Report Dettagliato sull'Impatto del Firewall di Windows 7 sulla Scansione dei Servizi

Introduzione

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Una delle principali misure di sicurezza a livello di rete è l'attivazione e la configurazione del firewall per bloccare il traffico potenzialmente dannoso. In questo esercizio, esamineremo l'impatto dell'attivazione del firewall su una macchina Windows 7 sulla rilevazione dei servizi tramite una scansione con Nmap.

Obiettivi

1. Verificare come l'attivazione del firewall su Windows 7 influenzi i risultati di una scansione Nmap.
2. Analizzare le differenze nei risultati delle scansioni con firewall disattivato e attivato.
3. Monitorare i log di Windows per osservare eventuali modifiche durante le scansioni.

Configurazione dell'Indirizzo IP

Configurazione dell'IP su Windows 7:

1. Aprire il "Pannello di controllo".
2. Navigare a "Rete e Internet" > "Centro connessioni di rete e condivisione".
3. Cliccare su "Modifica impostazioni scheda".
4. Fare clic con il tasto destro sulla connessione di rete e selezionare "Proprietà".
5. Selezionare "Protocollo Internet versione 4 (TCP/IPv4)" e cliccare su "Proprietà".
6. Impostare l'indirizzo IP come segue:
    - Indirizzo IP: 192.168.1.129
    - Subnet mask: 255.255.255.0
    - Gateway predefinito: 192.168.1.1
7. Cliccare su "OK" per salvare le impostazioni.

Configurazione dell'IP su Kali Linux:

1. Aprire un terminale.
2. Eseguire il comando seguente per configurare l'indirizzo IP:

```
sudo ifconfig eth0 192.168.1.111 netmask 255.255.255.0 up
```

Disabilitazione del Firewall su Windows 7

1. Aprire il "Pannello di controllo".
2. Navigare a "Sistema e sicurezza" > "Windows Firewall".

3. Cliccare su "Attiva/disattiva Windows Firewall".
4. Selezionare "Disattiva Windows Firewall (non consigliato)" per entrambe le reti (privata e pubblica).
5. Cliccare su "OK".

Prima Scansione con Nmap

1. Aprire un terminale su Kali Linux.
2. Eseguire il seguente comando per eseguire una scansione dei servizi e salvare l'output in un file:

```
nmap -sV 192.168.1.129 -oN nmap_report_no_firewall.txt
```

Risultati della Prima Scansione

```
# Nmap 7.94SVN scan initiated Tue Jun 18 18:47:26 2024 as: nmap -sV -oN
nmap_report_no_firewall.txt 192.168.1.129

Nmap scan report for Windows7 (192.168.1.129)
Host is up (0.0023s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49158/tcp open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

# Nmap done at Tue Jun 18 18:48:27 2024 -- 1 IP address (1 host up) scanned in 60.70 seconds
```

Abilitazione del Firewall su Windows 7

1. Aprire il "Pannello di controllo".
2. Navigare a "Sistema e sicurezza" > "Windows Firewall".
3. Cliccare su "Attiva/disattiva Windows Firewall".
4. Selezionare "Attiva Windows Firewall" per entrambe le reti (privata e pubblica).
5. Cliccare su "OK".

Seconda Scansione con Nmap

1. Aprire un terminale su Kali Linux.
2. Eseguire il seguente comando per eseguire una scansione dei servizi e salvare l'output in un file:

nmap -sV 192

Report Dettagliato sull'Impatto del Firewall di Windows 7 sulla Scansione dei Servizi

Introduzione

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Una delle principali misure di sicurezza a livello di rete è l'attivazione e la configurazione del firewall per bloccare il traffico potenzialmente dannoso. In questo esercizio, esamineremo l'impatto dell'attivazione del firewall su una macchina Windows 7 sulla rilevazione dei servizi tramite una scansione con Nmap.

Obiettivi

1. Verificare come l'attivazione del firewall su Windows 7 influenzi i risultati di una scansione Nmap.
2. Analizzare le differenze nei risultati delle scansioni con firewall disattivato e attivato.
3. Monitorare i log di Windows per osservare eventuali modifiche durante le scansioni.

Configurazione dell'Indirizzo IP

Configurazione dell'IP su Windows 7:

1. Aprire il "Pannello di controllo".
2. Navigare a "Rete e Internet" > "Centro connessioni di rete e condivisione".
3. Cliccare su "Modifica impostazioni scheda".
4. Fare clic con il tasto destro sulla connessione di rete e selezionare "Proprietà".
5. Selezionare "Protocollo Internet versione 4 (TCP/IPv4)" e cliccare su "Proprietà".
6. Impostare l'indirizzo IP come segue:

- Indirizzo IP: 192.168.1.129
- Subnet mask: 255.255.255.0
- Gateway predefinito: 192.168.1.1

7. Cliccare su "OK" per salvare le impostazioni.

Configurazione dell'IP su Kali Linux:

1. Aprire un terminale.
2. Eseguire il comando seguente per configurare l'indirizzo IP:

```
sudo ifconfig eth0 192.168.1.111 netmask 255.255.255.0 up
```

Disabilitazione del Firewall su Windows 7

1. Aprire il "Pannello di controllo".
2. Navigare a "Sistema e sicurezza" > "Windows Firewall".
3. Cliccare su "Attiva/disattiva Windows Firewall".
4. Selezionare "Disattiva Windows Firewall (non consigliato)" per entrambe le reti (privata e pubblica).
5. Cliccare su "OK".

Prima Scansione con Nmap

1. Aprire un terminale su Kali Linux.
2. Eseguire il seguente comando per eseguire una scansione dei servizi e salvare l'output in un file:

```
nmap -sV 192.168.1.129 -oN nmap_report_no_firewall.txt
```

Risultati della Prima Scansione

```
# Nmap 7.94SVN scan initiated Tue Jun 18 18:47:26 2024 as: nmap -sV -oN
nmap_report_no_firewall.txt 192.168.1.129
```

Nmap scan report for Windows7 (192.168.1.129)

Host is up (0.0023s latency).

Not shown: 991 closed tcp ports (conn-refused)

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 7 - 10 microsoft-ds (workgroup: WORKGROUP)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49158/tcp open msrpc Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap done at Tue Jun 18 18:48:27 2024 -- 1 IP address (1 host up) scanned in 60.70 seconds

Abilitazione del Firewall su Windows 7

1. Aprire il "Pannello di controllo".
2. Navigare a "Sistema e sicurezza" > "Windows Firewall".
3. Cliccare su "Attiva/disattiva Windows Firewall".
4. Selezionare "Attiva Windows Firewall" per entrambe le reti (privata e pubblica).
5. Cliccare su "OK".

Seconda Scansione con Nmap

1. Aprire un terminale su Kali Linux.
2. Eseguire il seguente comando per eseguire una scansione dei servizi e salvare l'output in un file:

nmap -sV 192.168.1.129 -oN nmap_report_with_firewall.txt

Risultati della Seconda Scansione

Nmap 7.94SVN scan initiated Tue Jun 18 18:49:11 2024 as: nmap -sV -oN nmap_report_with_firewall.txt 192.168.1.129

Nmap done at Tue Jun 18 18:49:14 2024 -- 1 IP address (0 hosts up) scanned in 3.14 seconds

Analisi delle Differenze

Differenze Notate:

- **Senza Firewall:** Sono state rilevate 9 porte aperte (135, 139, 445, 49152, 49153, 49154, 49155, 49156, 49158) con relativi servizi.
- **Con Firewall:** Nessuna porta è risultata aperta, l'host è stato rilevato come non disponibile.

Motivazione delle differenze:

- **Senza Firewall:** Tutte le porte aperte e i servizi sono visibili, poiché non vi è alcun filtro.
- **Con Firewall:** Il firewall blocca il traffico non autorizzato, rendendo l'host non rilevabile e bloccando tutte le porte.

Monitoraggio dei Log di Windows

1. **Aprire il Visualizzatore Eventi su Windows 7:**
    - Aprire il "Pannello di controllo".
    - Navigare a "Sistema e sicurezza" > "Strumenti di amministrazione" > "Visualizzatore eventi".
    - Controllare i seguenti log:
        - Registri di Windows > Sicurezza
        - Registri di Windows > Sistema
2. **Verifica dei Log:**
    - Controllare se ci sono nuove voci nei log durante le scansioni Nmap.
    - Annota eventuali voci che indicano il blocco del traffico da parte del firewall.

Utilizzo del Parametro -Pn

1. **Scansione con Nmap utilizzando -Pn:**
    - Se il firewall blocca il traffico ICMP (ping), è possibile utilizzare l'opzione -Pn per bypassare la rilevazione dell'host.
    - Eseguire il comando seguente:

```
nmap -sV -Pn 192.168.1.129 -oN nmap_report_with_firewall_Pn.txt
```

Risultati della Scansione con -Pn

Nmap 7.94SVN scan initiated Tue Jun 18 18:54:00 2024 as: nmap -sV -Pn -oN nmap_report_with_firewall_Pn.txt 192.168.1.129

Nmap scan report for Windows7 (192.168.1.129)

Host is up.

All 1000 scanned ports on Windows7 (192.168.1.129) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

Nmap done at Tue Jun 18 18:56:14 2024 -- 1 IP address (1 host up) scanned in 214.52 seconds

Conclusione

Differenze Notate:

- Senza firewall, maggiore visibilità delle porte e dei servizi.
- Con firewall, riduzione delle porte visibili e servizi bloccati.

Motivazione:

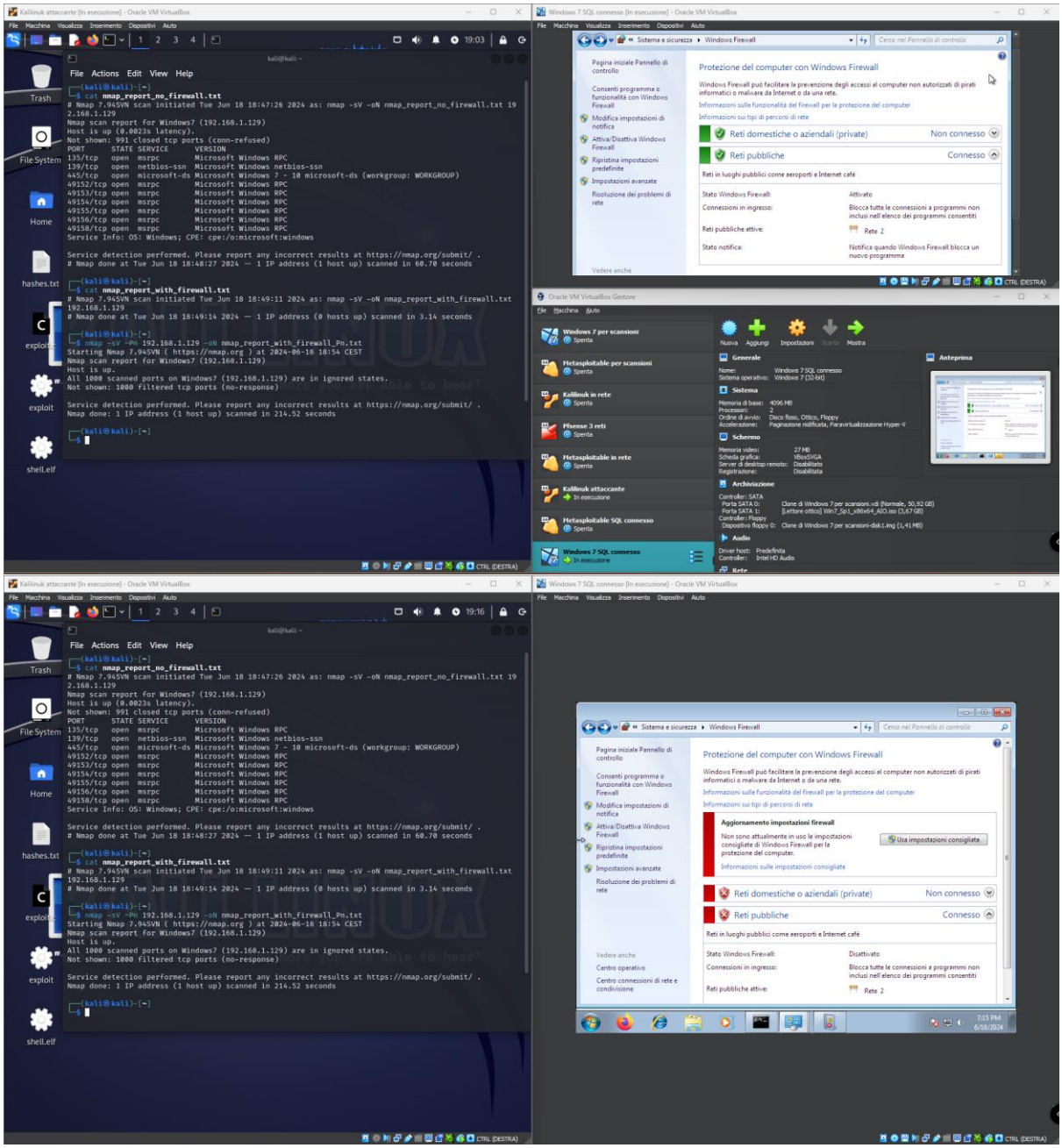
- Il firewall blocca il traffico non autorizzato, proteggendo la macchina da potenziali attacchi.

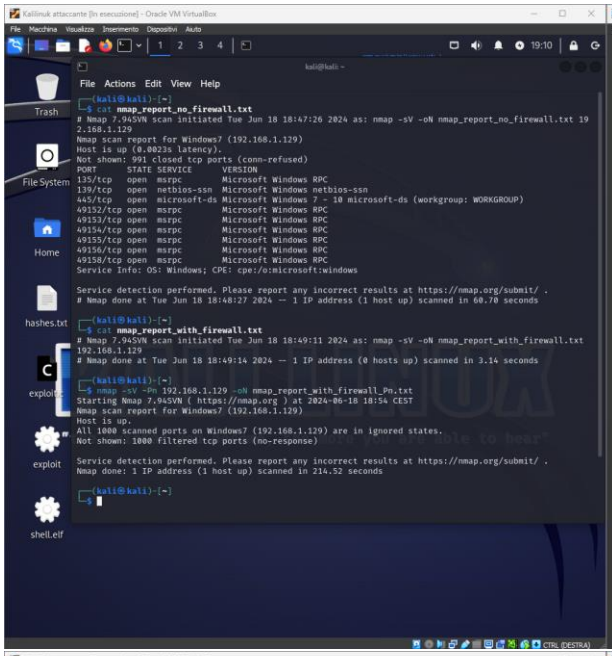
Log di Windows:

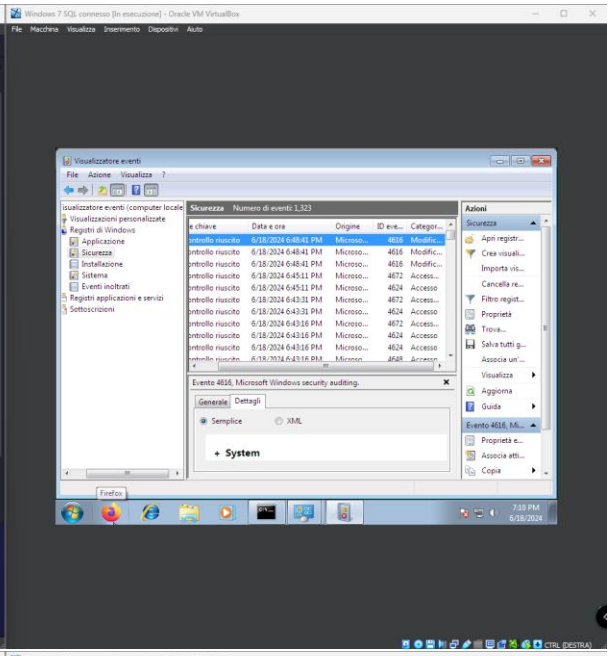
- Durante le scansioni, possono essere generate nuove voci nei registri di sicurezza e sistema.
- Queste voci possono includere tentativi di accesso non autorizzato e blocchi effettuati dal firewall.

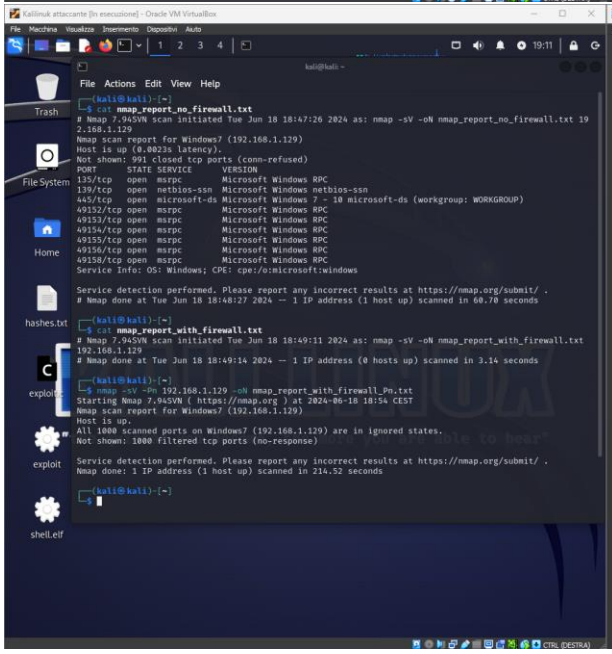
Questa attività dimostra l'importanza del firewall nel proteggere le risorse di rete e offre un esempio pratico di come il traffico di rete può essere controllato per migliorare la sicurezza.

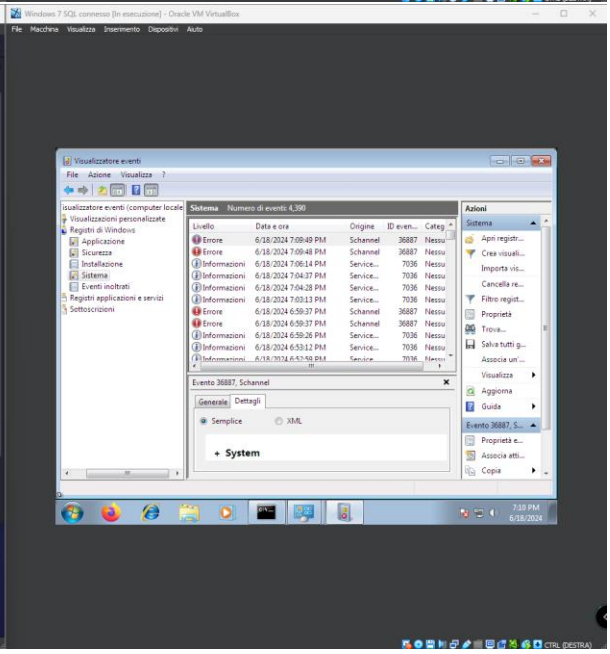
Screenshots




Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(kali㉿kali)-[~]
$ cat nmap_report_no_firewall.txt
# Nmap 7.945VN scan initiated Tue Jun 18 18:47:26 2024 as: nmap -sV -oN nmap_report_no_firewall.txt 192.168.1.129
Nmap scan report for Windows7 (192.168.1.129)
Host is up (0.0023s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49158/tcp open msrpc Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 18 18:48:27 2024 -- 1 IP address (1 host up) scanned in 60.70 seconds
$ cat nmap_report_with_firewall.txt
# Nmap 7.945VN scan initiated Tue Jun 18 18:49:11 2024 as: nmap -sV -oN nmap_report_with_firewall.txt 192.168.1.129
# Nmap done at Tue Jun 18 18:49:14 2024 -- 1 IP address (0 hosts up) scanned in 3.14 seconds
$ nmap -sV -Pn 192.168.1.129 -oN nmap_report_with_firewall_Pn.txt
Starting Nmap 7.945VN (https://nmap.org) at 2024-06-18 18:54 CEST
Nmap scan report for Windows7 (192.168.1.129)
Host is up.
All 1000 scanned ports on Windows7 (192.168.1.129) 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 214.52 seconds
Trash
File System
Home
hashes.txt
exploit
exploit
shell.elf


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Visualizzatore eventi
File Azione Visualizza
Sicurezza Numero di eventi: 1,323
Evento 4616, Microsoft Windows security auditing.
Generale Dettagli
Semplice XML
+ System
Azioni
Firefox


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(kali㉿kali)-[~]
$ cat nmap_report_no_firewall.txt
# Nmap 7.945VN scan initiated Tue Jun 18 18:47:26 2024 as: nmap -sV -oN nmap_report_no_firewall.txt 192.168.1.129
Nmap scan report for Windows7 (192.168.1.129)
Host is up (0.0023s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49156/tcp open msrpc Microsoft Windows RPC
49158/tcp open msrpc Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 18 18:48:27 2024 -- 1 IP address (1 host up) scanned in 60.70 seconds
$ cat nmap_report_with_firewall.txt
# Nmap 7.945VN scan initiated Tue Jun 18 18:49:11 2024 as: nmap -sV -oN nmap_report_with_firewall.txt 192.168.1.129
# Nmap done at Tue Jun 18 18:49:14 2024 -- 1 IP address (0 hosts up) scanned in 3.14 seconds
$ nmap -sV -Pn 192.168.1.129 -oN nmap_report_with_firewall_Pn.txt
Starting Nmap 7.945VN (https://nmap.org) at 2024-06-18 18:54 CEST
Nmap scan report for Windows7 (192.168.1.129)
Host is up.
All 1000 scanned ports on Windows7 (192.168.1.129) 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 214.52 seconds
Trash
File System
Home
hashes.txt
exploit
exploit
shell.elf


Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Visualizzatore eventi
File Azione Visualizza
Sistema Numero di eventi: 4,390
Evento 36887, Schannel
Generale Dettagli
Semplice XML
+ System
Azioni