Report UNIT 3 WEEK 9

Threat Intelligence & IOC

Impostazione indirizzi IP macchina Kali e Meta su rete interna per replicare il file scaricato.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3c:17:99
          inet addr:192.168.200.150  Bcast:192.168.200.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3c:1799/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:185 errors:0 dropped:0 overruns:0 frame:0
          TX packets:213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13419 (13.1 KB)  TX bytes:17148 (16.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.200.100  netmask 255.255.255.0  broadcast 192.168.200.255
        inet6 fe80::a00:27ff:fec7:e136  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 124  bytes 10816 (10.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3003 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Analizzando il file si può notare un port scanning eseguito tramite “**TCP connect scan**”, ovvero stabilendo una connessione TCP completa con la porta di destinazione per determinare se la porta è aperta o chiusa. Inviato un pacchetto **SYN**, si attende la risposta del server. Se la risposta è **SYN/ACK** la porta viene considerata aperta, altrimenti viene considerata chiusa (**RST**). Si può notare come le porte non siano filtrate per mancata configurazione firewall lato server.

12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=6424(
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=6424(
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=6424(
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=6424(
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=6424(
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Wir
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=
27	36.775141273	192.168.200.150	192.168.200.100	TCP	74	21 → 41182 [SYN, ACK] Seq=0 Ack=1
28	36.775174048	192.168.200.100	192.168.200.150	TCP	66	41182 → 21 [ACK] Seq=1 Ack=1 Win=

13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=6
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1

Comparando i risultati con un port scanner (nmap) vado ad analizzare la differenza tra le diverse scan ed i risultati riportati da nmap.

-sV

In una **scansione -sV** nmap invia pacchetti SYN che variano a seconda del protocollo e del servizio associato sulla porta (TCP e UDP). Il servizio in ascolto sulla porta riceve il pacchetto e può rispondere con una risposta standard, un banner di benvenuto o ignorare il pacchetto. In seguito, viene registrato il risultato dell'identificazione della versione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80,443 192.168.200.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-28 08:54
mass_dns: warning: Unable to determine any DNS servers. Reve
specify valid servers with --dns-servers
Nmap scan report for 192.168.200.150
Host is up (0.0023s latency).

PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
443/tcp closed https

Service detection performed. Please report any incorrect res
```

```
192.168.200.100  192.168.200.150  TCP   74 35744 → 443 [SYN] Seq=0 Win=64
192.168.200.150  192.168.200.100  TCP   74 80 → 60092 [SYN, ACK] Seq=0 Ac
192.168.200.150  192.168.200.100  TCP   60 443 → 35744 [RST, ACK] Seq=1 A
192.168.200.100  192.168.200.150  TCP   66 60092 → 80 [ACK] Seq=1 Ack=1 W
192.168.200.100  192.168.200.150  TCP   66 60092 → 80 [RST, ACK] Seq=1 Ac
192.168.200.100  192.168.200.150  TCP   74 60100 → 80 [SYN] Seq=0 Win=642
192.168.200.150  192.168.200.100  TCP   74 80 → 60100 [SYN, ACK] Seq=0 Ac
192.168.200.100  192.168.200.150  TCP   66 60100 → 80 [ACK] Seq=1 Ack=1 W
192.168.200.150  192.168.200.100  TCP   74 [TCP Retransmission] 80 → 6010
192.168.200.100  192.168.200.150  TCP   66 [TCP Dup ACK 15#1] 60100 → 80
192.168.200.100  192.168.200.150  HTTP  84 GET / HTTP/1.0
192.168.200.150  192.168.200.100  TCP   66 80 → 60100 [ACK] Seq=1 Ack=19
192.168.200.150  192.168.200.100  HTTP  11… HTTP/1.1 200 OK  (text/html)
```

-O

In una **scansione -O** nmap utilizza una combinazione di tecniche, come l'analisi delle risposte a livello di rete, la misurazione dei tempi di risposta e l'analisi delle opzioni IP, per cercare di identificare il sistema operativo corretto.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -p 80,443 192.168.200.150
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-28 08:57 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse
specify valid servers with --dns-servers
Nmap scan report for 192.168.200.150
Host is up (0.00056s latency).

PORT    STATE  SERVICE
80/tcp  open   http
443/tcp closed https
MAC Address: 08:00:27:3C:17:99 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS 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 h
```

```
23 0.953174629   192.168.200.100   192.168.200.150   TCP      70 39953 → 80 [SYN] Seq=0 Win=512 Len=0 MSS=265
24 0.953985487   192.168.200.150   192.168.200.100   TCP      70 80 → 39953 [SYN, ACK] Seq=0 Ack=1 Win=5792 L
25 0.954279763   192.168.200.100   192.168.200.150   TCP      54 39953 → 80 [RST] Seq=1 Win=0 Len=0
26 0.982216455   192.168.200.100   192.168.200.150   ICMP    162 Echo (ping) request  id=0xc64b, seq=295/9985
27 0.982544889   192.168.200.150   192.168.200.100   ICMP    162 Echo (ping) reply    id=0xc64b, seq=295/9985
28 1.008242534   192.168.200.100   192.168.200.150   ICMP    192 Echo (ping) request  id=0xc64c, seq=296/1024
29 1.008605851   192.168.200.150   192.168.200.100   ICMP    192 Echo (ping) reply    id=0xc64c, seq=296/1024
30 1.045481389   192.168.200.100   192.168.200.150   UDP     342 39714 → 38537 Len=300
31 1.045899762   192.168.200.150   192.168.200.100   ICMP    370 Destination unreachable (Port unreachable)
32 1.071948803   192.168.200.100   192.168.200.150   TCP      66 39960 → 80 [SYN, ECE, CWR, Reserved] Seq=0 W
33 1.072341362   192.168.200.150   192.168.200.100   TCP      66 80 → 39960 [SYN, ACK] Seq=0 Ack=1 Win=5840 L
34 1.072377196   192.168.200.100   192.168.200.150   TCP      54 39960 → 80 [RST] Seq=1 Win=0 Len=0
35 1.103378707   192.168.200.100   192.168.200.150   TCP      74 39962 → 80 [<None>] Seq=1 Win=131072 Len=0 W
36 1.135036669   192.168.200.100   192.168.200.150   TCP      74 39963 → 80 [FIN, SYN, PSH, URG] Seq=0 Win=25
```

-sC

In una **scansione -sC** nmap utilizza una serie di script predefiniti (conosciuti come script di default) per eseguire varie attività di rilevamento e identificazione dei servizi. Il contenuto specifico dei pacchetti dipenderà dagli script di default che vengono eseguiti durante la scansione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC -p 80,443 192.168.200.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-28 09:21
mass_dns: warning: Unable to determine any DNS servers. Reve
specify valid servers with --dns-servers
Nmap scan report for 192.168.200.150
Host is up (0.00053s latency).

PORT    STATE  SERVICE
80/tcp  open   http
|_http-title: Metasploitable2 - Linux
443/tcp closed https
```

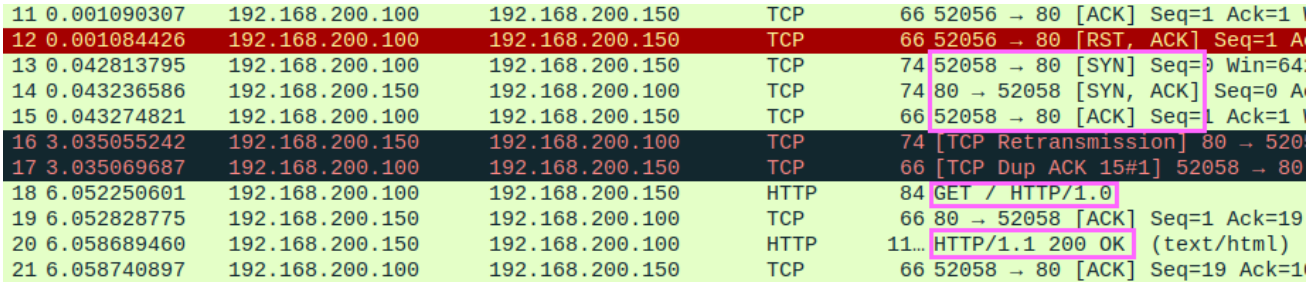
```
39 0.014846442   192.168.200.100   192.168.200.150   HTTP    377 POST / HTTP/1.1  (application/x-www-form-urlencoded)
40 0.015055033   192.168.200.150   192.168.200.100   TCP      74 80 → 42156 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
41 0.015055150   192.168.200.150   192.168.200.100   TCP      66 80 → 42152 [ACK] Seq=1 Ack=312 Win=6912 Len=0 TSval=4
42 0.015090583   192.168.200.100   192.168.200.150   TCP      66 42156 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=33
43 0.015409669   192.168.200.100   192.168.200.150   TCP      74 42162 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
44 0.015468619   192.168.200.100   192.168.200.150   HTTP    234 PROPFIND / HTTP/1.1
45 0.015815648   192.168.200.150   192.168.200.100   TCP      74 80 → 42162 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
46 0.015815678   192.168.200.150   192.168.200.100   TCP      66 80 → 42156 [ACK] Seq=1 Ack=169 Win=6912 Len=0 TSval=4
47 0.015844971   192.168.200.100   192.168.200.150   TCP      66 42162 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=33
48 0.026682351   192.168.200.150   192.168.200.100   HTTP    11… HTTP/1.1 200 OK  (text/html)
49 0.026699539   192.168.200.100   192.168.200.150   TCP      66 42156 → 80 [ACK] Seq=169 Ack=1087 Win=64128 Len=0 TSv
50 0.026862324   192.168.200.150   192.168.200.100   TCP      66 80 → 42156 [FIN, ACK] Seq=1087 Ack=169 Win=6912 Len=0
51 0.027721259   192.168.200.150   192.168.200.100   HTTP    11… HTTP/1.1 200 OK  (text/html)
52 0.027746554   192.168.200.100   192.168.200.150   TCP      66 42152 → 80 [ACK] Seq=312 Ack=1087 Win=64128 Len=0 TSv
53 0.028119481   192.168.200.150   192.168.200.100   TCP      66 80 → 42152 [FIN, ACK] Seq=1087 Ack=312 Win=6912 Len=0
54 0.028584224   192.168.200.100   192.168.200.150   TCP      74 42178 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_
55 0.028769705   192.168.200.100   192.168.200.150   TCP      66 42152 → 80 [FIN, ACK] Seq=312 Ack=1088 Win=64128 Len=
56 0.028940667   192.168.200.150   192.168.200.100   TCP      74 80 → 42178 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=
57 0.028940701   192.168.200.150   192.168.200.100   TCP      66 80 → 42152 [ACK] Seq=1088 Ack=313 Win=6912 Len=0 TSva
58 0.028949854   192.168.200.100   192.168.200.150   TCP      66 42178 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=33
59 0.029386949   192.168.200.100   192.168.200.150   HTTP    219 GET / HTTP/1.1
60 0.029732124   192.168.200.150   192.168.200.100   TCP      66 80 → 42162 [ACK] Seq=1 Ack=154 Win=6912 Len=0 TSval=4
61 0.030186123   192.168.200.100   192.168.200.150   TCP      66 42156 → 80 [FIN, ACK] Seq=169 Ack=1088 Win=64128 Len=
62 0.030269350   192.168.200.100   192.168.200.150   HTTP    229 GET /robots.txt HTTP/1.1
```

-A

Una **scansione -A** (aggressive scan) è un'opzione avanzata che combina diverse tecniche di scansione e rilevamento per fornire un'analisi completa e dettagliata della macchina di destinazione. La scansione -A include il rilevamento del sistema operativo e del tipo di dispositivo (-O), rileva la versione dei servizi (-sV), utilizza script di default (-sC) ed esegue il traceroute (-traceroute) per mappare il percorso di rete tra il computer di origine e la macchina di destinazione.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 80,443 192.168.200.150
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-28 09:57
mass_dns: warning: Unable to determine any DNS servers. Reve
pecify valid servers with --dns-servers
Nmap scan report for 192.168.200.150
Host is up (0.00048s latency).

PORT    STATE  SERVICE VERSION
80/tcp  open   http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
443/tcp closed https
```



11	0.001090307	192.168.200.100	192.168.200.150	TCP	66	52056 → 80 [ACK] Seq=1 Ack=1
12	0.001084426	192.168.200.100	192.168.200.150	TCP	66	52056 → 80 [RST, ACK] Seq=1 A
13	0.042813795	192.168.200.100	192.168.200.150	TCP	74	52058 → 80 [SYN] Seq=0 Win=64
14	0.043236586	192.168.200.150	192.168.200.100	TCP	74	80 → 52058 [SYN, ACK] Seq=0 A
15	0.043274821	192.168.200.100	192.168.200.150	TCP	66	52058 → 80 [ACK] Seq=1 Ack=1
16	3.035055242	192.168.200.150	192.168.200.100	TCP	74	[TCP Retransmission] 80 → 520
17	3.035069687	192.168.200.100	192.168.200.150	TCP	66	[TCP Dup ACK 15#1] 52058 → 80
18	6.052250601	192.168.200.100	192.168.200.150	HTTP	84	GET / HTTP/1.0
19	6.052828775	192.168.200.150	192.168.200.100	TCP	66	80 → 52058 [ACK] Seq=1 Ack=19
20	6.058689460	192.168.200.150	192.168.200.100	HTTP	11…	HTTP/1.1 200 OK (text/html)
21	6.058740897	192.168.200.100	192.168.200.150	TCP	66	52058 → 80 [ACK] Seq=19 Ack=1

61	6.065097579	192.168.200.100	192.168.200.150	HTTP	229	GET /robots.txt HTTP/1.1
62	6.065469647	192.168.200.150	192.168.200.100	TCP	66	80 → 32798 [ACK] Seq=1 Ack=164 Win=6912 Len=0 TSval=
63	6.065682835	192.168.200.100	192.168.200.150	HTTP	219	GET / HTTP/1.1
64	6.065722677	192.168.200.100	192.168.200.150	HTTP	243	GET /nmaplowercheck1687960633 HTTP/1.1
65	6.065746652	192.168.200.100	192.168.200.150	HTTP	228	GET /.git/HEAD HTTP/1.1
66	6.065769199	192.168.200.100	192.168.200.150	HTTP	377	POST / HTTP/1.1 (application/x-www-form-urlencoded)
67	6.065791513	192.168.200.100	192.168.200.150	HTTP	223	OPTIONS / HTTP/1.1
68	6.065816140	192.168.200.100	192.168.200.150	UDP	43	52271 → 1434 Len=1
69	6.065839524	192.168.200.100	192.168.200.150	HTTP	84	GET / HTTP/1.0
70	6.065862961	192.168.200.100	192.168.200.150	HTTP	281	OPTIONS / HTTP/1.1
71	6.065887420	192.168.200.100	192.168.200.150	HTTP	223	OPTIONS / HTTP/1.1
72	6.065910258	192.168.200.100	192.168.200.150	HTTP	234	PROPFIND / HTTP/1.1
73	6.065933506	192.168.200.100	192.168.200.150	HTTP	234	PROPFIND / HTTP/1.1
74	6.065995155	192.168.200.150	192.168.200.100	TCP	66	80 → 32802 [ACK] Seq=1 Ack=154 Win=6912 Len=0 TSval=
75	6.065995229	192.168.200.150	192.168.200.100	TCP	66	80 → 32818 [ACK] Seq=1 Ack=178 Win=6912 Len=0 TSval=
76	6.065957233	192.168.200.100	192.168.200.150	HTTP	685	POST /sdk HTTP/1.1
77	6.066129109	192.168.200.150	192.168.200.100	TCP	66	80 → 32828 [ACK] Seq=1 Ack=163 Win=6912 Len=0 TSval=
78	6.066129129	192.168.200.150	192.168.200.100	TCP	66	80 → 32840 [ACK] Seq=1 Ack=312 Win=6912 Len=0 TSval=
79	6.066129157	192.168.200.150	192.168.200.100	TCP	66	80 → 32842 [ACK] Seq=1 Ack=158 Win=6912 Len=0 TSval=
80	6.066129175	192.168.200.150	192.168.200.100	ICMP	71	Destination unreachable (Port unreachable)

CONSIGLI PER RIDUZIONE IMPATTI D'ATTACCO

Dai risultati mostrati nella scansione iniziale si può vedere come la macchina di destinazione risponda con dettagli ed informazioni sensibili. Nonostante un port scanning non sia un attacco in sé, l'information gathering effettuato da un port scanner potrebbe fornire informazioni preziose a un potenziale attaccante.

Misure preventive:

1. **Configurazione firewall** sulla macchina di destinazione correttamente configurato per filtrare e bloccare il traffico indesiderato, limitare l'accesso alle porte e ai servizi solo a quelli strettamente necessari per il funzionamento del sistema.
2. **Aggiornamenti e patch** sempre aggiornati con le ultime patch di sicurezza. Questo contribuirà a ridurre le vulnerabilità note che potrebbero essere sfruttate da potenziali attacchi futuri.
3. **Analisi delle vulnerabilità** sulla macchina di destinazione utilizzando tool appositi. Questo aiuterà a identificare eventuali vulnerabilità nel sistema e a prendere le misure correttive necessarie.
4. **Protezione dei servizi** sulla macchina di destinazione in modo sicuro, disabilitando o rimuovendo i servizi non necessari assicurandosi che quelli essenziali siano configurati in modo sicuro (autenticazione forte, cifratura SSL/TSL e accesso limitato).
5. **Monitoraggio traffico di rete** per rilevare attività sospette o inconsuete al fine di rilevare potenziali attacchi futuri ed intrusi nella rete.
6. **Consapevolezza della sicurezza** e uso di pratiche sicure come l'utilizzo di password robuste, limitare l'accesso ai dati e alle risorse solo a coloro che ne hanno effettivamente bisogno ed educazione degli utenti sulla sicurezza informatica.