Landeka, Hrvoje

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:387585

Rights / Prava: Attribution 3.0 Unported / Imenovanje 3.0

Download date / Datum preuzimanja: 2025-03-20



Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository





SVEUČILIŠTE U ZAGREBU FAKULTET ORGANIZACIJE I INFORMATIKE V A R A Ž D I N

Hrvoje Landeka

IDENTIFIKACIJA RANJIVOSTI OPERACIJSKIH SUSTAVA

ZAVRŠNI RAD

Sisak, 2022.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

VARAŽDIN

Hrvoje Landeka

Matični broj: 0016115482 (S-43634)

Studij: Primjena informacijske tehnologije u poslovanju

IDENTIFIKACIJA RANJIVOSTI OPERACIJSKIH SUSTAVA

ZAVRŠNI RAD

Mentor:

Prof. dr. sc. Ivan Magdalenić

Sisak, lipanj 2022.

Hrvoje Landeka

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Identifikacija ranjivosti operacijskih sustava je postupak kojim su u radu pomoću detekcijskih alata za tu namjenu provedena testiranja i skeniranja sigurnosne analize u svrhu prevencije i zaštite od zlonamjernih napada. U radu su primijenjeni alati: Nmap/Zenmap, Microsoft Baseline Security Analyzer (MBSA) i DNSdumpster. Testiranja i skeniranja su provedena u kontroliranom okruženju na domeni foi.hr preko računala autora, te IP adrese, OS Windows 10 i Linux Ubuntu 20.04. LTS instaliranih na računalo unutar virtualnog stroja Virtualbox 6.1. Metodologija rada je unaprijed predefinirana osnovnim postavkama i konfiguracijama alata, programskih paketa koji su preuzeti i korišteni u radu. Izvještaji i rezultati skeniranja preuzeti su iz korištenih programskih alata koji automatski generiraju izvještaje koji pružaju jasan uvid na potencijalne rizične faktore, konfiguracijsko sigurnosne propuste i opasnosti iz perspektive napadača. Postupak skeniranja na sva tri alata je uspješno izveden sa svim fazama koji su sa rezultatima testiranja i skeniranja prezentirani su u radu.

Ključne riječi: Operacijski sustavi, MBSA, Nmap/Zenmap, Dnsdumpster, analiza sigurnosti operacijskog sustava, testiranje ranjivosti OS.

Sadržaj:

1. Uvod	1
2. Metode i tehnike rada	2
3. Ranjivosti operacijskih sustava	3
3.1. Potencijalne opasnosti i rizici	3
3.2. Nmap/Zenmap	3
3.2.1. Postupak skeniranja alatom Nmap/Zenmap	4
3.3. Microsoft Baseline Security Analyzer (MBSA)	11
3.3.1. Opis i svrha alata	11
3.3.2. Postupak i rezultati analize	12
3.4. Dnsdumpster	16
3.4.1. Svrha i koncept alata	16
3.4.2. Postupak i rezultati skeniranja	17
4. Zaključak	19
5. Literatura	20
Popis slika	21

1. Uvod

Naslov teme završnog rada je: "Identifikacija ranjivosti operacijskih sustava". Tema je značajna iz razloga jer su testiranja i analize ranjivosti operacijskih sustava ključni faktori ranog, preventivnog otkrivanja potencijalnih prijetnji i rizika kojima su operacijski sustavi danas izloženi. Preventivno i rano otkrivanje može smanjiti ili pak potpuno zaustaviti zlonamjerne napade što s druge strane omogućuje nesmetani, neprekinuti rad operacijskog sustava i značajne uštede financija i vremena potrebnog za saniranja šteta zlonamjernih napada. Redovita sigurnosna skeniranja i analize su u doba današnjih virtualnih prijetnji i opasnosti postale nužna osnova sigurnosnih sustava za manje i veće poslovne organizacije, javne ustanove i privatne korisnike. Ugledna i eminentna tvrtka za područja istraživanja IT-a, Gartner, navodi u svojim izvješćima i istraživanjima [1] kako će 2023. godine, šteta prouzročena hakerskim napadima dosegnuti financijsku štetu od 50 milijardi dolara uz dodatne oblike štete kao što su krađa i uništavanje podataka, krađa intelektualnog vlasništva, izgubljena produktivnost, troškovi sanacija napada i drugi oblici šteta koje nanose zlonamjerni hakerski napadi. Iz navedenih razloga tema ovog rada je motivirana namjerom da prezentira kako teorijski, tako i praktičnim radom nekoliko postupaka sigurnosnih provjera, analiza i skeniranja kroz više programskih alata i aplikacija koji su korišteni u radu.

2. Metode i tehnike rada

Pristup izrade rada proveden je u tri faze. Prva faza je teorijsko upoznavanje sa samom materijom teme, ranjivosti operacijskih sustava zatim se u drugoj fazi rada prezentiraju alati koji su korišteni. Preuzete su informacije i podaci sa službenih stranica koji prezentiraju rad, svrhu i koncepte alata. Završna treća faza je izvedba praktičnog dijela skeniranja svakim pojedinim alatom. Za potrebe rada su instalirani programski alati pomoću kojih su odrađena skeniranja i analize na odabranim metama koje su za potrebe rada bile osobno računalo i OS (autora), te uz prethodni dogovor i odobrenje mentora, domena Fakulteta organizacije i informatike Varaždin: foi.hr. Odabrani alati u radu su: Nmap/Zenmap GUI, Dnsdumpster i Microsoft Baseline Security Analyzer 2.2 (MBSA). Sigurnosne provjere i postupci skeniranja provedeni na računalu autora rada unutar OS Windows 10, te u virtualnom okruženju na OS Linux/ Ubuntu 20.04. LTS distribuciji koja ja pokrenuta u programskom okruženju virtualnog stroja Oracle Virtualbox 6.1.

3. Ranjivosti operacijskih sustava

3.1. Potencijalne opasnosti i rizici

Najkritičnija i najrizičnija točka ranjivost OS-a dolazi od strane Interneta. Potencijalni napadači, zlonamjerne osobe, hakeri koji napadaju i kompromitiraju operacijske sustave koriste različite sofisticirane metode najčešće putem zlonamjernog i štetnog softvera (eng. Malware) kojim neovlašteno kompromitiraju resurse OS-a, baze podataka, povjerljive poslovne, financijske informacije, datoteke, lozinke itd. Ciljevi su im različiti no temeljno se mogu klasificirati u tri kategorije hakera. Takozvani Crni hakeri (eng. black hat) koji su ujedno i najrazorniji. Posjeduju visoku razinu znanja, vještina i opreme koje koriste u ilegalne aktivnosti provala i ilegalnih upada u sustave radi uništenja resursa OS-a, krađu identiteta, prisluškivanje, financijske malverzacije, špijunažu, kibernetičke napade i sl. Suprotno Crnim hakerima, na isti način i vrlo sličnom metodologijom djeluju Bijeli hakeri (eng. white hat) koji rade legalno i zakonito za tvrtke koje na tržištu nude tzv. etičko hakiranje, ali uz dozvolu i dopuštenje korisnika svojih usluga kojima penetracijskim testiranjima pružaju uvid u ranjivosti, opasnosti i rizične slojeve mreže. OS-a i cjelokupnom informatičkom sustavu tvrtke ili računala pojedinca. Sivi hakeri (eng. gray hat) su treća skupina koja radi kombiniranim načinom crnih i bijelih hakera, ali ilegalno bez znanja i odobrenja sustava i osoba koje napadaju s najčešćim motivom stjecanja financijske koristi ili javnog eksponiranja manipulacijom ukradenih povjerljivih podatka [2]. Najzloglasniji i najrasprostranjeniji zlonamjerni softveri (eng. Malware) su Virusi, Trojanski konj i Crvi.

3.2. Nmap/Zenmap

Nmap je (eng. *Open Source*) prema opisu na službenim stranicama [3] programski paket, a sam naziv Nmap izveden je od engleske skraćenice: *Network Mapper*. Zenmap je grafičko sučelje (eng. *Grafic User Interface* - GUI) Network Mapper-a koji primarno olakšava sam rad početnicima, no isto tako na raspolaganju mogućnosti i opcije koje su namijenjene iskusnijim korisnicima. Projektiran je prvenstveno za rad na skeniranju velikih mreža, ali jednako je efikasan i učinkovit pri skeniranju samo jednog hosta. U svom radu Nmap koristi IP pakete kojima se pronalazi i specificira koji su hostovi dostupni na mrežama, zatim koje su aplikacije, programski paketi, operacijski sustavi, vatrozid aktivan na skeniranom hostu. Kako se navodi u opisu i specifikaciji na službenim web stranicama, Nmap je najčešće

korišten za sigurnosni nadzor i skeniranje, međutim sistemski administratori ga preporučuju i koriste za uvide u mrežni inventar, upravljanje vremenom nadogradnje servisa, nadgledanja (eng. *Uptime)* računala ili servisa, odnosno ukupnog vremena rada računala ili mreže. Krajnji ishod pretraživanja, skeniranja Nmapa je popis skeniranih meta sa informacijama koje su strukturirane ovisno o postavljenim parametrima pretrage i skeniranja. Najvažniji podatak je sadržan u tablici portova u kojoj je ispisan broj porta i protokola, naziv servisa i stanje. Uz primarni izvještaj tablice portova, alat nudi i neke dodatne informacije o računalu, DNS imena, koji je operativni sustav u pitanju, te tipove uređaj i MAC adrese. Dobro je istaknuti kao osobitu pogodnost i prednost za korisnike da su detaljna uputstva dostupna na više svjetskih jezika, uključujući i hrvatski [4] što uvelike olakšava pristup i sam rad korisnicima bez obzirna na kojoj su razini informatičkih znanja.

3.2.1. Postupak skeniranja alatom Nmap/Zenmap

Instalacija programskog paketa Nmap/Zenmap GUI je vrlo jednostavna, brza i korisnički pristupačna (eng. *User Friendly*). Sam postupak instalacije na OS Windows 10 traje svega nekoliko minuta. Instalacija na virtualno okruženje, OS Linux/Ubuntu 20.04. unutar virtualnog stroja Oracle Virtualbox 6.1. (preuzet sa službenih stranica Oracle za potrebe rada) je također vrlo brza i jednostavna uz nekoliko konfiguracija unutar instalacijskih postavki i raspakiranja unutar Linux Terminala nakon čega je GUI Zenmap dostupan na Desktopu.

Na samom početničkom sučelju izbornika dostupan je unos mete skeniranja u koji unosimo domenu ili IP adresu, zatim se rezultati skeniranja prezentiraju u pet glavnih klasifikacijskih stavki: Nmap ispis, Portovi/računala, Topologija, Detalji računala, Skeniranja (slika 1). U svrhu rada, skenirana je domena: foi.hr, kao mrežno mjesto, te IP adresa osobnog računala (autora rada) unutar OS Linux/Ubuntu distribuciji na GUI kao i na Ubuntu Terminalu.



Slika 1. Korisničko sučelje Nmap/Zenmap GUI na OS Windows 10 nakon skeniranja.

Na slici 1 u polju "Target" (Meta) upisana je domena foi.hr koja je skenirana. U polju "Profil" u početnim postavkama predefinirana je opcija: "Intense scan". Dostupno je polje za naredbe, te mogućnost odabira računala ili servisa. Obzirom kako su portovi najranjivija mjesta i točke na računalu, tako će se za u ovom radu primarno i u fokusu prikazati rezultati skeniranja portova.

💕 Ubuntu [Pokrenuto] - Oracle VM VirtualBox		_	
Activities 🗢 Zenmap 🔻	Jun 12 16:24	. ·	(>) +Î ▼
	Zenmap		o 😣
Scan Tools Profile	Help		
Target: foi.hr	▼ Profile: Intense scan ▼	Scan	Cancel
Command: nmap -T4	-A -v foi.hr		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans		
OS Host 👻		-	Details
0			
A			
Filter Hosts			



Nmap skenira d 1600 TCP portova na računalu. U izvještaju se ne prikazuje stvarno stanje već ono što Nmap prepoznaje. Pod stavkom - Portovi/Računala - konfigurirani su sjedeći parametri: otvoreni, zatvoreni, filtrirani, nefiltrirani, otvoreni/filtrirani, zatvoreni/filtrirani. Ova klasifikacija izvještaja se odnosi na sljedeća značenja:

Otvoreni – aplikacija prihvaća TCP konekcije i UDP pakete što je omogućuje neometano testiranje, odnosno prikaz otvorenih portova koji nisu zaštićeni vatrozidom. Ovaj podatak je posebno bitan je su otvoreni portovi ujedno i potencijalno meta napadača. Iz istih podataka o otvoreni portovima doznajemo koji servisi i aplikacije su dostupi na mreži.

Zatvoreni – zatvoreni port je dostupan i odgovara na Nmap upit, ali nema aplikacije. Ova konfiguracija može pomoći u otkrivanju verzije OS. Administratori nastoje onemogućiti pristup ovakvim portovima pomoću vatrozida ili paketa filtera koji su interpretirani u nastavku, odnosno kategoriji – filtrirani.

Filtrirani – u ovom slučaju Nmap ne može otkriti je li port otvoren ili zatvoren jer su upiti prema portu blokirani (postavke rutera, vatrozida, paket filter) s toga Nmap mora poslati više uzastopnih upita kako bi se precizno utvrdilo postavljanje filtera. Ovaj postupak će dodatno usporiti skeniranje.

Nefiltrirani – ova klasifikacija, oznaka znači da je port dostupan, ali Nmap ne može ustanoviti jeli port otvoren ili zatvoren. U ovom slučaju postoje druge metode i skenovi koji mogu dati odgovor jeli port otvoren ili zatvoren.

Otvoreni/filtrirani – karakteristika ovog stanja je da Nmap ne može ustanoviti jeli port otvoren ili filtriran. Ovo stanje se aktivira kada upit ne dobiva nikakav povratni odgovor.

Zatvoreni/filtrirani – kada Nmap ne može ustanoviti jeli port zatvoren ili filtriran, identificirati će ga ovim stanjem.

👁 zenmap.exe			\times
Informacije o naredb]		
Naredba:	nmap	-T4 -A -v	foi.hr
Nmap inačica:	7.92		
Razina opširnosti:	1		
Razina debugiranja:	0		
Opće informacije			
Počeo je:	sviba	nj 26, 2022	- 15:10
Završio je:	sviba	nj 26, 2022	- 15:15
Aktivna računala:	1		
Neaktivna računala:	0		
Skenirana računala:	1		
Otvoreni portovi:	3		
Filtrirani portovi:	646		
Zatvoreni portovi:	351		
🖃 Informacije o skenira	inju - S	Syn	
Tip skeniranja:	syn		
Protokol:	tcp		
# skeniranih portova	a: 1000)	
Servisi:			~

Slika 3. Sažeti izvještaj o skeniranju foi.hr domene.

Iz ovog sažetka (Slika 3) izvještaja o skeniranoj domeni foi.hr doznajemo informacije o naredbi: nmap -T4 - A- v foi.hr, te opće informacije o točnom vremenu početka i završetka skeniranja. Ono što je važnije i interesantnije da je sken odrađen u TCP protokolu u opsegu od 1000 skeniranih portova. 351 port je zatvoren, 3 porta su otvorena i 646 portova je filtrirano. U izvještaju Nmap/Zenmap GUI skena portova na računalu (autora) pomoću IP adrese, ali na OS Linux/Ubunutu dobiju se sljedeći rezultati prikazani na slici 4. Nmap/Zenmap GUI nakon završetka skeniranja nudi opciju generiranja izvještaja u XML datoteci.

🏏 Ubuntu [Pol	krenuto]	- Oracle V	'M Virtu	alBox							-		×
Activities	G	ର୍ସ୍ Image	View	er 🔻		Jun	11 19:57				*	4))	Î -
	Q	88%		€	Screenshol	t from 20	22-06-11 18	-56-38.png	S			ō	8
	Acti	vities	С Т	erminal	T		Jun 11 18:5	6			A	4 0 +[•
		ſ				hrvoje	@hrvoje-Virt	ualBox: ~	Q				8
		Sta Nma Hos Oth Noth POR 22/ 80/ 443 Nma	voje@l arting ap sca st is ner ac c show t c show t c show t c p d c p d or d or d or d or d or d or d or d	hrvoje g Nmap an rep up (0 ddress wn: 99 STATE open open open ne: 1 hrvoje	-VirtualBox:-{ 7.80 (https: ort for foi.hr .055s latency) es for foi.hr 7 filtered por SERVICE ssh http https IP address (1 -VirtualBox:-{	<pre>\$ nmap fd ://nmap.c r (161.5:). (not sca rts host up; \$ gnome.s</pre>	oi.hr org) at 20 3.120.251) anned): 200 scanned f screenshot	022-06-11 1 01:b68:1408 ln 16.71 sea	3:55 (:f01::	:EST 15:c00	91		
?													
>_	-												
::::		•											



🍟 Ubuntu [Poki	renuto] - Oracle	VM VirtualBox						- 🗆 ×
Activities	enmap 🔻			Jun 13	15:25		💦 📣 + 🗋 👻	
6	Firefox	Web Browser			Zen	map		- a 😣
	Scan Io	Pronte	Неір					
	Target:	192.168.43.2	00		 Profile: 	Intenses	scan	▼ Scan Cancel
	Comman	d: nmap -T4	-A -v 1	92.168.43	.200			
	Hosts	Services	Nma	p Output	Ports / Hosts	Topolog	gy Host Details	Scans
	05	Uast		Port	Protocol	State	Service	Version
	os	HOSE	\bigcirc	135	tcp	open	msrpc	Microsoft Windows RPC
\mathbf{O}		192.108.43.2	\bigcirc	139	tcp	open	netbios-ssn	Microsoft Windows nett
			\bigcirc	445	tcp	open	microsoft-ds	
			×	880	tcp	filtered	unknown	
			\bigcirc	5357	tcp	open	http	Microsoft HTTPAPI http
			×	8089	tcp	filtered	unknown	
Â			ж	32773	tcp	filtered	sometimes-rpc9	
?								
:::								
•••	Filter	r Hosts						

Slika 5. Prikaz rezultata skena Porta/Hosta IP adrese na OS Linux/Ubuntu

<mark>7</mark> Ubuntu [Pokrenuto] - Oracle VM VirtualBox	—		\times
Activitie	s 🗈 Terminal 🔫 Jun 11 19:56	*	(•
	Image: Float in the second		ō	×
	<pre>hrvoje@hrvoje-VirtualBox:~\$ nmap -sP 192.168.43.200 Starting Nmap 7.80 (https://nmap.org) at 2022-06-11 19:54 CEST Note: Host seems down. If it is really up, but blocking our ping p n</pre>	robes,	, try	- P
	Nmap done: 1 IP address (0 hosts up) scanned in 3.01 seconds hrvoje@hrvoje-VirtualBox:~\$ nmap -Pn 192.168.43.200 Starting Nmap 7.80 (https://nmap.org) at 2022-06-11 19:55 CEST Nmap scan report for 192.168.43.200			
	Host is up (0.0087s latency). Not shown: 994 filtered ports PORT STATE SERVICE 135/tcp open msrpc			
	139/tcp open netbios-ssn 445/tcp open microsoft-ds 1433/tcp open ms-sql-s 1972/tcp open intersys-cache			
?	5357/tcp open wsdapi Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds hrvoje@hrvoje-VirtualBox:~\$ gnome-screenshot			
•	nrvojegnrvoje-vtrtuatbox:~\$			
::::				



💕 Ubuntu [Pokrenuto] - Oracle VM VirtualBox		- 🗆 🗙
Activities 🔷 Zenmap 👻	Jun 13 15:24	₽ ● →
	Zenmap	- 🕫 😣
Scan Tools Prof	ile Help	
Target: 192.168.4	43.200 ▼ Profile: Intense scan ▼ S	can Cancel
Command: nmap	-T4 -A -v 192.168.43.200	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS Host 👻	nmap -T4 -A -v 192.168.43.200	Details
 Eilter Hosts 	<pre>Scanning 192.168.43.200 [4 ports] Completed Ping Scan at 15:23, 0.12s elapsed (1 tot hosts) Initiating Parallel DNS resolution of 1 host. at 15 Completed Parallel DNS resolution of 1 host. at 15 1.01s elapsed Initiating SYN Stealth Scan at 15:23 Scanning 192.168.43.200 [1000 ports] Discovered open port 445/tcp on 192.168.43.200 Discovered open port 139/tcp on 192.168.43.200 Increasing send delay for 192.168.43.200 from 0 tc to 13 out of 31 dropped probes since last increase Increasing send delay for 192.168.43.200 from 5 tc to max_successful_tryno increase to 5 Warning: 192.168.43.200 giving up on port because retransmission cap hit (6). Discovered open port 5357/tcp on 192.168.43.200</pre>	al 5:23 5:23, 5 due 10 due
Filter Hosts		

Slika 7. Izvještaj Nmap/Ispis za IP adresu na OS Windows 10.

💴 Ubuntu (P	krenutol - Orac	le VM VirtualBox		— П X
Activitie			Jun 12 16:51	 ▲ ●) •∭ ▼
	, 2	chingp	Zenman	
	Scan To	ols Profile	Help	
	Scall 10	ots Frome		
	Target:	foi.hr	Profile: Intense scan	Scan Cancel
	Command	d: nmap -T4	I-A -v foi.hr	
	Hosts	Services	Nmap Output Ports / Hosts Topology Host Details Sca	ns
	OS H	Host	Hosts Viewer Fisheye Controls	gend Save Graphic
	🧶 f	oi.hr (161.5		
			T foi.hr (161.53.12	20.251)
\mathbf{A}			Gateway Jocalhost	
?				
		_		
	Filter	Hosts		

Slika 8. Prikaz topologije foi.hr na OS Linux/Ubuntu.

🔡 Ubuntu [Pokr	renuto] - Oracle VM VirtualBox				\times
Activities	🗢 Zenmap 🔫	Jun 13 15:28	<i>.</i> ?。 <	» + İ	-
(1)	Firefox Web Browser	Zenmap Help		đ	8
	Target: 192.168.43.2	00 Profile: Intense scan	Scan	Can	cel
	Command: nmap -T4	-A -v 192.168.43.200			
	Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans			
	OS Host	Hosts Viewer Fisheye Controls Legend	Save C	Iraphi	c
0	192.168.43.2				
Á		↓ Julia 192.168.43.200 _gateway ● localhost			
?					
	Filter Hosts				



.

3.3. Microsoft Baseline Security Analyzer (MBSA)

3.3.1. Opis i svrha alata

Microsoft Baseline Security Analyzer (MBSA) je alat podržan na OS Windows. Prilično je jednostavan alat namijenjen sigurnosnoj analizi i skeniranju ranjivosti jednog ili više računala. Instalacija programskog paketa se provodi u vrlo jednostavnom i brzom postupku kroz instalacijski Wizard. Radna konzola alata i početno korisničko sučelje je vizualno kvalitetno riješeno po pitanju dostupnosti, preglednosti naredbi i samog pokretanja rada, odnosno skeniranja. Za pokretanje skeniranja potrebno je unijeti IP adresu ciljanog računala ili više njih, te posjedovati administratorske ovlasti koje će program zatražiti kako bi mogao započeti proces skeniranja i rada. Nakon završetka skeniranja, MBSA automatski generira izvještaje koje korisnik može odmah pogledati, pohraniti ili printati. Svrha i rad alata se bazično može podijeliti u dvije kategorije. Koristan je u provjeri grešaka u konfiguraciji sustava Windows, te provjeri sigurnosnih postavki. Izvještaj nakon završetka analize generira podatke o administrativnim ranjivostima, zatim ranjivostima poslužitelja, snazi lozinki, SQL ranjivost te sigurnosnu ranjivosti. Alat je potpuno besplatan. vrlo koristan, brz, učinkovit i jednostavan za rad početnicima kao administratorima sigurnosnih postavki naprednijih znanja za rad na sustavima sa više računala. Aktualna verzija MBSA 2.2. uključuje i podržava 64-bitnu instalaciju. Skeniranja se mogu provesti preko komandnog retka (eng. Command Prompt) ili preko grafičkog sučelja alata. Alat MBSA ima iznimno pozitivnu konfiguraciju da nakon generiranja rezultata skeniranja i sigurnosne provjere, korisniku odmah nudi mogućnost, savjete korigiranja pogreški, nedostataka kao i stručnu pomoć i savjetovanje preko službenih Microsoft stranica koje su linkovima trenutno i odmah na raspolaganju korisniku iz radne konzole samog alata [5]. U nastavku su neki od rezultata skeniranja prikazani kroz fotografije (eng. Screenshot).

3.3.2. Postupak i rezultati analize

🎒 Microsoft Baseline Security Analyzer 2.2	
👀 🔮 Baseline Secur	ity Analyzer
Which computer d	o you want to scan?
Enter the name of the computer	or its IP address.
<u>C</u> omputer name:	GROUP\DESKTOP-6KEE3CJ × V (this computer)
IP address:	
Security report name:	%D% - %C% (%T%)
Options: Check for Windows adm Check for weak passwo Check for IIS administration Check for SQL administration Check for security upda Configure computer Advanced Update S Scan using Assi Scan using Micr Scan using Micr Scan using Micr	%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address inistrative vulnerabilities ative <u>vulnerabilities</u> rative vulnerabilities ates rs for Microsoft <u>Update</u> and scanning prerequisites Services <u>options</u> : gned Windows Server Update Services(WSUS) servers only osoft Update only ne catalog only
Learn more about Scanning	g Options



AN N	e secondy ranary	izer 2.2	- 0
U	^{Aicrosoft} Baseline	Security Analyzer	Micro
	Details for ity assessment inplete Scan (C	r WORKGROUP - DESKTOP-6KEE3CJ (2022-05-12 15:41:59)	
omputer P address iecurity re ican date: icanned w iatalog sy	name: 8 eport name: 9 ith MBSA versi 9 nchronization o	WORKGROUP/DESKTOP-8/EE3C1 192,168,56,1 WORKGROUP-0ESKTOP-4/EE3C1 (12.05.2022, 15-41) 12.05.2022, 15-41 12.05.2022, 15-10 6 date: Security updates scan not performed	
ort Order: ecurity U	Score (worst fire	st) 🗸	
Score	Issue	Result	
! /indows !	Security Updates Scan Results	Carnot load security CAB file. How to correct this	
l Vindows :	Security Updates Scan Results ative Vulnerabi	Carnot load security CAB file. How to correct this Illities	
lindows : Administra Score	Security Updates Scan Results ative Vulnerabi Issue Automatic	Carnot load security CAB file. How to correct this liftices Result The Automatic Lipdates system service is not configured to be started as Automatic.	
l Vindows : Administra Score	Security Updates Scan Results ative Vulnerabi Issue Automatic Updates Local Account	Carrot load security CAB file. How to correct this Inters Result The Automatic Updates system service is not configured to be started as Automatic. What was scanned how to correct this Correct and correc	
I Administra Score	Security Updates Scan Results ative Vulnerabit Issue Automatic Updates Local Account Password Test	Carnot load security CAB file. How to correct this illutes Result The Automatic Updates system service is not configured to be started as Automatic. Virbat was scarned File to be correct this Some user accounts (or 5) have bank or simple passwords, or could not be analyzed. Watar was scarned New to correct this	
Indows Administra Score	Security Updates Scan Results ative Vulnerabi Issue Automatic Updates Local Account Password Test Password Expiration	Carnot load security C48 file. How to correct this illutes Illutes Result The Automatic Updates system service is not configured to be started as Automatic. What was scanned How to correct this Some user accounts (5 of 5) have bank or simple assistoria, or could not be analyzed. What was scanned Result details — Note to correct this Some user accounts (6 of 5) have non-expiring passwords, or What was scanned Result details — Note to correct this	
Indows : Administra Score	Security Updates Scan Results ative Vulnerabi Issue Automatic Updates Local Account Password Test Expiration Incomplete Updates	Carnot lad search y CAB file. How to correct this	
Indows Administra	Security Updates Scan Results ative Vulnerabi Issue Automatic Updates Local Account Password Test Password Test Password Test Password Test Password Test Password Test Password States Windows Sceneral	Carnot load searify C48 file. How to correct this	
I findows s Administra Score 2 0 0 0 0 2 2	Security Updates Scan Results ative Vulnerabi Issue Automatic Updates Local Account Password Test Password Test Password Test Password Expiration Incomplete Updates Windows Firewall File System	Carnot load security C48 file. How to correct this	
I findows : Administra Score I I I I I I I I I I I I I I I I I I I	Security Updates Scan Results ative Vulnerabi Issue Local Account Desaword Test Password Test Password Test Password Expiration Incomplete Updates Windows Freeval File System	Carrol to de seaurly CAB file. How to correct this	
I findows : Administra Score 2 0 0 0 0 2 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Security Updates Scan Results attive Vulnerabil Issue Load Account Password Test Password Test Passw	Carbon Los de sacrity CAB Rie. How to correct the	

Slika 11. Glavni izvještaj alata nakon postupka skeniranja.

	C Dubern	ine Security Analyz	ler ZZ	- 0	×
@	ê'	Microsoft Baseline	Security Analyzer	Microso	oft
	Ø	Autologon	Autologon is not configured on this computer.		
	۷	Guest Account	What was suffred		
	۷	Restrict	Vinat was survived Computer is properly restricting anonymous access.		
	Ø	Administrators	what was scanned No more than 2 Administrators were found on this computer. What was scanned Result details		
A	dditiona	al System Inform	ation		
	Score	Issue	Result		
	0	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.		
	0	Services	No potentially unnecessary services were found.		
	0	Shares	S share(s) are present on your computer.		
	0	Windows Version	Computer is running Microsoft Windows Unknown. What was scanned		l
Int	ternet	Information Se	rvices (IIS) Scan Results		
	Score	Issue	Result		
		IIS Status	IIS is not running on this computer.		
De	sktop	Application Sca	n Results		
A	dministi	trative Vulnerabili	ttes		
	Score	Issue	Result		
	Ø	IE Zones	Internet Explorer zones have secure settings for all users.		
		Macro Security	No supported Microsoft Office products are installed.		
					~
Brint t	his repor	rt	👔 Copy to doboard 💿 Previous security report View security report		
				OK	

Slika 12. Drugi dio glavnog izvještaja rezultata skeniranja.

Microsoft Bas	seline Security Analyzer 2.2		
00 🖁	Baseline Sec	urity Analyzer	
	Scanning	Downloading security update information from Microsoft	

Slika 13. Prikaz procesa skeniranja u grafičkom sučelju.

lows lectio	firewall is enabled and has exceptions.	ns configured. Windows Fir	ewall is enabled on all network
ult Det	ails		
nectio	ns listed without a score do not have	Windows Firewall capabilitie	s.
			Company Manage
Score	Connection Name	Firewall	Exceptions
Score	Connection Name All Connections	Firewall On	Programs, Services
Score	Connection Name All Connections Ethernet	Firewall On On	Programs, Services Programs*, Services*
Score	Connection Name All Connections Ethernet Local Area Connection	Firewall On On On	Programs, Services Programs*, Services* Programs*, Services*
Score	Connection Name All Connections Ethernet Local Area Connection VirtualBox Host-Only Network	Firewall On On On On	Programs, Services Programs*, Services* Programs*, Services* Programs*, Services*

Slika 14. Izvještaj o mrežnim konekcijama i vatrozidu.

-

 \times

📄 Microsoft Baseline Security Analyzer -- Webpage Dialog







Slika 16. lzvještaj o aktivnim diskovima na računalima

—

3.4. DNSdumpster

3.4.1. Svrha i koncept alata

DNSdumpster je *Open Source* okvir, alat koji distribuira respektabilna tvrtka Hacker Target (www.hackertarget.com) koja zastupa svoje usluge na tržištu od 2007. god [6]. Skeneri ranjivosti tvrtke Hacker Target obrađuju milijune IP adresa godišnje. Kako se navodi na službenim Internet stranicama tvrtke [7], polazišna vizija i cilj je podizanje svijesti o vrijednosti sigurnosnih rješenja otvorenog koda. Alat DNSdumpster je dostupan u više modula i korisničkih opcija, a za potrebe rada korištena je besplatna osnovna, *Basic* konfiguracija. Složenije verzije i konfiguracije koje se nazivaju PRO u ponudi, zahtijevaju naprednije razine znanja i naplaćuju se. U sažetoj, jednostavnoj interpretaciji sa službenih stranica [7], alat služi za istraživanje domena i otkrivanje hostova povezanih s domenom. Sigurnosna procjena i provjera se provodi pronalaženjem vidljivih hostova iz perspektive napadača alatima za skeniranje sigurnosnih ranjivosti otvorenog koda i alatima za mrežnu inteligenciju. Korisničko sučelje i radna konzola, dostupna je i na hrvatskom jeziku. Rezultate skeniranja, DNSdumpster automatski generira kao izvještaj u Excel datoteci koju je moguće preuzeti.



Slika 17. Početna stranica i korisničko sučelje DNSdumpster.

3.4.2. Postupak i rezultati skeniranja

Za potrebe izrade završnog rada i u sklopu obavljanja stručne prakse, alatom DNSdumpster, skenirana je domena foi.hr. Alat je identificirao GeoIP lokacije, u slučaju foi.hr domene uz hrvatsku, uključena je i Njemačka i Nizozemska, gdje se nalaze hostovi povezani sa serverom Fakulteta. Detaljniji izvještaj o tome prikazan je u Excel datoteci.





Kroz automatski generirani izvještaj u Excel datoteci dostupan je detaljan uvid u rezultate sigurnosnog skeniranja. Izvještaj je raspoređen po stavkama. Na prvome mjestu je naziv Hosta, zatim IP adresa, DNS i dalje, prema preostalima stavkama liste (slika 19).

			· ·		-		v			-
1	Hostname 🗾	IP Address 🛛	T v	Reverse DNS 🛛 👻	Netblock Owner 🛛 👻	Country	Tech / Apps 🛛 🔻	HTTP / Title 🛛 🔽	HTTPS / Title 🛛 🔽	FTP / SSH / Telnet 🛛 🔽
	venera.foi.hr	31.147.204.111	Α	venera.foi.hr	CARNET-AS J.Marohnica 5, 10000	Croatia	IIS,8.0	Microsoft-IIS/8.0		rdp: Remote Desktop (3389)
					Zagreb		ASP.NET	title: Microsoft Internet		
2								Information		
	athena.foi.hr	161.53.120.227	Α	athena.foi.hr	CARNET-AS J.Marohnica 5, 10000	Croatia				
					Zagreb					
3										
	bbb2.foi.hr	161.53.120.24	Α		CARNET-AS J.Marohnica 5, 10000	Croatia		nginx	nginx	ssh: SSH-2.0-OpenSSH_7.6p1
					Zagreb				title: 307 Temporary Redirect	Ubuntu-4ubuntu0.5
4									CN: bbb.foi.hr	
	loki2.foi.hr	161.53.120.233	Α	loki2.foi.hr	CARNET-AS J.Marohnica 5, 10000	Croatia				
-					Zagreb					
5										
	oss2.foi.hr	161.53.120.29	Α	oss2.foi.hr	CARNET-AS J.Marohnica 5, 10000	Croatia				
					Zagreb					
6										
	1.0.0			1. 16.1	CARDIER AN ANY ANY ANY ANY ANY ANY ANY ANY ANY					

Slika 19. Primjer izvještaja rezultata skeniranja foi.hr domene u Excel datoteci.

19].fo1.hr. 3 +)	188.166.38.33 nsl.foi.hr	DIGITALOCEAN-ASN Netherlands
ns2.foi.hr. G - 가 겨 추 : 종 💠	161.53.120.10 ns2.foi.hr	CARNET-AS J.Marohnica 5, 10000 Zagreb Croatia
ns3.foi.hr. 3 • 7 * * • • •	161.53.120.11 ns3.foi.hr	CARNET-AS J.Marohnica 5, 10000 Zagreb Croatia
X Records ** This is where email f	for the domain goes 18.196.56.200	AMAZON-02
Ⅲ ≭ ⊚ 	mail2.foi.hr	Germany
10 barok.foi.hr. ∰ ズ ⊗ ∲	161.53.120.3 barok.foi.hr	CARNET-AS J.Marohnica 5, 10000 Zagreb Croatia
10 barok.foi.hr. ■ 本 ◆ ◆ XT Records ** Find more hosts in S	161.53.120.3 barok.foi.hr Sender Policy Framework (SPF) configurations	CARNET-AS J.Maronnica 5, 10000 Zagreb Croatia
10 barok.foi.hr. ■ ★ ● ◆ XT Records ** Find more hosts in 3 "google-site-verification=CwP2okx_"	161.53.120.3 barok.foi.hr Sender Policy Framework (SFF) configurations YKxxfyNKaRhdfptOzsqoiU9tY05z5Mc0F2c*	CARNET-AS J.Maronnica 5, 10000 Zagreb Croatia
10 barok.foi.hr. # X © XT Records ** Find more hosts in 1 "google-site-verification=CwP2okx_" "google-site-verification=1PrmaNpD;	161.53.120.3 barok.foi.hr Sender Policy Framework (SPF) configurations YKxxfyNKaRhdfptOzsqoiU9tY05z5MCoF2c" 14r4v8182NuwkDCwGod4mwK8-Jayx57DYYQ"	CatMer-AS J.Maronnica 5, 10000 Zagreb Croatia

Slika 20. lzvještaj skeniranja hostova na domeni foi.hr.

4. Zaključak

U današnjem vremenu brzog razvoja informacijskih tehnologija kao i njihova primjena, odnosno brža i sveobuhvatnija integracija u gotovo sve segmente gospodarstva, društva i načina modernog života zahtjeva visoke sigurnosne protokole. Taj brzi sveobuhvatni razvoj i integracija IT-a, nezaobilazno prati i porast negativnih trendova kao što su prijetnje kibernetičkoj sigurnosti, porast Internet kriminala i hakerskih aktivnosti u raznim oblicima i namjerama. Navedene okolnosti zahtijevaju i nameću sve veće, više standarde pružanja i omogućavanja sigurnosti kako velikih korporativnih organizacija, raznih gospodarskih subjekata, javnih ustanova čije poslovanje se oslanja na velike mrežne i serverske sustave, ali isto tako i zaštitu pojedinca, individualnog korisnika računala koje ima integrirani OS i pristup Internetu. Alati prezentirani u ovom radu kao Nmap/Zenmap, Dnsdumpster i Microsoft Baseline Security Analyzer, samo su mali dio ponude takvih alata kao i pozitivnog trenda u kojem vodeće globalne IT kopanije i korporacije pružaju svojim korisnicima mogućnost vlastitog, samostalnog i valja naglasiti, besplatnog u osnovnim slojevima, usluge skeniranja OS, sigurnosne preglede i analize vlastitih računala kao i pristup Internetu, snagu lozinki i sl. Koristi i benefiti ovakvih Open Source alata su iznimno velike i značajne, posebno u vidu pomoći i lakog (eng. User Friendly) pristupa korisnicima s manjim i osnovnim, početničkim informatičkim znanjima koji mogu potpuno besplatno i u svega nekoliko minuta provjeriti osnovne, bazične sigurnosne konfiguracije vlastitog računala i operacijskog sustava, pristup Internetu, potencijalne opasnosti ili propuste, snagu lozinki iz perspektive potencijalnog napadača i sl. Navedene usluge su brzo i lako dostupne u većem opsegu besplatne. Instalacija programskih paketa ne zahtjeva velike memorijske kapacitete OS-a. Pristupačne su i korisnicima početnicima s manjim, ali i korisnicima s većim opsegom znanja. Pitanje sigurnosti pristupa Internetu kao i zaštita osobnih podatka, privatnosti svakog individualnog korisnika kao i nužna osnovna razina informatičkih znanja se postale neizostavan dio opće kulture suvremenog načina života uključujući i poslovno informacijsku sigurnost velikih gospodarskih subjekata koji u slučaju zlonamjernih napada trpe goleme gubitke. Navedeni sigurnosni izazovi i znanja korištenja ovakvih alata postaju imperativ u prevenciji rizika, potencijalnih opasnosti i ranjivosti OS-a.

5. Literatura

- [1] <u>https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we</u> [Pristupano: 23.05.2022.]
- [2] Luka, Ljubičić [2020.] Master's thesis/Diplomski rad. Repozitorij Fakulteta organizacije i informatike, Varaždin. [Na Internetu]. Dostupno: Dabar. <u>https://urn.nsk.hr/urn:nbn:hr:211:231137</u> [Preuzeto: 24.05.2022.]
- [3] <u>https://nmap.org/zenmap/</u> [Pristupano: 25.05.2022.]
- [4] <u>https://nmap.org/man/hr/man-briefoptions.html</u> [Pristupano: 25.05.2022.]
- [5] <u>https://support.microsoft.com/hr-hr/topic/microsoftovo-sigurnosno-savjetovanje-kumulativno-a%C5%BEuriranje-za-activex-ubiti-bits-40285e45-6bbe-e1e4-c770-9215c876030a</u> [Pristupano: 11.05.2022.]
- [6] <u>www.hackertarget.com</u> [Pristupano: 21.05.2022.]
- [7] <u>www.dnsdumpster.com</u> [Pristupano: 21.05.2022.]

Popis slika

Slika 1. Korisničko sučelje Nmap/Zenmap GUI na OS Windows 10 nakon skeniranja	5
Slika 2. Početno korisničko sučelje Nmap/Zenmap na Linux/Ubuntu	6
Slika 3. Sažeti izvještaj o skeniranju foi.hr domene	7
Slika 4. Sken foi.hr domene u Terminalu Linux/Ubuntu	8
Slika 5. Prikaz rezultata skena Porta/Hosta IP adrese na OS Linux/ubuntu	8
Slika 6. Skeniranje IP adrese u Terminalu Linux/Ubuntu	9
Slika 7. Izvještaj Nmap/Ispis za IP adresu na OS Windows 10	9
Slika 8. Prikaz topologije foi.hr na OS Linux/Ubuntu	10
Slika 9. Topologija za IP adresu na OS Linux/Ubunutu	10
Slika 10. Početno korisničko sučelje MBSA	12
Slika 11. Glavni izvještaj alata nakon postupka skeniranja	12
Slika 12. Drugi dio glavnog izvještaja rezultata skeniranja	13
Slika 13. Prikaz procesa skeniranja u grafičkom sučelju	13
Slika 14. lzvještaj o mrežnim konekcijama i vatrozidu	14
Slika 15. Izvještaj o lozinkama	15
Slika 16. Izvještaj o aktivnim diskovima na računalima	15
Slika 17. Početna stranica i korisničko sučelje DNSdumpster	16
Slika 18. GeoIP lokacije domene foi.hr	17
Slika 19. Primjer izvještaja rezultata skeniranja foi.hr domene u Execl datoteci	17
Slika 20. Izvještaj skeniranja hostova na domeni foi.hr	18