



NovaData
Tech

REPORT

BY MORGAN PETRELLI



OVERVIEW

01

About Us

02

Ingaggio e
preventivo

03

S9/L1

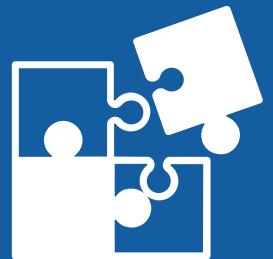
04

05

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.

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

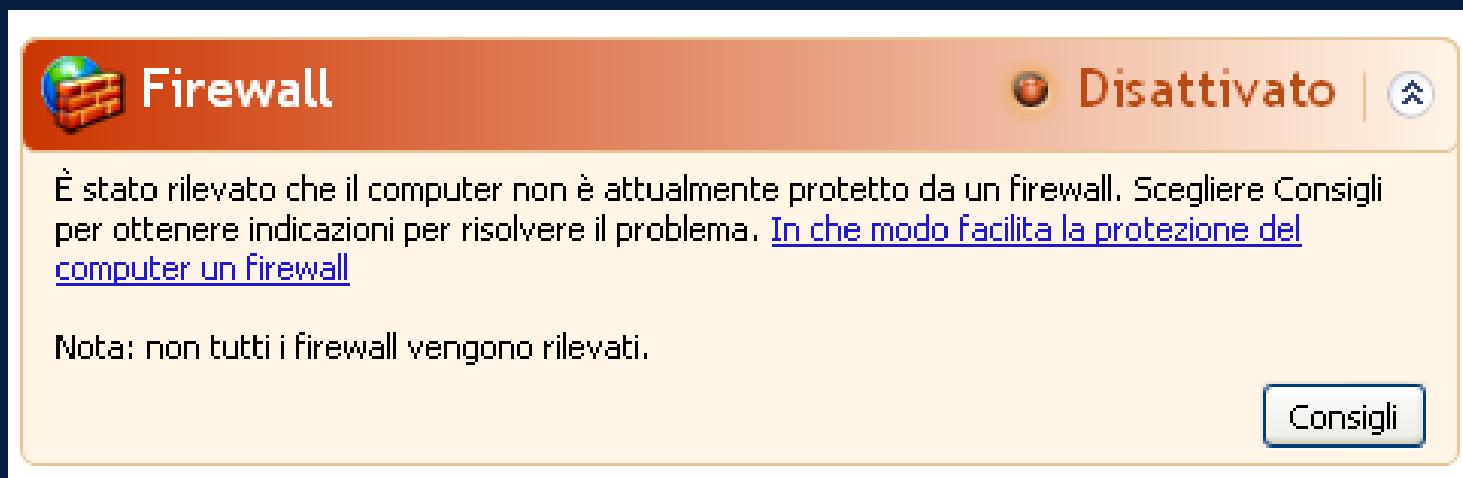
PER ACCETTAZIONE
(firma NoVaData Tech)

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>
```

```
→ ITC011ig  
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
```

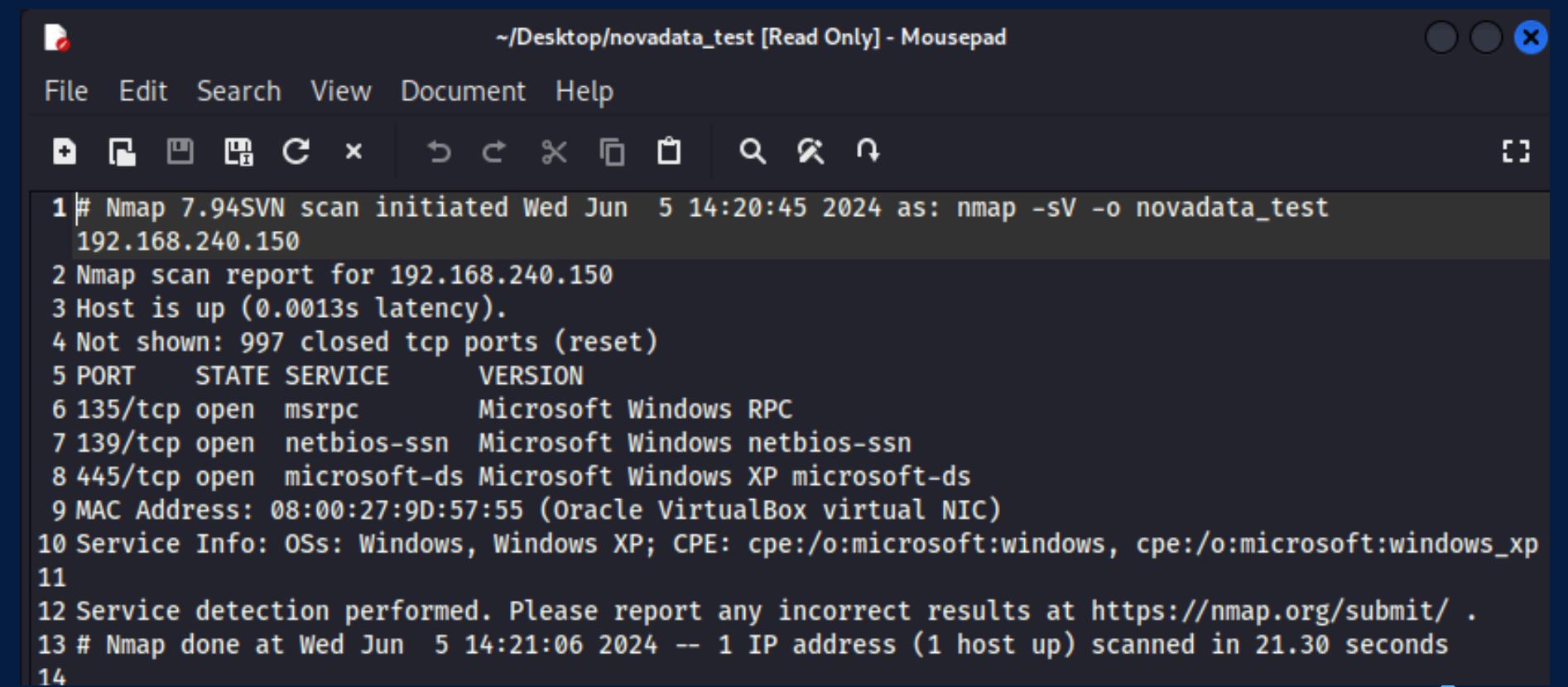
SCANSIONE NMAP

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

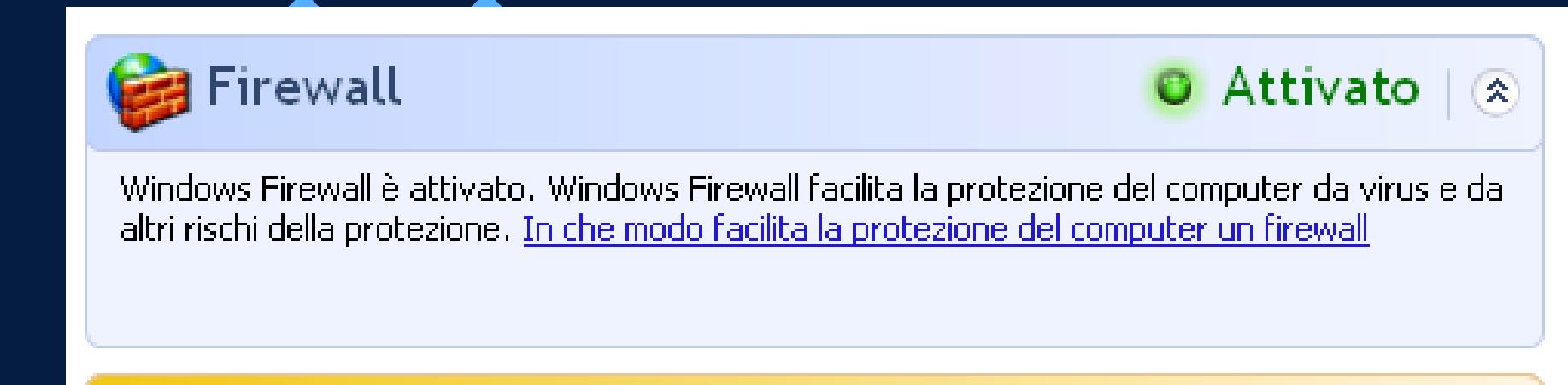
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds
```



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. Please 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
```