezan za metu sa IP adresom 192.168.1.1, port 443 s TCP protokolom. Pod Subject vidimo gdje se nalazi slabost, odnosno gdje se koristi certifikat. Izdavač certifikata je vidljiv u sljedećem redu.

Drugi primjer sa slike se nalazi na meti 192.168.1.5 na port-ovima 1583 i 8834. Također je vidljivo mjesto gdje se nalazi slabost te izdavač certifikata.

Slika 27 Isključeno digitalno potpisivanje

Digitalno potpisivanje nije zahtijevano prilikom uspostavljanja konekcije s poslužiteljem, što je prikazano na slici 27. Napadač može iskoristiti tu slabost kako bi napravio *man-in-the-middle*- napad. Za rješenje je predloženo mijenjanje postavaka polica te su priložene dodatne poveznice za više informacija o samoj slabosti i uklanjanju slabosti. Na kraju izvješća za navedenu slabost su navedene mete 192.168.1.5 i 192.168.1.6 s port-om 445 kao mjesto pronađene slabosti.

Sljedeća bitnija slabost je SSL/TLS Renegotiation Handshakes koja koristi enkripciju podataka, ali dozvoljava nesigurne promjene konekcije nakon inicijalne sigurne uspostave konekcije. Napadač je u mogućnosti iskoristiti ovu slabost te izvesti *Man-in-the-middle* napad. Na IP adresi 192.168.1.1 koriste se usluge TLSv1 i SSLv3 sa navedenom slabosti.

Ostale pronađene slabosti su vezane uz korištenje slabih šifranata u postupku enkripcije i stvaranja *hash-a*. Za rješenje je predloženo korištenje šifranata veće duljine te upotreba novih enkripcijskih postupaka.

5.3 Nexpose Community Edition

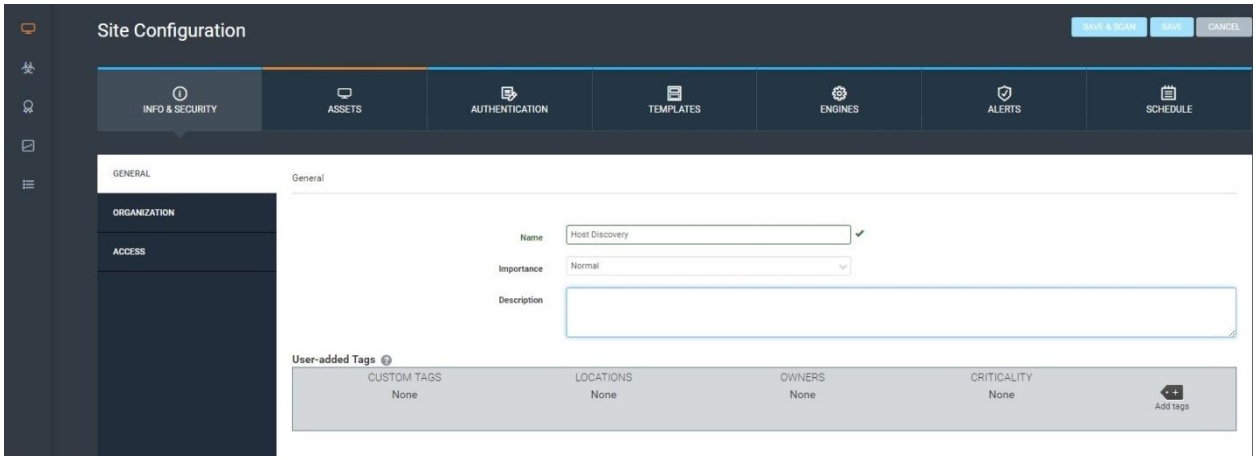
Nexpose Community Edition koji će biti korišten u ovome radu je besplatni alat za testiranje i pronalaženje slabosti mreže. Community Edition zadržava mnoge odlike od verzija koje se plaćaju. Najveća razlika je ograničenje na 32 IP adrese koje je

moguće skenirati. Među ostalim razlikama je izuzeće određenih dodataka koji su vezani za lakše upravljanje slabostima mreža većih poslovnih tvrtki. Time je Community Edition dobro rješenje za male tvrtke te za privatnu upotrebu. Nedostatak ove verzije pa tako i ostalih verzija su veliki sistemski zahtjevi od računala na kojemu se instalira programski alat.[44]

Nexpose prilikom skeniranja identificira aktivne usluge, otvorene port-ove i pokrenute aplikacije na svakome računalu u mreži. Pokušava pronaći sve slabosti bazirane na informacijama o uslugama i aplikacijama. Rezultate skeniranja je moguće promijeniti kako bi se prvo prikazale slabosti s najvećom ocjeno mopasnosti. Nexpose integriran s *Metasploit Pro* alatom može ukloniti krivo detektirane slabosti, potvrđivanje postojanja slabosti te testiranje mjera za uklanjanje postojeće slabosti.[45]

U ovome poglavlju će se preskočiti dio otkrivanja računala u mreži zbog ograničenja verzije programskog alata na 32 IPadrese.

Programski alat se pokreće preko internetskog preglednika te korištenjem port-a određenog tijekom instalacije alata.



Slika 28 Sučelje Nexpose Community Edition

Nakon pokretanja programskog alata i pritiskom na *Site Configuration* kreće se u pripremanje skeniranja. Polja za ispunjavanje opcija prikazana su na slici 28. U prvome

prozoru se upisuje ime te opcionalno i opis skeniranja. U području *Assets* se upisuju mete za skeniranje dok je od ostalih područja još bitno područje Templates.

Slika 29 Odabir profila skeniranja

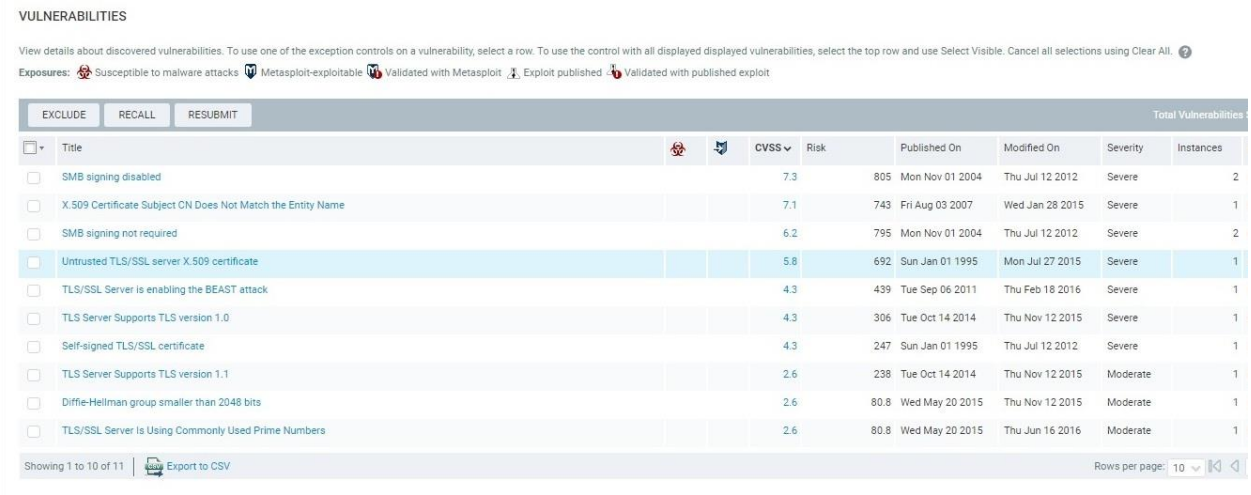
Na slici 29. vidljiv je dio ponuđenih profila skeniranja. Odabran je profil *Full audit*dok su mete u području IP adresa od 192.168.1.100 do 192.168.1.130 unesene u području *Assets*. Ostala područja su vezana uz autentikaciju ukoliko je potrebna, obavijesti tijekom skeniranja te planiranja vremena skeniranja.

Nakon završetka skeniranja dobije se više različitih oblika rezultata. Rezultati koji su prikazani u sučelju te izvješća u PDF (engl. *Portable Document Format,* PDF)iliHTML (engl. *Hypertext Markup Language,* HTML) formatu. Izvješća se dijele na *Executive Report* i *Audit Report*. *Executive Report* je izvješće u kojemu se nalaze najvažnije stavke skeniranja s malom količinom detalja. Takvo izvješće je predviđeno kako bi olakšalo prikaz stanja sigurnosti mreže zaposlenicima koji nemaju predznanje o sigurnosti računalnih mreža te je predviđeno kao izvješće koje se predaje nadređenima u tvrtci.

Audit Report je izvješće koje sadrži sve detalje vezano za skeniranje te je znatno veće od *Executive Report-a*. Sastoji se oddevet poglavlja od kojih je prvo sažetak *Executive Report-a*. Drugo poglavlje sadrži otkrivene čvorove u mreži, operativne sustave koji se koriste, pridružena faktora rizika i alias čvora. U trećem poglavlju

izvješća se prelazi na otkrivene i potencijalne opasnosti. Opasnosti su pojedinačno opisane, navedene su IP adrese gdje se opasnost nalazi te dodatne poveznice za detaljnije informacije i rješenje za uklanjanje opasnosti.

U sljedećem poglavlju izvješća se prelazi na otkrivene usluge te nakon toga na otkrivene korisnike i grupe. U zadnjim poglavljima se navode otkrivene baze podataka, podaci i direktoriji te evaluacije korištenih polica.

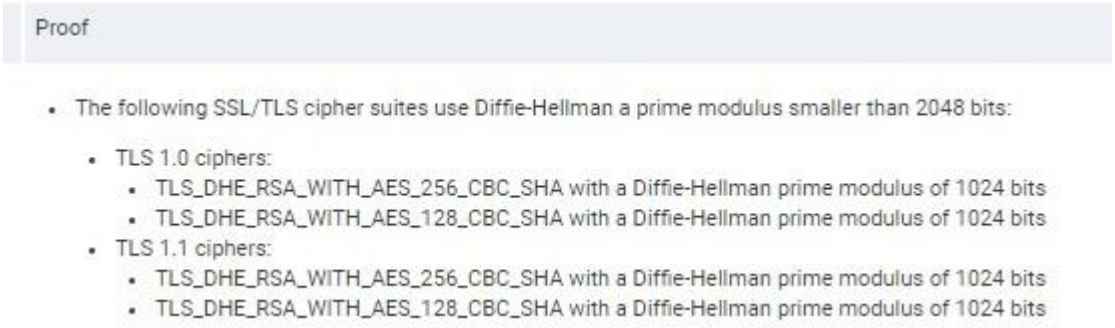


Slika 30 Prikaz pronađenih slabosti

Na slici 30. prikazane su pronađene slabosti te su poredan po CVSS-u (engl. *Common Vulnerability Scoring System*, CVSS) odnosno ocjena opasnosti[9]. Svakoj slabosti se pridružuje određena ocjena opasnosti ovisno u vrsti slabosti, vremenu koje slabost već postoji te o postojanju štetnih programa za iskorištavanje slabosti. Ocjene za opasnost su od jedan do deset s time da je deset najveća ocjena za opasnost.Sa slike 30. je vidljivo da je najveća pronađena opasnost isključeno digitalno potpisivanje te je takvoj opasnosti pridružen CVSS od 7.3 te se takva opasnost pojavljuje na dva mjesta. Slijedi opasnost zbog nepravilnosti u certifikatu X.509. Podaci uneseni u polje za javno ime certifikata ne slažu se imenom entiteta koji je izdao certifikat.Za treću najveću opasnost ponovo je navedeno ne zahtijevanje digitalnog potpisivanja. Nakon toga slijedi nepovjerljivi TLS/SSL poslužitelj s X.509 certifikatom. Ponovo se pojavljuje

[9]CVSS – Standardni sustav vrijednovanja detektiranih slabosti

opasnost s već navedenim X.509 certifikatom. Zamjenom X.509 certifikata u ovome slučaju bi se uklonile dvije opasnosti. Dalje na listi vidiljive su opasnosti vezane uz TLS/SSL poslužitelj. Za opanosti vezane uz poslužitelj navedene su: dopušta BEAST (engl. *Browser Exploit Against SSL/TLS,* BEAST) napad[10], podržava nesigurne TLS usluge verzije 1.0 i 1.1 te koristi javno poznate prim brojeve u enkripciji. Ostatak liste čini samopotpisani TLS/SSL certifikat te ključevi za Diffie-Hellman postupak koji su manji od 2048bita. Ulaskom u detalje slabosti navedeno da tim znanstvenika može dešifrirati komunikaciju s prim brojevima do 768 bitova dok državne službe mogu dešifrirati do 1024 bita.



Slika 31 Pojavljivanje Diffie - Hellman slabih šifranata

Na slici 31. vidljiva su četiri mjesta gdje se koriste prim brojevi od 1024 bita za šifrante. Pojavljuju se u TLS verziji 1.0 i 1.1 u verzijama sa AES 128 i 256 enkripcijskim standardima. Ovakva slabost je od značaja za velike korporacije jer postupak za iskorištenje ovakve slabosti zahtijeva velike resurse.

[10]BEAST napad koristi slabosti CBC postupka šifriranja za napad na usluge sa SSL protokolom

Slika 32 Grafički prikaz pronađenih slabosti

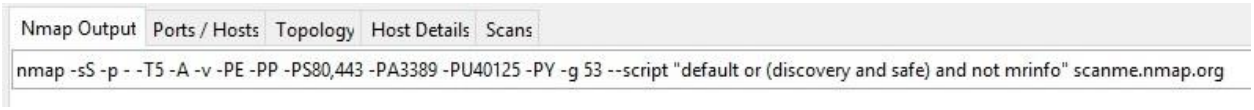
Na slici 32. grafički su prikazane slabosti podijeljene u dva grafa: graf slabosti po ocjeni CVSS-a i graf iskoristivosti slabosti ovisno o znanju napadača. Lijevi graf pokazuje podjelu slabosti po ocjeni CVSS-a. Najveći dio čine slabosti ocjenjene između 4 i 5.9 te su u grafu prikazane tamno plavom bojom i ukupno ih je 16. Slijede ih slabosti s ocjenama od 6 do 7.9 koje su prikazane crvenom bojom na grafu i ukupno ih je četiri. Desni graf se odnosi na napadačevo znanje. Za iskorištenje dvije slabosti je potreban napadač s znatnim znanjemdok za ostale 23 slabosti ne postoji javno poznati način iskorištenja slabosti.

6. Usporedna analiza programskih alata Network Mapper, Nessus i Nexpose

U ovome poglavlju će se upotrijebiti sva tri programska alata na jednoj meti te će se usporediti razlike, međusobni odnosi u obliku nedostataka i odlika pojedinih alata. Za metu je odabrana scanme.nmap.org na kojoj je dozvoljena upotreba programskih alata za sigurnost te i korištenje svih vrsta skeniranja.

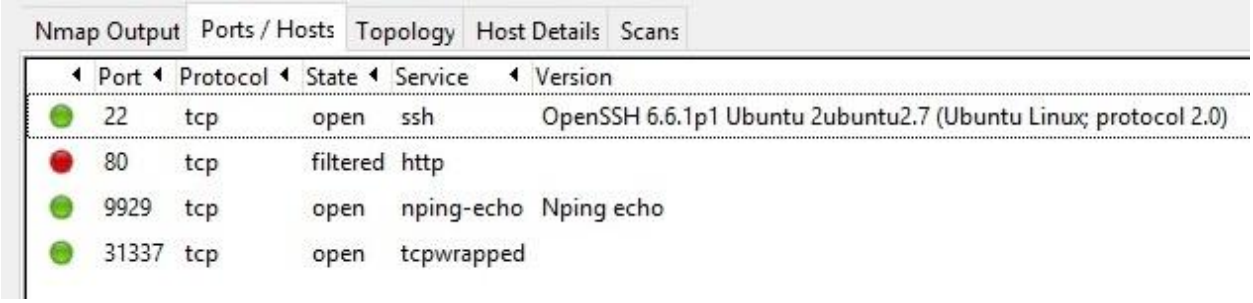
6.1 Network Mapper

Kao prvi programski alat odabran je Network Mapper. Korištena je izmjenjena verzija *Slow Comprehensive Scan*-a s dodatkom jedne naredbe te izuzećem pokretanja jedne skripte.



Slika 33 Korištene naredbe za skeniranje pomoću Network Mapper-a

Razlika od prethodno korištenog *Slow Comprehensive Scan-a* je u dodatku naredbe –p- koja omogućuje skeniranje svih port-ova za razliku od standardnih 1000 port-ova u tome profilu skeniranja. Druga razlika je ne pokretanje skripte dodavanjem naredbe "*and not mrinfo*" zbog koje dolazi do greške prilikom pokretanja na računalu sa Windows 10 operativnim sustavom. Korištene naredbe prikazane su na slici 33.



Slika 34 Otkriveni port-ovi

Na slici 34. prikazana je lista detektiranih port-ova. Vidljivo je da se na sva četiri port-a koristi TCP protocol, te su tri port-a otvorena te je jedan filtriran. Ovi port-ovi će dalje poslužiti za detekciju operativnog sustava mete. Također su na slici 34. vidljive pokrenute usluge te njihove pripadajuće verzije.

Dalje se u rezultatima prelazi na detaljnije informacije dobivene s određenih port-ova. Najveća količina informacija je dobivena sa port-a 22 spokrenutom SSH uslugom.

```
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.7
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
```

Slika 35 Informacije vezane za "otisak prsta" javnog ključa poslužitelja

Na slici 35. u zadnja tri reda prikazane su informacije o “otisku prsta” javnog ključa poslužitelja. Sam otisak prsta predstavlja skraćeni zapis javnoga ključa. Otiskom prsta autentificira se javni ključ. Daljnjim izvlačenjem informacija te pokretanjem određenih skripti moguće je doći i do samog javnog ključa. No javni ključ ne predstavlja sigurnosnu slabost.[45]

Nakon informacija o javnim ključevima slijedi popis korištenih algoritama za razmjenu ključeva, enkripcijskih algoritama, MAC algoritama za autentikaciju poruka te kompresijski algoritmi. Otkriveno je osam algoritama za razmjenu ključeva, 16 enkripcijskih algoritama, 19 MAC algoritama i dva kompresijska algoritma. Svi ovi algoritmi su vezani za SSH usluguna port-u 22.

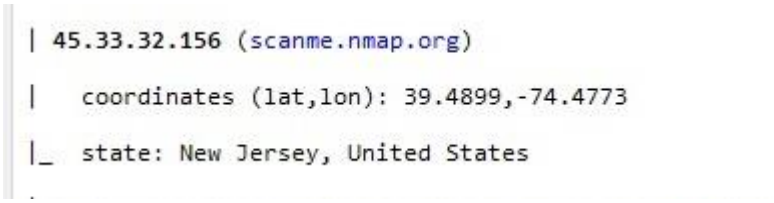
Slika 36 Dio otkrivenih algoritama korištenih u SSH usluzi

Sa slike 36.vidljiv je dio otkrivenih enkripcijskih algoritama korištenih za SSH uslugu. Enkripcijski algoritam se koristi u oba smjera klijentsko-poslužiteljske veze budući da nije drugačije navedeno.[46]

Za port 80 nema dostupnih detaljnijih informacija budući da je on korištenim skeniranjem detektiran kao filtriran port. Za ostala dva otvorena port-a nema dodatnih informacija nasprem dobivenih u već prikazanome Ports/Hosts prozoru.

Za operativni sustav pokrenut na meti dana su dva moguća: Linux 3.13 ili 4.2 te je navedena mrežna udaljenost od 12 skokova.U prozoru Host Details se daje veća vjerojatnost verziji 4.2 operativnog sustava Linux.

Dolazi se do rezultata dobivenih poretanjem skripti. Prvo su navedeni podaci o autonomnom sustavu. Za državu je dobiveno USA odnosno SAD te je kasnije navedeno detaljnije New Jersey sa točnom geolokacijomkao što je prikazano na slici 37.



Slika 37 Lokacija skenirane mete

Među pokrenutim skriptama nalazi se skripta koja prati put do mete te geolokaciju svakog čvora koji obilježava jedan skok u mreži.

Slika 38 Put do mete označen u skokovima u mreži

Na slici 38.je vidljiv broj skokova u mreži počevši od računala s kojega se vrši skeniranje te završno s metom na kojoj se vrši skeniranje. Za svaki skok je vidljiv i RTT (engl.*Round Trip Time,* RTT) te DNS i IP adresa. U zadnjem stupcu vidljiva je geolokacija određenog čvora.

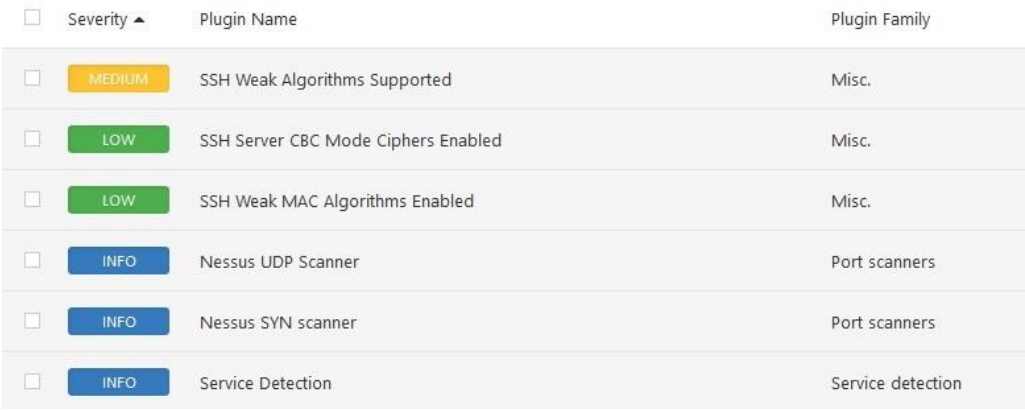
Slika 39 Rezultat WhoIS skripte

Pokretanjem *WhoIs* skripte pretražuju se baze podataka kako bi se došlo do informacija vezanih za podmrežu u kojoj se nalazi meta te kontaktu vezanom za podmrežu. Na slici 39. je vidljivo da je meta dio podmreže 45.33.0.0 – 45.33.127.255 te da je naziv podmreže LINODE-US koja pripada tvrtci Linode. Ponovno je vidljivo da se meta nalazi u državi New Jersey te je na kraju naveden kontakt u obliku elektronske pošte.

6.2 Nessus

Za skeniranje mete scanme.nmap.org pomoću programskog alata Nessus korišten je isti profil skeniranje *Advanced Scan* kao i u prethodnom poglavlju. Korištene su iste akreditacije unutar profila skeniranja. Trajanje skeniranja je znatno duže od skeniranja Network Mapper-a. Trajanje skeniranja Network Mapper-a je 294 sekunde odnosno otprilike pet minuta dok je trajanje skeniranja Nessus-a trajalo 1 sat i 26 minuta.

Prilikom skeniranja otkrivena je jedna slabost ocijenjena srednjom opasnosti, dvije slabosti ocijenjene niskom opasnosti te 29 dodatnih informacija vezanih za metu.



Severity	Plugin Name	Plugin Family
MEDIUM	SSH Weak Algorithms Supported	Misc.
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.
LOW	SSH Weak MAC Algorithms Enabled	Misc.
INFO	Nessus UDP Scanner	Port scanners
INFO	Nessus SYN scanner	Port scanners
INFO	Service Detection	Service detection

Slika 40 Rezultat skeniranja programskog alata Nessus

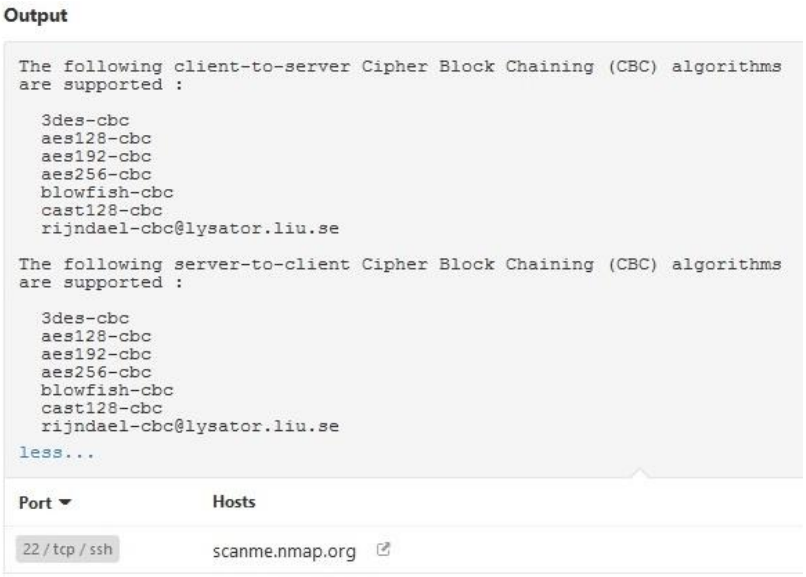
Za najveću detektiranu slabost ocijenjeno je korištenje slabih algoritama za šifriranje na SSH poslužitelju što je vidljivo sa slike 40. Ulazom u detalje dobiva se informacija da je poslužitelj konfiguriran da koristi Arcfour šifrante ili da ih ne koristi upotpunosti. Dokument RFC 4253 predlaže da se arcfour (engl. *Rivest Cipher 4*, arcfour) ne koristi zbog njegovih slabosti.

Slika 41 Slabi enkripcijski algoritmi u upotrebi

Na slici 41. prikazani su slabi enkripcijski algoritmi u upotrebi te su podijeljeni ovisno u smjeru komunikacije. Vidljivo je da se algoritmi arcfour, arcfour128 i arcfour 256 koriste za enkripciju od poslužitelja prema klijentu i obrnuto. U zadnjem redu je

vidiljiv DNS mete te broj port-a, vrsta protokola koja se koristi, koji je u ovome slučaju TCP te usluga SSH.

Za sljedeću slabost je navedeno korištenje CBC (engl. *Cipher Block Chaining,* CBC) postupka za šifriranje. SSH poslužitelje je konfiguriran da koristi CBC postupak šifriranja. Prilikom ovakvoga postupka šifranja se dobiva ista šifrirana poruka za istu unesenu poruku koja se šifrira. Napadač je u mogućnosti otkriti izvornu poruku. Za rješenje slabosti je navedena zamjena CBC sa CTR (engl. *Counter Mode,* CTR)ili GCM (engl. *Galois/Counter Mode,* GCM) postupcima šifriranja.



Slika 42 Slabi CBC algoritmi u upotrebi

Na slici 42. je vidljiv popis slabi CBC algoritama koji se koriste za oba smjera komunikacije te su vezani za SSH uslugu na port-u 22.

Zadnja pronađena slabost su slabi MAC algoritmi. SSH poslužitelj je konfiguriran da dopusti upotrebu MD5 i 96 bitne MAC algoritme koji se koriste za autentikaciju poruka.

Output

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com
```

Slika 43 Slabi MAC algoritmi u upotrebi

Sa slike 43. vidljiv je popis slabih algoritama za autentikaciju poruka kojima se dopušteno korištenje.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

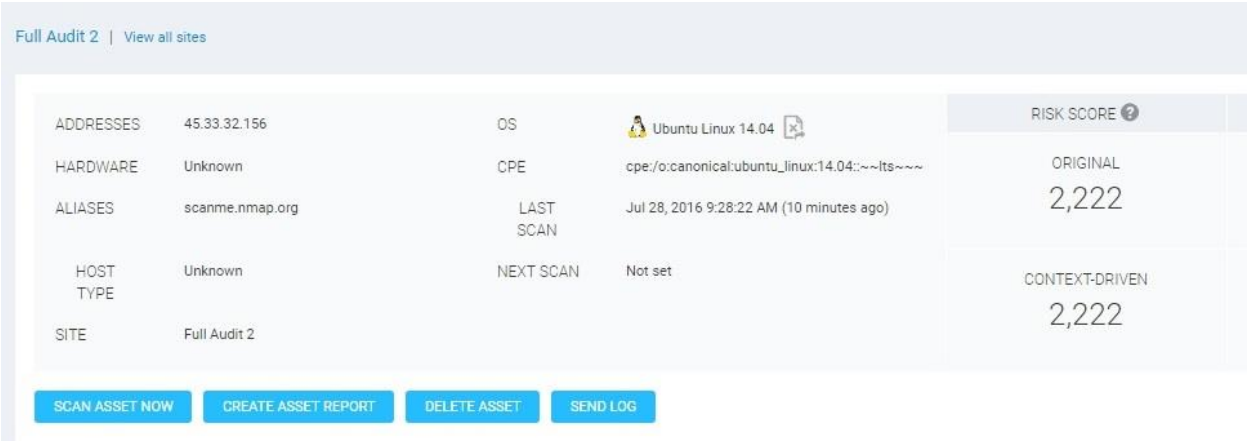
Slika 44 Opis slabih algoritama za autentikaciju poruka

Sa slike 44. je vidljivo da Nessus stavlja MD5 i 96 bitne algoritme u skupinu slabih algoritama koji ne osiguravaju dovoljnu razinu sigurnosti. Slabost je ocjenjena sa opasnošću od 2.6 čime ne predstavlja značajnu opasnost već slabost koju treba s vremenom zamijeniti s jačim algoritmima.

Od bitnijih informacija su četiri otvorena UDP port-a te tri otvorena TCP port-a. Detektirane su 3 aktivne usluge: SSH poslužitelj na port-u 22, HTTP usluga na port-u 80 te NTP usluga na port-u 123. Za operativni sustav je detektiran Linux Kernel 2.6. Dodane su informacije za SSH poslužitelj za kojega detektirano da podržava autentikaciju putem javnog ključa ili lozinke. Na kraju je napisana ruta od računala koje skenira do mete. Uz rutu nisu priloženi RTT, DNS i geolokacija.

6.3 Nexpose

Za skeniranje mete scanme.nmap.org progmraskim alatom Nexpose odabran je profil skeniranja Full Audit kao i u prethodnom primjeru. Naziv spremljenog skeniranja je Full Audit 2 zbog iskorištenog naziva u prethodnome primjeru. U ovome profilu skeniranja su za razliku od prošlog skeniranja alatom Nexpose dodane opcije skeniranja svih port-ova te korištenje UDP paketa za skeniranje UDP port-ova.



Slika 45 Rezultat skeniranja Nexpose programskim alatom

Sa slike 45.je vidljiva IP adresa i DNS mete, operativni sustav koji je pokrenut, datum kada je izvršeno skeniranje te ocjena rizika.

Title	CVSS	Risk
Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	6.8	405
Apache HTTPD: HTTP Trailers processing bypass (CVE-2013-5704)	5	201
TCP Sequence Number Approximation Vulnerability	5	194
Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183)	5	187
Apache HTTPD: mod_dav crash (CVE-2013-6438)	5	161
Apache HTTPD: mod_log_config crash (CVE-2014-0098)	5	161
Apache HTTPD: mod_cgid denial of service (CVE-2014-0231)	5	159
Apache HTTPD: mod_cache crash with empty Content-Type header (CVE-2014-3581)	5	157
Apache HTTPD: mod_lua: Crash in websockets PING handling (CVE-2015-0228)	5	153

Slika 46 Popis detektiranih slabosti

Sa slike 46. je vidljiv dio popisa detektiranih slabosti, poredanih po CVSS-u. Za prvu i treću slabost je u trećem stupcu pridružen simbol. Simbol označava da postoji poznati program koji može iskoristiti određenu slabost.

Dalje u izvješću skeniranja nalazi se popis programa koji se mogu iskoristiti za napad na slabosti skenirane mete.

EXPLOITS

Exploit	Source Link
Apache 2.4.7 mod_status Scoreboard Handling Race Condition	Exploit Database
Microsoft Windows - Malformed IP Options DoS Exploit (MS05-019)	Exploit Database
Microsoft Windows 2000/XP - TCP Connection Reset Remote Attack Tool	Exploit Database
Multiple OS (Win32/Aix/Cisco) - Crafted ICMP Messages DoS Exploit	Exploit Database
Multiple Vendor TCP Sequence Number Approximation Vulnerability (1)	Exploit Database
Multiple Vendor TCP Sequence Number Approximation Vulnerability (2)	Exploit Database
Multiple Vendor TCP Sequence Number Approximation Vulnerability (3)	Exploit Database
Multiple Vendor TCP Sequence Number Approximation Vulnerability (4)	Exploit Database
Stream / Raped - Denial of Service Attack (Windows)	Exploit Database
TCP Connection Reset Remote Exploit	Exploit Database

Slika 47 Popis programa za iskorištavanje detektiranih slabosti

Na slici 47. prikazan je popis programa koji mogu biti upotrebljeni za iskorištavanje slabosti. Prvi program putem Apache 2.4.7 poslužitelja u mogućnosti je izvestiDenial of Service odnosno napad s prekidanjem usluga koje pruža poslužitelj[11]. Također je u mogućnosti doći do povjerljivih informacija o akreditaciji ili izvršiti određene komande na poslužitelju. Ovakva slabost se pojavljuje na svim verzijama prije Apache 2.4.10 u *Race Condition-u*.[47]

Ostalih devet stavaka na listi se odnosi na različite programe i alate koji putem TCP, IP i ICMP pakete kako bi izvršili DoS (engl. *Denial of Service,*DoS) napad. Vidljivo

[11]Denial of Service je napad pri kojemu se slanjem velikog broja lažnih zahtjeva preopterećuje poslužitelj

je da postoji mnogo načina da se izvede Denial of Service napad te da korisnici poslužitelja nisu u mogućnosti koristiti usluge poslužitelja.

Za rješenja slabosti je navedeno ažuriranje na Apache 2.4.10 verziju te digitalno potpisivanje TCP paketa.

SERVICES

Service Name	Product	Port	Protocol	Vulnerabilities
SSH	OpenSSH 6.6.1p1	22	TCP	0
HTTP	HTTPD 2.4.7	80	TCP	12
NTP		123	UDP	0
<unknown>		31337	TCP	0

Slika 48 Detektirane usluge

Na slici 48. su detektirane 4 usluge. U prvome stupcu su nazivi usluga: SSH, HTTP i NTP (engl. *Network Time Protocol,* NTP*)* dok je jedna ostala nepoznata. U sljedećem stupcu su navedene verzije za određenu uslugu. Također suna slici navedeni port-ovi na kojima je usluga aktivna. Bitan detalj sa slike je 12 slabosti vezan za HTTP 2.4.7 uslugu na port-u 80. Sve prethodno navedene slabosti i programi i alati koji mogu iskoristiti slabosti vezani su za HTTP uslugu. Odnose na jednu uslugu na jednome port-u. Ažuriranjem verzije usluge i promjenom postavaka TCP komunikacije uklonile bi se sve navedene opasnosti.

6.4 Usporedba alata

U ovome poglavlju će se usporediti programski alati po općim karakteristikama te po rezultatima skeniranja odnosno pronađenim slabostima.

Tablica 1 Usporedba alata po općim karakteristikama

	Vrijeme skeniranja	Otkrivanje računala u mreži	Topologija	Ocjenjivanje slabosti	Rješenja za uklanjanje slabosti
Network Mapper	Brzo	Moguće	Detaljan prikaz	Nedostupno	Nedostupno
Nessus	Sporo	Moguće	Osnovni "traceroute" podaci	Dostupno	Dostupno
Nexpose	Brzo	Ograničeno brojem IP adresa	Nema informacija o topologiji	Dostupno	Dostupno

U stupcu Vrijeme skeniranja u Tablici 1 vidljiva je kratak opis vremena potrebnog za izvršenje skeniranja. Nexpose je najbrže izvršio skeniranje, potrebne su mu bile 4 minute. Network Mapper je prilično blizu s trajanjem skeniranja od 5 minuta. Nessus značajno zaostaje s trajanjem skeniranja od 1 sat i 26 minuta. Vidljivo je značajno odstupanje Nessus-ovog vremena potrebnog da se izvrši skeniranje. Važno je napomenuti da vremena skeniranja u primjerima iz prethodnih poglavlja nisu imala značajno odstupanje od ostala dva programska alata iako su bila sporija.

Network Mapper i Nessus nisu ograničeni brojem IP adresa te se mogu koristiti za detekciju računala i ostalih uređaja koji su na mreži dok Nexpose Community Edition je ograničen na 32 IP adrese.

Network Mapper detaljno opisuje rutu do mete uz koju uključuje RTT, DNS čvora te pripadajuću geolokaciju. Također jedini vizualno prikazuje topologiju. Nessus programski alat u rezultatima prikazuje listu čvorova koji su u ruti te njihove IP adrese. Nexpose ne prilaže informacije vezane za topologiju.

Nessus i Nexpose rangiraju detektirane slabosti po CVSS vrijednostima. Nexpose uz tu vrijednost dodaje vrijednost Risk u koju se uračunava vrijeme proteklo od javne objave slabosti, vrijeme koje slabost postoji na skeniranom računalu te o postojanju programa za iskorištavanje slabosti. Dolazi se do zaključka kako Nexpose ima bolji sustav rangiranja slabosti od Nessus-a, dok Network Mapper nema mogućnost ocjeniti slabost.

Također Nessus i Nexpose imaju mogućnost prilaganja mogućih rješenja za uklanjanje slabosti za razliku od Network Mapper-a. Lista štetnih programa koju Nexpose koristi, omogućuje točnije definiranje slabosti pa i time i točnije predlaganje rješenja za uklanjanje slabosti.

Tablica 2Usporedba alata po detektiranim uslugama i slabostima

Meta	Network Mapper	Nessus	Nexpose
SSH usluga	Detektirana usluga i verzija	Detektirana uslugai verzija	Detektirana usluga i verzija
Slabosti detektirane uz SSH uslugu	Detektirani slabi MAC, CBC i SSH enkripcijski algoritmi	Detektirani slabi MAC, CBC i SSH enkripcijski algoritmi	—
HTTP usluga	Detektirana usluga	Detektirana usluga i verzija	Detektirana usluga i verzija
Slabosti detektirane uz HTTP uslugu	—	—	Detektirano 12 slabosti
NTP usluga	—	Detektirana usluga	Detektirana usluga

U tablici 2 ukratko su prikazani rezultati skeniranja sva tri programska alata. U prvome stupcu su navedene sve slabosti. U sljedeća tri stupca ukratko je opisano da li

je programski alat detektirao uslugu i njezine pripadajuće slabosti. Prvotno je vidljivo da ni jedan alat nije detektirao sve slabosti. Na port-u 22 alati su detektirali SSH uslugu verzije Open SSH 6.6.1. Nexpose nije detektirao korištenje slabih šifranata i algoritama u SSH usuzi. Network Mapper-a i Nessus-a su detektirali slabe algoritme te dolazi do razlike u izlaganju dobivenih rezultata. Nessus je slabe algoritme prepoznao te ih naveo kao najveću opasnost. Network Mapper navodi sve algoritme koji su podržani unutar usluge, ali nema mogućnost prijaviti ih kao slabost.

Sljedeće se prelazi na rezultate vezane za HTTP uslugu na port-u 80. Network Mapper je detektirao postojanje HTTP usluge, ali ne i njezinu verziju. Nessus je detektirao i verziju, ali ne i slabosti vezane uz korištenu verziju. Nexpose ovdje pokazuje veliku prednost. Detektira uslugu i njenu verziju te uz verziju nalazi 12 slabosti. Nadalje uz 12 slabosti prilaže i 2 javno poznata štetna programa koja mogu iskoristiti navedene slabosti. Ovdje Network Mapper i Nessus propuštaju uočiti najveću opasnost vezanu za poslužitelja. Većina slabosti je vezana za Apache verzije 2.4.7 te se one uklanjaju ažuriranjem na verziju 2.4.10. Ažuriranjem uklanjaju postojeće slabosti putem kojih je moguće izvesti DoS napad odnosno prekinut rad poslužitelja.

Zadnja je navedena NTP usluga. Nessus i Nexpose su detektirali NTP uslugu te nisu prijavili nikakve pronađene slabosti. Bitna je razlika što su detektirali postojanje NTP usluge. Daljnjim korištenjem drugih profila skeniranja alati su u mogućnosti saznati više informacija. Razlika je što alat pruža korisniku potrebne informacije za uzimanje daljnjih koraka u zaštiti računalne mreže.[48]

7. Zaključak

Sigurnost računalnih mreža predstavlja dio problematike računalnih mreža koja s povećanjem njihove upotrebe poprima sve veći značaj. Standardni zahtjevi za integritetom podataka, autorizacijom i autentikacijom korisnika su definirani te je cilj osigurati sigurno korištenje računalnih mreža raznim metodama i mehanizmima zaštite. Metode i mehanizmi zaštite se s vremenom mijenjaju i unaprjeđuju kako bi osigurali zaštitu od novih opasnosti koje se svakodnevno pojavljuju te je potrebno ići u korak s novim tehnologijama zaštite računalnih mreža.

Radom je prikazana detekcija slabosti upotrebom programskih alata. Postupak detekcije slijedi postupak uklanjanja slabosti te održavanje sigurnosti.Potrebna je redovita upotreba alata kako bi se održavala razina sigurnosti računalnih mreža. Drugi zahtjev je konstantno unaprjeđenje samih programskih alata i načina na koji oni detektiraju slabosti.

Analizom rezultata dobivenih upotrebom programskih alata dolazi se do zaključka kako ni jedan alat nije detektirao sve postojeće slabosti. Nexpose je jedini detektirao slabost vezanu uz verziju poslužitelja koja predstavlja najveću detektiranu opasnost od sva tri programska alata. Uz detekciju slabosti Nexpose je naveo 12 različitih napada koje je moguće izvesti na poslužitelju što ga stavlja ispred Network Mapper-a i Nessus-a koji su detektirali samo slabosti niže razine.

Sigurnost računalnih mreža je područje kojemu se pridaje sve više pozornosti, ali u praksi često ostane zapostavljeno. Potrebno je povećati svijest društva o potrebi upotrebe programskih alata i ostalih mehanizama za zaštitu računalnih mreža. Ljudski faktor ima bitnu ulogu u sigurnosti računalnih mreža jer nenamjernom pogreškom ili s planiranom štetnom namjerom u mogućnosti je učiniti veliku štetu unatoč svim postavljenim zaštitama. Radom se ukazuje na potrebu korištenja programskih alata i obvezu konstantnog napretka unutar područja kako bi se postigla te održala razina sigurnosti u računalnim mrežama kakvu usluge i korisnici zahtijevaju.

Literatura

[1.] Kavran, Z.; Grgurević, I.: Autorizirana predavanja iz kolega Računalne mreže, Fakultet prometnih znanosti, Sveučilište u Zagrebu, Zagreb, travanj 2016.

[2.] Internetski izvor: http://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm (14.travanj2016.)

[3.] Internetski izvor: https://forrester-infosystems.wikispaces.com/file/view/Ring_topology.jpg/129467917/Ring_topology.jpg (18.travanj2016.)

[4.] Barrett, D., King, T.: Computer Networking Illuminated, Jones and Bartlett Publishers, SAD, 2005.

[5.] Internetski izvor: http://computernetworkingsimplified.com/category-1/network-topologies/what-is-a-star-topology-network/(18.travanj2016.)

[6.] Internetski izvor: http://www.ciss100.com/lecture-topics-modules/networking-internet/network-topologies/ (5. rujan2016.)

[7.] Internetski izvor: http://3.bp.blogspot.com/_Ndsxv_4TBK0/THv0SHDlfCI/AAAAAAAAASU/12kVPmV7fAY/s1600 (5. rujan 2016.)

[8.] Internetski izvor: https://networktopologytutorials101.wordpress.com/(18. travanj2016.)

[9.] Internetski izvor: http://www.ianswer4u.com/2012/05/hybrid-topology-advantages-and.html#axzz46AqdszV7 (18. travanj2016.)

[10.] Bonaventure, O.: Computer Networking: Principles, Protocols and Practice, 2011.

[11.] Tanebaum, A., Wetherall, D.: Computer Networks Fifth Edition, Pearson, SAD, 2011.

[12.] SysTool Inc., Internetski izvor: http://blog.systoolsgroup.com/types-of-networks.html(5. rujan 2016.)

[13.] Intel, Internetski izvor: http://itpeernetwork.intel.com/top-10-reasons-to-setup-a-client-server-network/ (5. rujan 2016.)

[14.] Internetski izvor: http://www.ianswer4u.com/2011/05/p2p-what-is-peer-to-peer.html#axzz46MAWu1aH (20. travanj 2016.)

[15.] Microsoft, Internetski izvor: https://msdn.microsoft.com/en-us/library/windows/desktop/dd433192(v=vs.85).aspx (5. rujan 2016.)

[16.] SecureMac, Internetski izvor: http://www.securemac.com/malware/what-is-malware (5. rujan 2016.)

[17.] Kaspersky Lab, Internetski izvor: http://www.kaspersky.com/internet-security-center/threats/viruses-worms(21. travanj 2016.)
[18.] ESET, Internetski izvor: http://www.virusradar.com/en/glossary/file-viruses(5. rujan 2016.)
[19.] PCtools Symantec, Internetski izvor: http://www.pctools.com/security-news/what-is-a-computer-worm/(21. travanj 2016.)
[20.] Kaspersky Lab, Internetski izvor: https://usa.kaspersky.com/internet-security-center/threats/trojans#.VxkZw0eyfIV (21. travanj 2016.)
[21.] PCtools Symantec, Internetski izvor: http://www.pctools.com/security-news/what-is-adware-and-spyware/(21. travanj 2016.)
[22.] Microsoft, Internetski izvor: https://www.microsoft.com/en-us/security/online-privacy/phishing-symptoms.aspx (22. travanj 2016.)
[23.] Cisco Systems, Internetski izvor: http://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2(5. rujan 2016.)
[24.] Kurose, J., Ross, K.: Computer Networking: A Top-Down Approach – Sixth Edition, Pearson, SAD, 2013.
[25.] Internetski izvor: http://chipdesignmag.com/print.php?articleId=1162?issueId=22(18. svibnja 2016.)
[26.] Peterson, L., Davie, B.: Computer Networks: System Approach – Fifth Edition, Elsevier, SAD, 2012.
[27.] Oracle, Internetski izvor: https://docs.oracle.com/cd/E19798-01/821-1841/bnbxb/index.html (5. rujan 2016.)
[28.] FirewallCX, Internetski izvor: http://www.firewall.cx/networking-topics/the-osi-model/177-osi-layer6.html(5. rujan 2016.)
[29.] FirewallCX, Internetski izvor: http://www.firewall.cx/networking-topics/firewalls.html (5. rujan 2016.)
[30.] Microsoft, Internetski izvor: https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx(5. rujan 2016.)
[31.] Microsoft, Internetski izvor: https://technet.microsoft.com/en-us/library/bb531150.aspx (26. travanj 2016.)
[32.] Cisco Systems, Internetski izvor: http://www.ciscopress.com/articles/article.asp?p=31731&seqNum=5(5. rujan 2016.)
[33.] Network Mapper Internetski izvor: http://nmap.org/book/zenmap.html(29. lipnja 2016.)
[34.] Network Mapper, Internetski izvor: http://nmap.org/book/zenmap-scanning.html (26. lipnja 2016.)
[35.] Network Mapper, Internetski izvor: http://nmap.org/book/man-briefoptions.html(26. lipnja 2016.)
[36.] Network Mapper, Internetski izvor: https://nmap.org/book/man-host-discovery.html(13. srpnja 2016.)
[37.] Network Mapper, Internetski izvor: https://nmap.org/book/zenmap-topology.html (27. srpanj 2016.)

[38.] Dale, C., Internetski izvor: http://www.securesolutions.no/zenmap-preset-scans/(27. srpnja 2016.)
[39.] Network Mapper, Internetski izvor: https://nmap.org/nsedoc/scripts/nbstat.html(27. srpnja 2016.)
[40.] Network Mapper, Internetski izvor: https://nmap.org/nsedoc/scripts/smb-security-mode.html(27. srpnja 2016.)
[41.] Tenable, Internetski izvorhttps://www.tenable.com/plugins/(5. rujan 2016.)
[42.] Tenable, Internetski izvor: https://www.tenable.com/tips/how-to-enable-credentialed-checks-on-unix(2. kolovoza 2016.)
[43.] Rogers, R.: Nessus Network Auditing Second Edition, Elsevier, SAD, 2008.
[44.] Rapid7, Internetski izvor: www.rapid7.com/products/nexpose/editions.jpg (8. srpnja 2016.)
[45.] Rapid7, Internetski izvor: https://help.rapid7.com/metasploit/Content/discovering-validating-vulns/v1/nexpose-scan.html(5. rujan 2016.)
[46.] Network Mapper, Internetski izvor: https://nmap.org/nsedoc/scripts/ssh-hostkey.html(10. kolovoz 2016.)
[47.] Network Mapper, Internetski izvor: https://nmap.org/nsedoc/scripts/ssh2-enum-algos.html(10. kolovoz 2016.)
[48.] National Vulnerability Database, Internetski izvor: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0226(11. kolovoz 2016.)
[49.] Cisco Systems, Internetski izvor: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160603-ntpd(23. kolovoz 2016.)

Popis kratica

Kratica	Značenje kratica
AES	Advanced Encryption Standard, Napredni enkripcijski standard
ARCFOUR	Rivest Cipher 4, Rivest-ov postupak šifriranja 4
ARP	Address Resolution Protocol, Protokol za rješavanje adresa
BEAST napad	Browser Exploit Against SSL/TLS, Napad koji iskorištava slabosti internet preglednika sa SSL/TLS uslugom
CBC	Cipher Block Chaining, Šifriranje blokove poruka po redoslijedu
CredSSP	Credential Security Support Provider, Davatelj podrške za zaštitu korištenjem akreditacije
CTR	Counter Mode, Enkripcijski postupak s upotrebom brojača
CVSS	Common Vulnerability Scoring System, Standardni sustav za ocjenjivanje slabosti
DES	Data Encryption Standard, Standard za enkripciju podataka
DNS	Domain Name System, Ime domene
DoS	Denial of Service, Napad kojime se preopterećuje poslužitelja lažnih zahtjevima
FQDN	Fully Qualified Domain Name, Potpuno ime domene
FTP	File Transfer Prototocol, Protocol Za slanje datoteka
GCM	Galois/Counter Mode, Simetrična enkripcija s upotrebom brojača
HTML	Hypertext Markup Language, Prezentacisjki jezik za izradu internetskih stranica
HTTP	Hypertext Transfer Protocol, Protokol za prijenos teksta

HTTPS	Hypertext Transfer Protocol Secure, Protokol za prijenos teksta sa sigurnosnim dodacima
ICMP	Internet Control Message Protocol, Protokol za kontrolne internetske poruke
IEEE	The Institute of Electrical and Electronics Engineers, Institut inženjera elektrike i elektronike
IP	Internet Protocol, Internet protokol
IPsec	Iternet Protocol Secure, Internet protokol sa sigurnosnim dodacima
LAN	Local Area Network, Lokalna mreža
LM	LAN Manager hash, Upravitelj sažetaka poruka u lokalnim mrežama
MAC address	Media Access Control address, Adresa mrežne kartice
MAC algorithm	Message Authentication Code, Algoritam za autentikaciju poruka
MAN	Metropolitan Area Network, Gradska mreža
MD5	Message Digest Algorithm 5, Algoritam za provjeru poruke 5
MIMO	Multiple Input Multiple Output, višestruki ulazi i višestruki izlazi
NASL	Nessus Attack Scripting Language, Nessus-ov jezik za kreiranje napadačkih skripti
NTLM	Windows New Technology LAN Manager, Windows-ova nova tehnologija za upravljanje sažecima u lokalnim mrežama
NTP	Network Time Protocol, Protokol za mrežno vrijeme
OSI	Open Systems Interconnection model, Model za otvoreno povezivanje sustava
P2P	Peer – to – Peer, ravnopravni odnos
PDF	Portable Document Format, Prenosivi format dokumenta
RFC	Request For Comment, Dokument koji opisuje tehnologije u razvoju

QoS	Quality of Service, kvaliteta usluge
RTT	Round Trip Time, Vrijeme potrebno da signal stigne do odredišta i vrijeme potrebno da potvrda stigne iz odredišta
SCTP	Stream Control Transmission Protocol, Protokol za kontorlu struje podataka
SHA1	Secure Hash Algorithm 1, Sigurni algoritam za sažetke 1
SMB	Server Message Block, Blok poruka poslužitelja
SMTP	Simple Mail Transfer Protocol, Protokol za jednostavno slanje elektroničke pošte
SNMP	Simple Network Management Protocol, Protokol za jednostavno upravljanje mrežom
SSH	Secure Shell, Mrežni protokol za sigurnu komunikaciju preko nesigurne mreže
SSL	Secure Sockets Layer, Standard za sigurno uspostavljanje konekcije
TCP	Transport Layer Security, Sigurnosni protocol transportnog sloja
TLS	Transport Layer Security, Sigurnosni protocol transportnog sloja
TOKEN	Komunikacijski protokol za lokalne mreže s topologijom prstena
UDP	User Datagram Protocol, Protokol za prijenos datagrama
WAN	Wide Area Network, Mreža širokog područja
WEP	Wired Equivalent Privacy, Privatnost jednaka žičnom prijenosu
Wi-Fi	Wireless Fidelity, Bežična lokalna mreža bazirana na 802.11 IEEE standardu
WMI	Windows Management Instrumentation,Windows instrumenti za upravljanje

Popis slika

Slika 1 Shematski prikaz mreže s topologijom sabirnice [2] 4
Slika 2 Prikaz topologije prstena [3] 5
Slika 3 Prikaz topologije zvijezde [5] 6
Slika 4 Prikaz stablaste topologije [7] 6
Slika 5 Prikaz mreže s isprepletenom topologijom [7] 7
Slika 6 Prikaz mreže sa kombinacijom više vrsta mreže [8] 8
Slika 7 Prikaz odnosa MAN i LAN mreža [12] 10
Slika 8 Primjer mreže sa poslužiteljem i korisnicima[13] 11
Slika 9 Primjer mreže sa ravnopravnim korisnicima [14] 12
Slika 10 Prikaz komunikacije koristeći simetrični ključ[25] 17
Slika 11 Početno sučelje Network Mapper-a 23
Slika 12 Unos naredbe za otkrivanje čvorova u mreži 26
Slika 13 Prikaz topologije 27
Slika 14 Detalji računala 28
Slika 15 Naredbe korištene za detaljno skeniranje računala 29
Slika 16 Rezultati skeniranja 30
Slika 17 Rezultati skripti - NetBIOS 31
Slika 18 Rezultati skripti - Domena 31
Slika 19 Početno sučelje Nessus 34
Slika 20 Otkrivanje uređaja na mreži koristeći Nessus 34
Slika 21 Odgovor na ARP ping 35
Slika 22 Akreditacije korištene u Advanced Scan 36
Slika 23 Rezultat skeniranja Advanced Scan 37
Slika 24 Popis detektiranih slabosti rangiranih po opasnosti 38
Slika 25 Opis slabosti 38
Slika 26 Ispis izvora slabosti 39
Slika 27 Isključeno digitalno potpisivanje 40
Slika 28 Sučelje Nexpose Community Edition 41
Slika 29 Odabir profila skeniranja 42
Slika 30 Prikaz pronađenih slabosti 43
Slika 31 Pojavljivanje Diffie - Hellman slabih šifranata 44

Slika 32 Grafički prikaz pronađenih slabosti 45
Slika 33 Korištene naredbe za skeniranje pomoću Network Mapper-a 46
Slika 34 Otkriveni port-ovi 47
Slika 35 Informacije vezane za "otisak prsta" javnog ključa poslužitelja 47
Slika 36 Dio otkrivenih algoritama korištenih u SSH usluzi 48
Slika 37 Lokacija skenirane mete 49
Slika 38 Put do mete označen u skokovima u mreži 49
Slika 39 Rezultat WhoIS skripte 50
Slika 40 Rezultat skeniranja programskog alata Nessus 51
Slika 41 Slabi enkripcijski algoritmi u upotrebi 51
Slika 42 Slabi CBC algoritmi u upotrebi 52
Slika 43 Slabi MAC algoritmi u upotrebi 53
Slika 44 Opis slabih algoritama za autentikaciju poruka 53
Slika 45 Rezultat skeniranja Nexpose programskim alatom 54
Slika 46 Popis detektiranih slabosti 54
Slika 47 Popis programa za iskorištavanje detektiranih slabosti 55
Slika 48 Detektirane usluge 56

Popis tablica

Tablica 1 Usporedba alata po općim karakteristikama 57
Tablica 2 Usporedba alata po detektiranim uslugama i slabostima 58

METAPODACI

Naslov rada: Analiza programskih alata za sigurnostračunalnih mreža

Student: Ivan Miškulin

Mentor: doc. dr. sc. Ivan Grgurević

Naslov na drugom jeziku (engleski):

Analysis of Software Tools for Computer Networks Security

Povjerenstvo za obranu:

- Prof. dr. sc. Zvonko Kavran predsjednik
- Doc. dr. sc. Ivan Grgurević mentor
- Siniša Husnjak, mag. ing. traff. član
- Izv. prof. dr. sc. Dragan Peraković zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta uZagrebu

Zavod: Informacijsko – komunikacijski promet

Vrsta studija: preddiplomski

Studij: Promet

Datum obrane diplomskog rada: 13. rujna 2016.

Sveučilište u Zagrebu
Fakultet prometnih
znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na **objavljenu literaturu što pokazuju korištene bilješke i bibliografija.**

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz **necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.**

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj **visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.**

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada **pod naslovom** **Analiza programskih alata za sigurnost računalnih mreža**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom **repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.**

Student/ica:

U Zagrebu, 29.08.2016. **Ivan Miškulin**

(potpis)