

THREAT INTELLIGENCE & IOC

Analizziamo pacchetto per pacchetto:

1. Il primo pacchetto è **un annuncio inviato da un dispositivo (192.168.200.150) verso tutti gli altri dispositivi nella rete (192.168.200.255), dal quale capiamo che la macchina target è Metasploitable**
2. Il secondo pacchetto indica che un dispositivo (192.168.200.100) sta cercando di connettersi a un altro dispositivo (192.168.200.150) **sulla porta 80 (HTTP).**
3. Il terzo pacchetto è simile al precedente, ma questa volta la connessione viene tentata sulla **porta 443 (HTTPS).**
4. Il quarto pacchetto è la risposta del dispositivo 192.168.200.150 al tentativo di connessione inviato dal dispositivo 192.168.200.100. **Il pacchetto conferma che la connessione è stata sincronizzata correttamente.**
5. Il quinto pacchetto è una risposta di **reset** inviata da 192.168.200.150 al dispositivo 192.168.200.100 sulla porta 443. **Questo è tipico di una scansione SYN effettuata con Nmap.**
6. Il sesto pacchetto è un pacchetto di conferma inviato dal dispositivo 192.168.200.100 a 192.168.200.150, **indicando che la connessione è stata stabilita correttamente.**
7. Il settimo pacchetto è **un pacchetto di reset** inviato dal dispositivo 192.168.200.100 a 192.168.200.150. Potrebbe indicare una terminazione anomala della connessione.
8. Il pacchetto numero 8 è un pacchetto **ARP (Address Resolution Protocol)** inviato da un dispositivo con un determinato indirizzo MAC alla rete, chiedendo chi possiede l'indirizzo IP 192.168.200.100.
9. Il pacchetto numero 9 è **la risposta ARP al pacchetto precedente.** Il dispositivo con l'indirizzo IP 192.168.200.100 afferma che il suo indirizzo MAC è **"08:00:27:39:7d:fe".**
10. Il pacchetto numero 10 è **un altro pacchetto ARP.** Questa volta, il dispositivo con un determinato indirizzo MAC sta cercando di scoprire l'indirizzo MAC del dispositivo con l'indirizzo IP 192.168.200.150.

11. Il pacchetto numero 11 è **la risposta ARP al pacchetto precedente**. Il dispositivo con l'indirizzo IP 192.168.200.150 afferma che il suo indirizzo MAC è **"08:00:27:fd:87:1e"**.

12. Il pacchetto numero 12 è un pacchetto TCP inviato dal dispositivo 192.168.200.100 a 192.168.200.150 **sulla porta 23 (TELNET)**.

13. Il pacchetto numero 13 è simile al precedente, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione TCP **sulla porta 111 (RPC)**.

14. Il pacchetto numero 14 è simile ai precedenti, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione **TCP sulla porta 443 (HTTPS)**.

15. Il pacchetto numero 15 è simile ai precedenti, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione TCP **sulla porta 554 (RTSP)**.

16. Il pacchetto numero 16 è simile ai precedenti, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione TCP **sulla porta 135 (RPC)**.

17. Il pacchetto numero 17 è simile ai precedenti, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione TCP **sulla porta 993 (IMAP)**.

18. Il pacchetto numero 18 è simile ai precedenti, ma questa volta il dispositivo 192.168.200.100 sta cercando di stabilire una connessione TCP **sulla porta 21 (FTP)**.

19. Il pacchetto numero 19 è la risposta del dispositivo 192.168.200.150 al tentativo di connessione inviato dal dispositivo 192.168.200.100 **sulla porta 23 (TELNET)**. **Il pacchetto conferma che la connessione è stata sincronizzata correttamente.**

20. Il pacchetto numero 20 è simile al precedente, ma questa volta il dispositivo 192.168.200.150 sta rispondendo al tentativo di connessione **TCP sulla porta 111 (RPC)** effettuato dal dispositivo 192.168.200.100.

21. Il pacchetto numero 21 è **una risposta di reset** inviata dal dispositivo 192.168.200.150 al dispositivo 192.168.200.100 sulla porta 33878. **Questo è tipico di una scansione SYN effettuata con Nmap.**

22. Il pacchetto numero 22 è **una risposta di reset** inviata dal dispositivo 192.168.200.150 al dispositivo 192.168.200.100 sulla porta 58636.

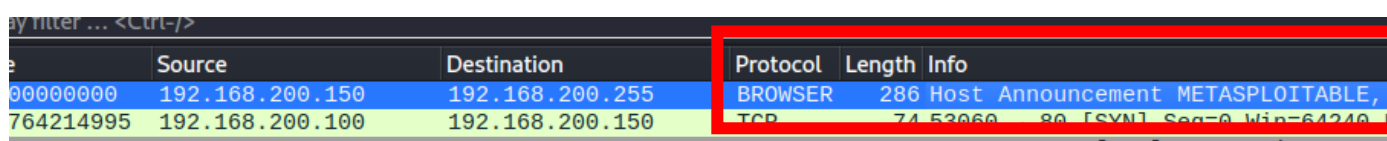
23. Il pacchetto numero 23 è **una risposta di reset** inviata dal dispositivo 192.168.200.150 al dispositivo 192.168.200.100 sulla porta 135.

Dopo aver analizzato una ventina di pacchetti sniffati con Wireshark, **possiamo passare ad un'analisi della situazione che si sta verificando.**

Anzitutto, si può notare che entrambi gli indirizzi IP sono sulla stessa rete **192.168.200.X**

Si notano immediatamente **una serie di pacchetti SYN, nmap -sS** inviati da diversi indirizzi IP sorgente 192.168.200.100 a un indirizzo IP di destinazione 192.168.200.150 **su diverse porte di destinazione.**

Il primo pacchetto mostra che la macchina target è Metasploitable, che sappiamo essere una macchina virtuale vulnerabile spesso usato per test sulla sicurezza informatica.



	Source	Destination	Protocol	Length	Info
00000000	192.168.200.150	192.168.200.255	BROWSER	286	Host Announcement METASPLOITABLE,
764214995	192.168.200.100	192.168.200.150	TCP	74	52060 -> 80 [SYN] Seq=0 Win=64240

Tuttavia, i pacchetti SYN non vengono seguiti da una risposta ACK o dalla fase di completamento della connessione, ma invece **vengono inviati immediatamente pacchetti RST (reset) per interrompere le connessioni.** Questo comportamento indica un'attività anomala, e che con tutta **probabilità è in corso un attacco di tipo "Scansione SYN" con nmap -sS.** Questo tipo di attacco sfrutta il protocollo TCP per inviare un grande numero di richieste di connessione, **risultando comunque meno invasivo rispetto ad una TCP scan con nmap -sT.**

La presenza di richieste di sincronizzazione (SYN) **a porte note come 80 (HTTP), 443 (HTTPS)** e altre, potrebbe indicare una **scansione delle porte o un tentativo di individuare servizi e vulnerabilità specifiche.**

Inoltre, oltre alle porte 80 e 443, si nota che **le scansioni vengono effettuate altresì su altre porte note, 21 (FTP), 23 (TELNET), 111 (RPC), 113 (IDENT), 135 (RPC), 554 (RTSP), 993 (IMAPS).**

PONTEZIALI REMEDIATION ACTION:

- Assicurarsi di avere tutti gli aggiornamenti necessari per i servizi vulnerabili e il sistema operativo. Installare le ultime patch disponibili per risolvere eventuali bug o vulnerabilità.
- Bloccare l'indirizzo IP da cui provengono le richieste di connessione sospette. Impedire l'accesso al sistema da parte di quell'indirizzo IP specifico.
- Configurare il firewall per impedire l'accesso non autorizzato al sistema. Creare regole nel firewall per consentire solo il traffico legittimo e bloccare qualsiasi tentativo di accesso indesiderato.
- Chiudere le porte della macchina bersaglio che non sono necessarie per l'utente o per i servizi in esecuzione. Disabilitare i servizi non utilizzati o configurarli in modo che ascoltino solo su determinate porte.

