TRACCIA TASK 03/12/24

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:

- OS fingerprint.
- Syn Scan.
- TCP connect trovate differenze tra i risultati della scansioni TCP connect e SYN?
- Version detection.

E la seguente sul target Windows:

OS fingerprint.

TASK 03/12/24

Configurazione di Rete

Metasploitable: 192.168.50.101
Windows 10: 192.168.50.102

• Macchina Kali Linux (Nmap): 192.168.50.100

Scansioni Richieste

Metasploitable (192.168.50.101)

OS Fingerprint: Determinare il sistema operativo

nmap -O 192.168.50.101

Motivazione:

Il flag -O consente di identificare il sistema operativo del target analizzando le risposte ai pacchetti inviati.

```
(Nalie Rali)-[~]

Symmap -0 192.168.50.101

Starting Nmap 7.945VM ( https://nmap.org ) at 2024-12-03 08:23 EST

Nmap scan report for 192.168.50.101

Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open sch

23/tcp open telnet

25/tcp open smtp

53/tcp open domain

80/tcp open http

111/tcp open retbios-ssn

445/tcp open microsoft-ds

512/tcp open exec

513/tcp open microsoft-ds

512/tcp open microsoft-ds

512/tcp open microsoft-ds

512/tcp open shell

1099/tcp open mirgistry

1524/tcp open ingreslock

2049/tcp open ingreslock

2049/tcp open ingreslock

2049/tcp open mirgistry

1524/tcp open cycroxy-ftp

3306/tcp open mysql

5432/tcp open postgresql

5900/tcp open vnc

6000/tcp open vnc

6000/tcp open vnc

6000/tcp open uknown

MAC Address: 08:00:27:A5:A5:B4 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

S CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

Syn Scan: Eseguire una scansione con pacchetti SYN

nmap -sS 192.168.50.101

Motivazione:

Il flag -sS che invia pacchetti TCP con il flag SYN impostato per iniziare una connessione.

```
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 08:24 EST
Nmap scan report for 192.168.50.101
Host is up (0.0043s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
139/tcp open microsoft-ds
512/tcp open microsoft-ds
512/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open nfs
2121/tcp open postgresql
5900/tcp open ync
6000/tcp open vnc
6000/tcp open vnc
6000/tcp open irc
8009/tcp open unknown
MAC Address: 08:00:27:A5:A5:B4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

TCP Connect Scan: Confrontare i risultati con la Syn Scan

nmap -sT 192.168.50.101

Motivazione:

II flag -sT utilizza il normale processo di connessione TCP (3-way handshake).

Confronto con Syn Scan:

TCP Connect Scan (-sT)

Descrizione: La TCP completa il processo di handshake per ogni porta aperta, il che la rende più affidabile ma meno discreta.

SYN Scan (-sS)

Descrizione: La SYN invia solo pacchetti SYN e non completa l'handshake. È più veloce e stealth rispetto alla TCP Connect Scan.

Confronto tra i principali risultati

Porte:

 Entrambi i metodi rilevano le stesse porte aperte su Metasploitable, confermando che non ci sono porte aggiuntive rilevate da un metodo rispetto all'altro.

Prestazioni:

- La SYN Scan è significativamente più veloce rispetto alla TCP Connect Scan...
- La TCP Connect Scan richiede più tempo perché completa le connessioni.

Log del target:

- La TCP Connect Scan lascia tracce nei log del target perché stabilisce connessioni complete.
- La SYN Scan è meno rilevabile perché interrompe la connessione prima di completare l'handshake.

Version Detection: Identificare le versioni dei servizi attivi

nmap -sV 192.168.50.101

Motivazione:

Il flag -sV consente di identificare i servizi attivi sulle porte aperte e di rilevare le loro versioni.

```
| Ckali@ kali) - [~]
| Sudo mmap - 5V 192.168.50.101
| Starting Nmap 7.945VN (https://nmap.org ) at 2024-12-03 08:28 EST
| Nmap scan report for 192.168.50.101
| Host is up (0.00048s latency).
| Not shown! 0.90048s latency).
| Not shown! 0.977 closed tcp ports (reset)
| PORT STATE SERVICE VERSION |
| 21/tcp open ftp vsftpd 2.3.4 |
| 22/tcp open ssh OpenSSH 4.7p1 Debian Bubuntu1 (protocol 2.0) |
| 23/tcp open stell Linux telnetd |
| 25/tcp open smtp Postfix smtpd |
| 25/tcp open domain ISC BIM 9.4.2 |
| 80/tcp open domain ISC BIM 9.4.2 |
| 80/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 1445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 151/tcp open netbios-ssn Samba smbd 3.X -
```

Windows 10 (192.168.50.102)

OS Fingerprint: Determinare il sistema operativo

nmap -O 192.168.50.102

Motivazione:

Il flag -O consente di identificare il sistema operativo del target analizzando le risposte ai pacchetti inviati.

```
P kali)-[~]
nmap -0 192.168.50.102

Nmap 7.94SVN (https://nmap.org ) at 2024-12-03 08:28 EST
report for 192.168.50.102
p (0.000895 latency).
: 981 closed tcp ports (reset)
STATE SERVICE
open echo
open discard
open dyd
open dytime
open qotd
open chargen
open http
open msrpc
open microsoft-ds
open microsoft-ds
open msmq
open zephyr-clt
open eklogin
open ms-wbt-server
open wsdapi
open ms-wbt-server
open ajp13
open http-proxy
open http-salt
ss: 08:00:27:CE:EE:C4 (Oracle VirtualBox virtual NIC)
pe: general purpose
Microsoft Windows 10
pe:/o:microsoft:windows_10
s: Microsoft Windows 10 1507 - 1607
istance: 1 hop

ion performed. Please report any incorrect results at https://nmap.org/si:
1 IP address (1 host up) scanned in 2.65 seconds
```

Report in HTML

Metasploitable (192.168.50.101)

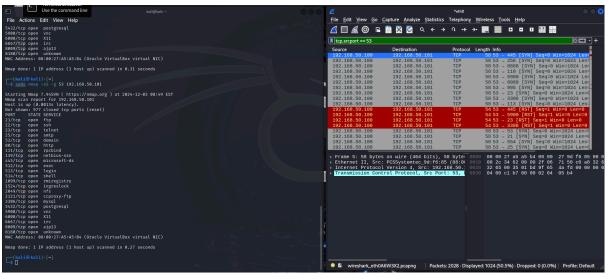
Nmap Sca	Report - Scanned at Tue Dec 3 08:30:	41 2024					
	mary 192.148.20.101	·······					
Scan Summa	Y						
Western G. Drivel	Colonia Series I (N. 1) 6 201 oli Tene apprenti. A sal mangandan passara (N. 166 kili 181						
	c106.11.04.2005; 1.9 abbrev() had appeared in 34.25 worsh.						
192,148,50,1	31						
######################################	F (part) MAN - Clade Woodfiles at last WC (res)						
N7 participal	dhá ná dean bha amhráin d ead Ioladh mai l						
Part I	No.	Militage to a p. March.	Rendon Fo	Spread .	Product vilipsi	25.5 25.5	Misside
		Impan, IP light allower (FP rate 29)					
		TO September 19 HE LIST SEE SEE SEE SEE SEE SEE SEE SEE SEE S					
		Company of the Compan					
		call before two, so in it plant opp within 8 h.h swapp, fair, dealer had of state.				6.ht fetter Barriel	minute.
22	No. Considery	per an electrical and the Contract of the cont	w.	sprak	OperAM	6.7pl Satter Behrald	princi 2 d
21 28	9	gen gen	lated unity	tyrak tyrak	Linux Heridal Ricilla sotipal		
		201 D RESS SHARING S. Procurer No.					
	areas	Salgoti comerimentalisi ken insulaminingerioritekantiliki/satelehoriteskanflare is se set titig sahide Uicantrjiaantii da citiz tehan 196 til 1954 dil da citiz den 200 til 1954 dil					
	and	Stock regarded Stock St.					
		GCL, SCL, SCL, SCPL with Mrc, Str., Str., Str., Mrc, Str., Str., Str., SCL, STL, et. CK, SCPL with Mrc, Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Str., Str., Mrc, Str., Str., Str., Str., Str., Str., Str., Str., Str., Str., Mrc, Str.,					
	edicorrent.	TO THE DESIGNATION OF SHARES, WITH SHARES, WITH, FIRST, STATE OF, PROSECULATIONS, SETTINGS, ON					
KX .		gen.	desir	sprak	NEWS	942	
MD		Mild care face (LL)	100	Served.	Ambridge	224	Abricani
	North Street	Mosphradd - Una					
111		Spatic E.E. (Sturin) 56(5)	netred	seret.		1	MF (100MB)
	polis	Table Tabl					
		MAN ALL MAN AL					
		MALE LOS SERVICE COMPANY					
100			refine so:	seret.	Nederold .	33-14x 33.37-04um	webynap VORCROF
600 813	1	igen igen	resident van reside Segen Segen Segen oppmå paker trat stordyself	sprak sprak	Norderword Norderword rottin-do-ment (rottin-do-ment) (quittin-do-ment)	33.200cm	welsynsp VCRCRCLP
100 1000	2	4m 4m	interestation of the control of the	spread spread	Silk Clauseth growinging Silk Clauseth growinging Manageth growing to delice		
739 446 813 814 938 938 938 217 228	10	= = = = = = = = = = = = = = = = = = =	indicate ide.	cyrob cyrob cyrob cyrob cyrob cyrob cyrob cyrob cyrob cyrob		94 131 147 March 1	MPC COOKING
YES	Se S	The state of the s	med .	spread	N/G	ASSTr Model	
		Natural II (in hand) Institute (in hand) Institute (in the control of the control					
		Sales Adaptive Consider the Constant of the Co				840-847	
100	n) or i	spen. Adjoint connections between the local description of the connection of the co	bridgest	spreak	Religions DR	A16-A17	
	n/ core	Security Security Comments (Security Security Se					
HER		pm	w	sprak	wc		print 1.1
		National constant 5.1 Secretary again. of Collectional Coll.					
MARKET MARKET	to to	um um	XII is	spreak spreak	United No.		amand
		com 1 in which the second seco					
		server for Anteglished n. (8) service conscil. A. S. i. in Anteglished n. (8) selver 8 (ap. 80.00)					
		teatro front (Implies Appare America III propr Chicky (Int. Santon) (St. St. St. St. St. St. St. St. St. St.					
ALTER ST		spec. Miled to get a solid regions for the IPTSK region.	pH		Aportal bary		Related vi.1
H160	No.	spec Specier Search S.A.	Mb	sprad	Apade Sireal/Cryste Stiffengere	11	
	Nipranse tealer	Species Copyring C. S.					
Beneda Special	ng System Detection						
Medical B	(App Dates) Nat (Ameri) Nat (Ameri) Nat (Ameri) Nat Add - Add (Methy)						
Real Birtyl Gul	ref						
Marigit Phones arrives allegately		Militar Mate 16-20 Series					
		Compare Contract And Relation's Contract And Relation's Contract C					
untransactly read		personal payer great authorities attack that is come and the property of the come of the come and the property of the come of the companion, that default)					
chaleshow		more Staffe, desires Staffe, ander in					
chall-three rintal		SHEEK van HISPATING, SHEEK van valoren, SHEEK HO valoren (edese)					
onit time		Protect regelation falled (MIC)					
OLD US							

Windows 10 (192.168.50.102)

Nmap Scan	Report - Scanned at Tue Dec 3 08:32:16 2024						
Scan Summary							
Sear Total Concession of	ded at No Dec 1 19, 12 19, 2021 with those arguments of mediantity comment PE 2 MARTING						
Water Street	**						
Stop are d Series 1	(86, 96, 11, 2004), 1. Production (1 had up) control in 176.76 cannots.						
192.169.50.102							
Address							
, 190.146.86.100	(m.f.) (m.f.) - Dealer Maralline votat MC (mm.)						
Perts	Ol - Date Walking or Lat MC (mar)						
	nal rail description controlled a should						
Water	with most						
Port	te.	Mildings and protection	erio dumi	Operation operat	Pedal	Western	Moster
	lip .	-	duced	oprodit			
27	to to	em em	digitine spiral disagen	opradi opradi	Phone Vindon Versional define Union qui		Bylo
14		40°	No.	seral.	Plantal Tit Nipal	100	
	Nipranariasia	Normalis (19) SAA					
	Mydia	Ti dinte.					
	Mp-rethols	Netetially risig witnes: 1967					
278	To .	_	regis.	openia.	Planted Virolant IPC		
60	lo lo	un un	melitar van melitar van merapi merapi merapi	openia.	Plannel Vindom reliza von Straken 11 Pro 1010-record vin		witpour 109000.F
2000	io io	spen spen	mana maya	opnaž opnaž	Plant Vision PC		
578 578 690 5905 2008 2008 2008 2008	8	in the second se	Major Major	oproadi oproadi oproadi oproadi oproadi oproadi oproadi	Montel Vinion, IPC Montel Vinion, IPC		
E SAN	No.	spen	richitatur	Sprain .			
		201 2 RES RESIDENCE IN Free some file.					
	agradionals.	Compt. Sect. 1974-129 (1924) Intelligible Companies Sect. 1974-1974 (19					
		No. Companies Asset. SECULO NA SECU					
		Product Service: IA.A. SASA Spring Their IARS of MYST SURGANIA					
	sinati	Service and Servic					
MIRO	No.	spec Sente (martiste	Mp	speak	Manual MTMM rojul	2.3	XXXXX
	Myremen health						
		Normalis (ENV), Q.A.					
SARES RECORD	to to	Norwalth 1978/07/2,3 spen spen	profused spit	oyendi oyendi	Apole Spec		Page 0.1
	No No spreshab	Riveral VERICLS open open spen fallet in get a suite trapene for the SPSB report					Reservit
HERE HERE	to to	Normalis 1939(1).2 assess sees sees fulfills to get a utilist require for the SPSS require sees	progrand up:11 May	oproals oproals	Back Sec Aprile SeculSpick SM regre	15	Maurich 1
	No.	Minuserh (1990).2.4 see files file				13	Read CT
	Бр Бр прочиблай. Бр Мунфектургану	Record (1997) 2				12	Admin.51
	Ne N	Record (1995) a serior (1995) a serior (1995) a confider regione for the SPIDIS Region Serior (1995) a confider regioner for the SPIDIS Region Serior (1995) a confiderative regions Serior (1995) a				ы	Masset
100	No.	Homan (1992) A Well We	Mp	quad			Reserved
	Ne N	Record (1995) a serior (1995) a serior (1995) a confider regione for the SPIDIS Region Serior (1995) a confider regioner for the SPIDIS Region Serior (1995) a confiderative regions Serior (1995) a				15	Nese/3
H20	Marie Operation All properation All p	Amount of Michigan Michigang and other and the Amilian and Amilian Michigang and other and the Amilian and Amilian Michigang and and amilian Michigang and and amilian Michigang a	Mp	quad		13	MARKET
H20	No of the second	Amendments The part of the month of print depart May part of the month of print depart May part of the month of print depart May part of the month of the mon	Mp	quad		1.5	Marie (1)
H20	Marie Operation All properation All p	Amount of Michigan Michigang and other and the Amilian and Amilian Michigang and other and the Amilian and Amilian Michigang and and amilian Michigang and and amilian Michigang a	Mp	quad		1.5	Marcol
N00		Amendments The part of the month of print depart May part of the month of print depart May part of the month of print depart May part of the month of the mon	Mp	quad		1.0	Manufi
Next Specialis	The second secon	Amendments The part of the month of print depart May part of the month of print depart May part of the month of print depart May part of the month of the mon	Mp	qual		15	Maret
sees	The second secon	Amendments The part of the month of print depart May part of the month of print depart May part of the month of print depart May part of the month of the mon	Mp	qual		и	Manufi
Manualta Operating Designed Sites Designed Sites Designed Sites	We will be a second of the sec	Amendments The part of the month of print depart May part of the month of print depart May part of the month of print depart May part of the month of the mon	Mp	qual		ш	Maret
Name of Space of the Control of Space of the Control of Space of the Control of t	The second secon	Name of the Control o	Mp	qual		u	Maret
Manualta Operating Designed Sites Designed Sites Designed Sites	The second secon	Amount of the Control	Mp	qual			Manufi
Manualla Operation Designal Sites Operation Sites Operation Sites Operation Sites Stand Bengli Galge Manual Stand Standard Standard Standard Standard Standard Standa	Section 1 Sectio	The contract of the contract o	Mp	qual		u	Maret
Name of Space of the Control of Space of the Control of Space of the Control of t	Section 1 Sectio	The contract of the contract o	Mp	qual			Maret
Memoria Operation Designed Sites	Section 1 Sectio	The contract of the contract o	Mp	qual			Manufi
Section Special Section Sectio	Section 1.	Name of the Control o	Mp	qual			Manert
Benefit Speciality of the Committee of t	Section 1	Manufacture of the Part of the	Mp	qual			Maner
Section Special Section Sectio	Section 1	Manufacture of the Part of the	Mp	quad			Manufi
Benefit Speciality of the Committee of t	The second secon	Here of the Control o	Mp	quad		W	Maners
Sees Sees Sees Sees Sees Sees Sees Sees	The second secon	Here of the Control o	Mp	quad		O.	Manufi
Remain Special	Section 1	The second secon	Mp	quad		u	Maret
Sees Sees Sees Sees Sees Sees Sees Sees	Section 1	Here of the Control o	Mp	quad		U	March

EXTRA TASK 03/12/24

Comando con l'opzione -g



sudo nmap -sS -g 53 192.168.50.101

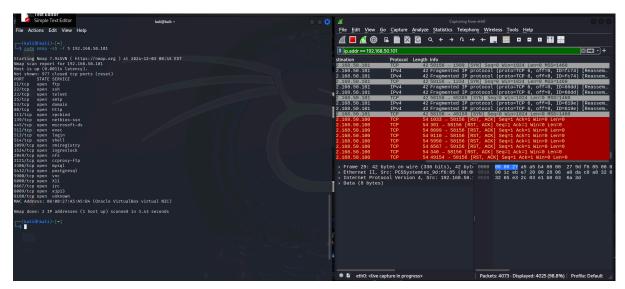
Effetto di -g:

- L'opzione -g specifica la porta sorgente per i pacchetti TCP generati da Nmap.
- Nel caso specifico, ho impostato la porta 53, simulando traffico DNS per cercare di aggirare firewall o IDS che considerano i pacchetti provenienti da porta 53 come affidabili.

Wireshark:

- Nei log di Wireshark, il campo Source Port per i pacchetti SYN inviati da Nmap è impostato a 53, come specificato nel comando.
- Il traffico viene identificato correttamente come TCP con porta sorgente 53.
- Alcune porte del target rispondono con RST (Reset), segnalando che il servizio non accetta connessioni, mentre altre rispondono con SYN-ACK per indicare che sono aperte.

Comando con l'opzione -f



sudo nmap -sS -f 192.168.50.101

Effetto di -f:

- L'opzione -f frammenta i pacchetti IP generati da Nmap, rendendo più difficile per firewall e IDS analizzare il traffico.
- Questa tecnica tenta di eludere controlli di sicurezza che si basano sull'ispezione dei pacchetti completi.

Wireshark:

- Wireshark mostra chiaramente pacchetti IP frammentati, riconoscibili dal campo
 Fragment Offset nel protocollo IP.
- I servizi sulle porte aperte rispondono ai pacchetti frammentati con SYN-ACK, indicando che la frammentazione non ha ostacolato la comunicazione.

Differenze nei risultati

Opzione -g:

Tutte le porte aperte rilevate sono uguali rispetto a una scansione standard SYN (-sS), ma l'uso di una porta sorgente personalizzata (53) può eludere firewall configurati per consentire il traffico DNS.

Opzione -f:

La frammentazione dei pacchetti non influisce sul rilevamento delle porte aperte. Tuttavia, aumenta il numero totale di pacchetti inviati e può richiedere più risorse per il riassemblaggio lato target.