



NovaData
Tech

REPORT

BY MORGAN PETRELLI



OVERVIEW

01

About Us

02

Ingaggio e
preventivo

03

S9/L1

04

S9/L2

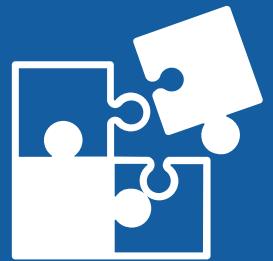
05

S9/L3

06



ABOUT NOVADATA TECH



NovaData Tech è una start-up innovativa nel settore delle tecnologie dell'informazione, fondata nel 2022 e con sede a Roma. L'azienda si specializza nello sviluppo di soluzioni avanzate per la gestione e l'analisi dei dati, rivolgendosi principalmente a piccole e medie imprese che cercano di migliorare la propria efficienza operativa attraverso l'uso strategico dei dati.



NovaData Tech ha richiesto un Vulnerability Assessment e un Penetration Testing per valutare la sicurezza della propria rete aziendale, in particolare per garantire che le soluzioni offerte ai clienti siano sicure e conformi agli standard di sicurezza più elevati. L'azienda è consapevole delle crescenti minacce informatiche e vuole assicurarsi che i propri dati e quelli dei clienti siano protetti.



REGOLE DI INGAGGIO

Definire le regole di ingaggio per il pen test di NovaData Tech per garantire che il test venga eseguito in modo sicuro, efficace e con il minimo impatto sulle operazioni aziendali.

- Scopo del Test:
 - Valutare la sicurezza dell'infrastruttura IT di NovaData Tech.
 - Identificare vulnerabilità nei sistemi, applicazioni, reti e database.
 - Testare l'efficacia delle politiche di gestione delle identità e degli accessi.
 - Fornire raccomandazioni per migliorare la sicurezza complessiva.
- Autorizzazioni:
 - Accordo di Riservatezza (NDA): Firmato da tutte le parti coinvolte.
 - Autorizzazione Formale: Documento che dettaglia l'ambito, gli obiettivi e le date del test.
 - Accessi Temporanei: Forniti per tutte le aree e i sistemi inclusi nel test.
- Limiti e Restrizioni:
 - Orario del Test: Test condotti durante orari lavorativi predefiniti per ridurre l'impatto sulle operazioni.
 - Sistema Critici: Identificati e trattati con maggiore cautela per evitare interruzioni.
- strumenti utilizzati:
 - nmap: utilizzato per scansionare le porte aperte sulla macchina windows xp e valutare il comportamento del Firewall e garantire che un determinato traffico, potenzialmente dannoso, venga bloccato.
 - Wireshark: Consente agli utenti di catturare e interattivamente navigare nel traffico che passa attraverso una rete di computer. È utilizzato da professionisti della sicurezza, amministratori di rete e sviluppatori per monitorare, analizzare e risolvere problemi di rete.

PREVENTIVO

Morgan Petrelli
Via Mauro Amoruso 18
70124 Bari
Cf. PTRMGN01
P.IVA 1234567

Spett. Ditta
NOVADATA TECH
Via Rossi 1
00000 Milano

Oggetto: preventivo per la realizzazione di Penetration Testing

DESCRIZIONE	PERSONALE PREVISTO	ORE TOTALI LAVORATIVE MINIME PREVISTE	COSTO ORARIO EURO	TOTALE EURO
Costi personale	1	54	100	5.400
Costo strumenti necessari alla la realizzazione del progetto	---	---	450	450
TOTALE PROGETTO				5.850

Il progetto avrà una durata di 7 giorni lavorativi, a partire dalla consegna del materiale necessario (password, dati) per la realizzazione del lavoro stesso.

All'accettazione del contratto, la ditta NovaTech Data dovrà versare il 30% del totale come acconto a mezzo bonifico su conto intestato a Morgan Petrelli, iban IT1234567890. Il restante 70% sarà versato entro 15 giorni dalla consegna del lavoro. **Il costo totale è IVA esclusa.**

Morgan Petrelli
Firma

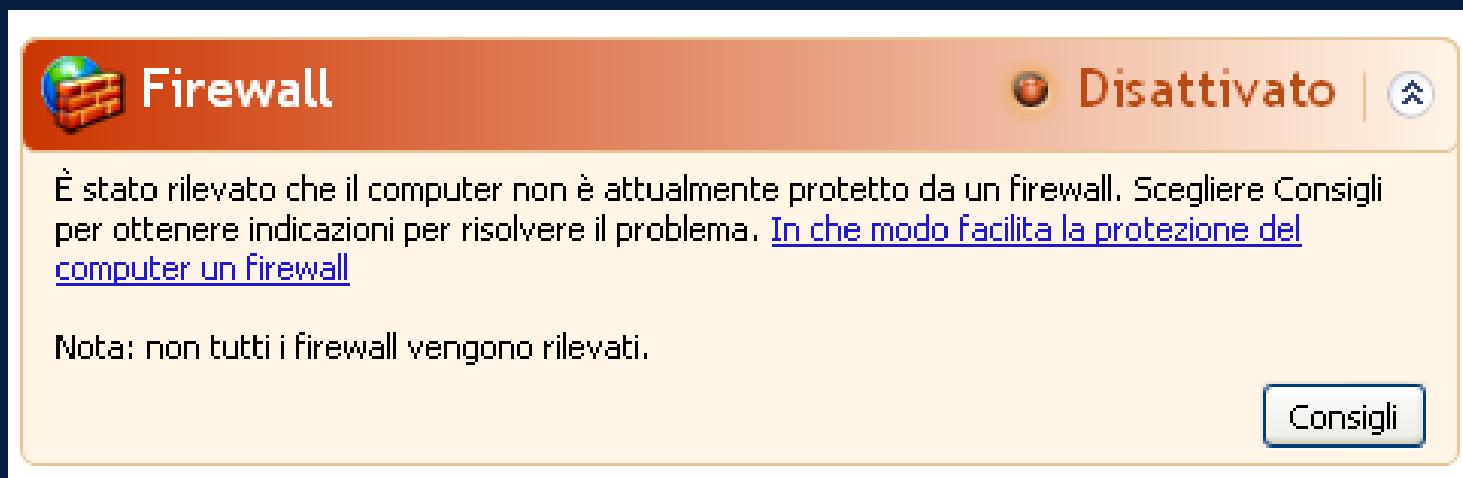
PER ACCETTAZIONE
(firma NoVaData Tech)

L'ESERCIZIO DI OGGI È VERIFICARE IN CHE MODO L'ATTIVAZIONE DEL FIREWALL IMPATTA IL RISULTATO DI UNA SCANSIONE DEI SERVIZI DALL'ESTERNO.

PER QUESTO MOTIVO:

- 1. ASSICURATEVI CHE IL FIREWALL SIA DISATTIVATO SULLA MACCHINA WINDOWS XP**
- 2. EFFETTUATE UNA SCANSIONE CON NMAP SULLA MACCHINA TARGET (UTILIZZATE LO SWITCH-SV, PER LA SERVICE DETECTION E -O NOMEFILEREPORT PER SALVARE IN UN FILE L'OUTPUT)**
- 3. ABILITARE IL FIREWALL SULLA MACCHINA WINDOWS XP**
- 4. EFFETTUATE UNA SECONDA SCANSIONE CON NMAP, UTILIZZANDO ANCORA UNA VOLTA LO SWITCH-SV.**
- 5. TROVARE LE EVENTUALI DIFFERENZE E MOTIVARLE.**

inizio settando i vari indirizzi ip come richiesto dalla traccia e verifico che il firewall sia disattivato.



```
::\Documents and Settings\Epicode_user>ipconfig  
Configurazione IP di Windows  
  
Scheda Ethernet Connessione alla rete locale (LAN):  
  
Suffisso DNS specifico per connessione:  
Indirizzo IP . . . . . : 192.168.240.150  
Subnet mask . . . . . : 255.255.255.0  
Gateway predefinito . . . . . : 192.168.240.1  
  
::\Documents and Settings\Epicode_user>
```

```
→ 1:~# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255  
      inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>  
        ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
          RX packets 6 bytes 848 (848.0 B)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 25 bytes 3128 (3.0 KiB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
      inet 127.0.0.1 netmask 255.0.0.0  
      inet6 ::1 prefixlen 128 scopeid 0x10<host>  
        loop txqueuelen 1000 (Local Loopback)  
          RX packets 8 bytes 480 (480.0 B)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 8 bytes 480 (480.0 B)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

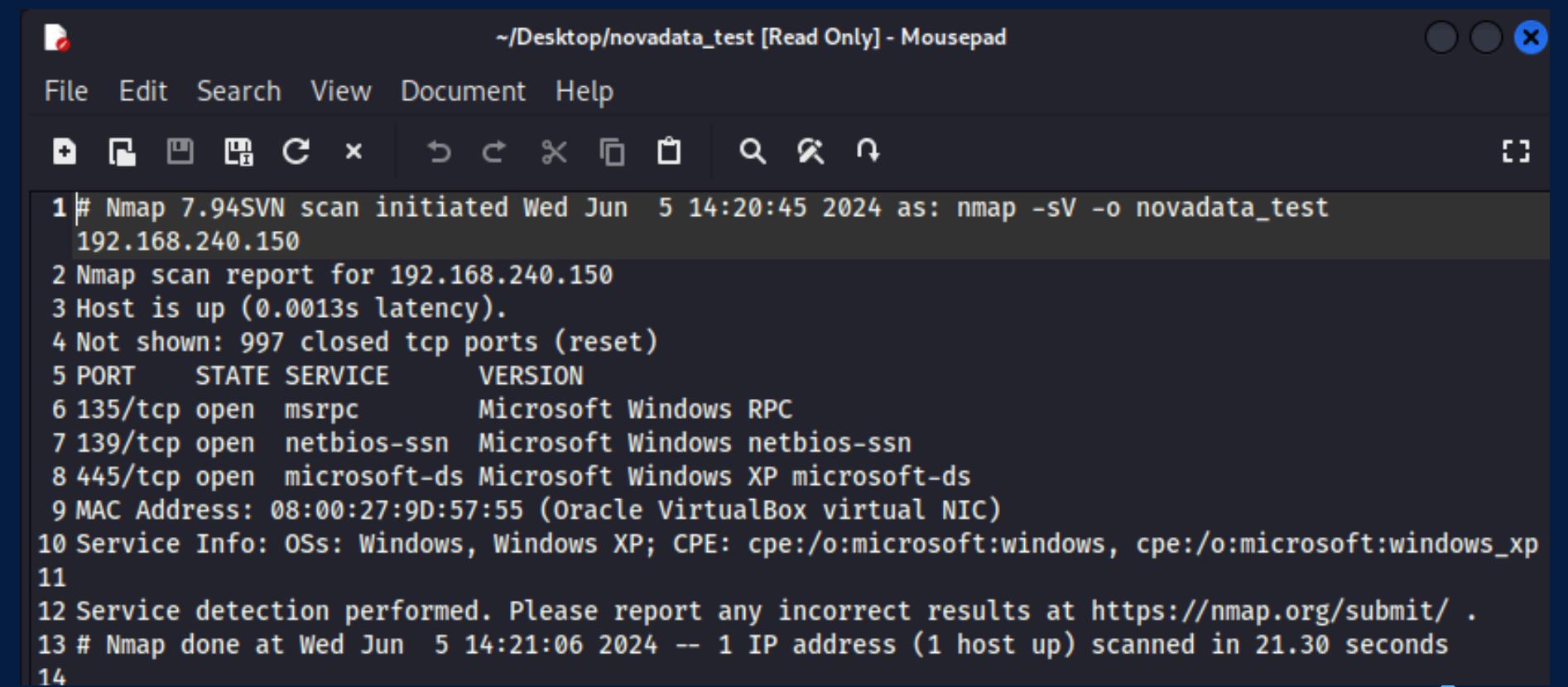
SCANSIONE NMAP

usando il comando nmap -sV 192.168.240.150 -o novadata_test ho effettuato una scansione delle porte verso la macchina windows xp. Come risultato ho ricevuto come risposta le porte e il servizio in ascolto e avendo usato lo switch -sV anche il tipo di versione del servizio.

```
└$ sudo nmap -sV 192.168.240.150 -o novadata_test
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 14:20 CEST
Nmap scan report for 192.168.240.150
Host is up (0.0013s latency).

Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:9D:57:55 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

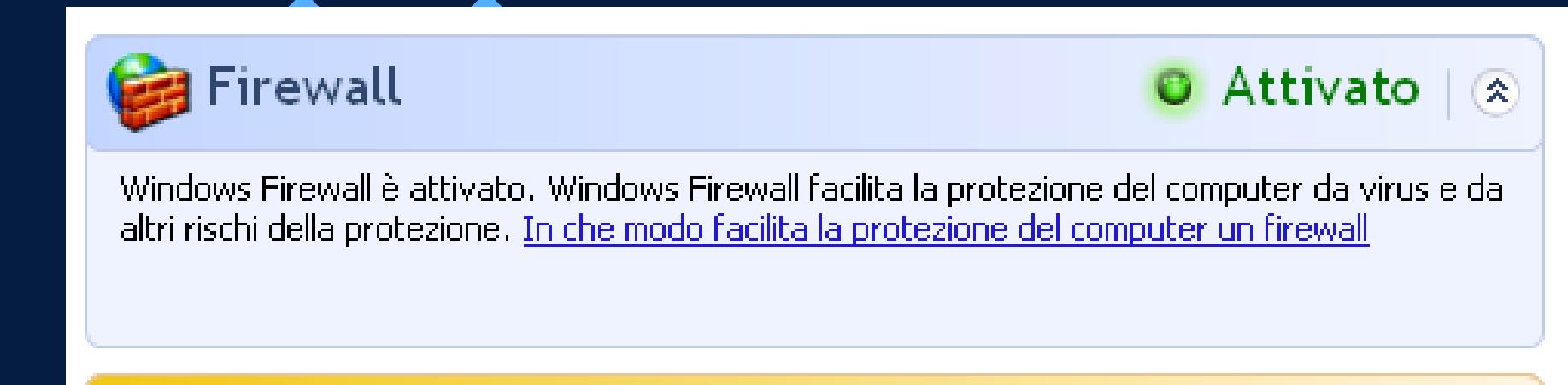
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
```



The screenshot shows a terminal window titled '~/Desktop/novadata_test [Read Only] - Mousepad'. The window contains the command-line output of an Nmap scan. The output details the following information:

- Scan initiated on Wednesday, June 5, 2024, at 14:20:45.
- Scanned host: 192.168.240.150.
- Host status: Host is up (0.0013s latency).
- Ports scanned:
 - 135/tcp: open, msrpc, Microsoft Windows RPC.
 - 139/tcp: open, netbios-ssn, Microsoft Windows netbios-ssn.
 - 445/tcp: open, microsoft-ds, Microsoft Windows XP microsoft-ds.
- MAC Address: 08:00:27:9D:57:55 (Oracle VirtualBox virtual NIC).
- Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp.
- Service detection performed, with a note to report any incorrect results at <https://nmap.org/submit/>.
- Scan completed at 14:21:06 on June 5, 2024, with 1 IP address scanned in 21.30 seconds.

una volta attivato il Firewall provo a rifare la scansione con nmap



riprovo con il comando di prima ma questa volta il risultato riportato è che la macchina o è spenta o che qualcosa sta bloccando il nostro tentativo di scansionare le porte. provo aggiungendo lo switch -Pn per saltare il ping e passare direttamente al service Discovery. Ricevo come risposta che tutte le porte sono filtrate questo mi fa capire che il Firewall sta bloccando le nostre richieste. Questo è utile al fine di ridurre attacchi dall'esterno.

```
└$ nmap -sV 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 15:12 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.13 seconds
```

```
└$ nmap -sV 192.168.240.150 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 15:24 CEST
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.80 seconds
```

CON IL SUPPORTO DEI DATI PRESENTI NELLE TABELLE CHE SEGUONO, CALCOLARE LA PERDITA ANNUALE CHE SUBIREBBE LA COMPAGNIA NEL CASO DI TERREMOTO, INCENDIO, INONDAZIONE SUI TRE ASSET:

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

PERDITA ANNUALE

per calcolare le perdite annuali (ALE) bisogna prima calcolare l'impatto che avrebbe il singolo(SLE) evento per poi moltiplicarlo per le volte in cui l'evento si stima si potrebbe verificare (ARO)

FORMULE:

$$SLE = \text{VALORE ASSET (AV)} \times \text{PERCENTUALE IMPATTATA IN CASO DI EVENTO (EF)}$$

$$ALE = SLE \times ARO$$

EDIFICIO PRIMARIO	EDIFICIO SECONDARIO	DATACENTER
Inondazione SLE: $(350.000 \times 0,55) = 192.500$ ALE: $(192.500 \times 0,02) = 3.850$	Inondazione SLE: $(150.000 \times 0,4) = 60.000$ ALE: $(60.000 \times 0,02) = 1.200$	Inondazione SLE: $(100.000 \times 0,35) = 35.000$ ALE: $(35.000 \times 0,02) = 700$
Incendio SLE: $(350.000 \times 0,6) = 210.000$ ALE: $(210.000 \times 0,05) = 10.500$	Incendio SLE: $(150.000 \times 0,5) = 75.000$ ALE: $(75.000 \times 0,05) = 3.750$	Incendio SLE: $(100.000 \times 0,6) = 60.000$ ALE: $(60.000 \times 0,05) = 3.000$
Terremoto SLE: $(350.000 \times 0,8) = 280.000$ ALE: $(280.000 \times 0,03) = 8.400$	Terremoto SLE: $(150.000 \times 0,8) = 120.000$ ALE: $(120.000 \times 0,03) = 3.600$	Terremoto SLE: $(100.000 \times 0,95) = 95.000$ ALE: $(95.000 \times 0,03) = 2.850$

Analizzare la cattura con wireshark attentamente e rispondere ai seguenti quesiti:

Identificate eventuali IOC, ovvero evidenze di attacchi in corso In base agli IOC trovati

Fate delle ipotesi sui potenziali vettori di attacco utilizzati

Consigliate un'azione per ridurre gli impatti dell'attacco

ANALIZZO GLI INDICATORI DI COMPROMISSIONE (IOC)

Gli IOC sono evidenze che suggeriscono che un sistema o una rete possono essere stati compromessi. Questi indicatori aiutano gli analisti di sicurezza a rilevare, rispondere e indagare su possibili violazioni di sicurezza.

No.	Time	Source	Destination	Protocol	Length	Info
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74	53060 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522427 TSecr=0 WS=128
3	23.764287789	192.168.200.100	192.168.200.150	TCP	74	33876 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810522428 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74	80 → 53060 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294951165 TSecr=810522427 WS=64
5	23.764777427	192.168.200.150	192.168.200.100	TCP	60	443 → 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
7	23.764899091	192.168.200.100	192.168.200.150	TCP	66	53060 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810522428 TSecr=4294951165
12	36.774143445	192.168.200.100	192.168.200.150	TCP	74	41304 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
13	36.774218116	192.168.200.100	192.168.200.150	TCP	74	56120 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74	33878 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535437 TSecr=0 WS=128
15	36.774366305	192.168.200.100	192.168.200.150	TCP	74	58636 → 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
16	36.774405627	192.168.200.100	192.168.200.150	TCP	74	52358 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74	46138 → 993 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74	41182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=810535438 TSecr=0 WS=128
19	36.774685505	192.168.200.150	192.168.200.100	TCP	74	23 → 41304 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
20	36.774685652	192.168.200.150	192.168.200.100	TCP	74	111 → 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=4294952466 TSecr=810535437 WS=64
21	36.774685696	192.168.200.150	192.168.200.100	TCP	60	443 → 33878 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	60	554 → 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.774685776	192.168.200.150	192.168.200.100	TCP	60	135 → 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774700464	192.168.200.100	192.168.200.150	TCP	66	41304 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66	56120 → 111 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535438 TSecr=4294952466
26	36.775141104	192.168.200.150	192.168.200.100	TCP	60	993 → 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Osservando la cattura di wireshark ho notato una richiesta ripetuta di un protocollo TCP da parte dell'Ip 192.168.200.100 verso il target 192.168.200.150 questo potrebbe essere una potenziale scansione delle porte da parte di qualcuno, lo si capisce anche perchè in alcune righe sono presenti delle risposte SYN-ACK quando la porta del target è aperta e RST-ACK quando la porta è chiusa. Questo è spesso un passo preliminare per identificare i servizi in esecuzione sul target e trovare potenziali vulnerabilità da sfruttare.

Per ridurre gli impatti dell'attacco si può isolare l'Ip sospetto (192.168.200.100) per evitare ulteriori scansioni e configurare il firewall in modo da bloccare altri tentativi di scansione