Monitoring and Hardening Windows 10 VM with KFSensor and Nmap

Overview

In this project, I set up a Windows 10 virtual machine (VM) to monitor network traffic using KFSensor, a honeypot-based intrusion detection system. I also used Nmap from my host machine to identify open ports on the VM, then applied Windows Firewall rules to reduce the attack surface, confirming the hardening through a follow-up Nmap scan.

Tools Used

- **KFSensor** – Honeypot-based intrusion detection for monitoring traffic.
- **Nmap** – Network scanning tool for discovering open ports and services.
- **Windows Firewall** – Built-in Windows tool for managing inbound and outbound traffic.

Process

1. **Initial Setup:**
    - Installed KFSensor on the Windows 10 VM to monitor incoming traffic and log connection attempts.
    - Disabled Windows Firewall on the Windows 10 VM, increasing attack surface.
    - Ran an initial Nmap scan from the host machine to identify open ports on the VM, information that could be used maliciously by an attacker.
    - When ports such as 21, and 22 are open, attackers can take advantage.
    - KFSensor logs reflected the connection attempts and showed the services responding on open ports.
2. **Hardening:**
    - Configured Windows Firewall rules to limit exposure by closing unnecessary ports and services.
    - Focused on reducing the attack surface by allowing only essential inbound and outbound traffic.
3. **Verification:**
    - Conducted a follow-up Nmap scan from the host machine:
    - The results showed a significant reduction in open ports, confirming the effectiveness of the firewall rules.

Results

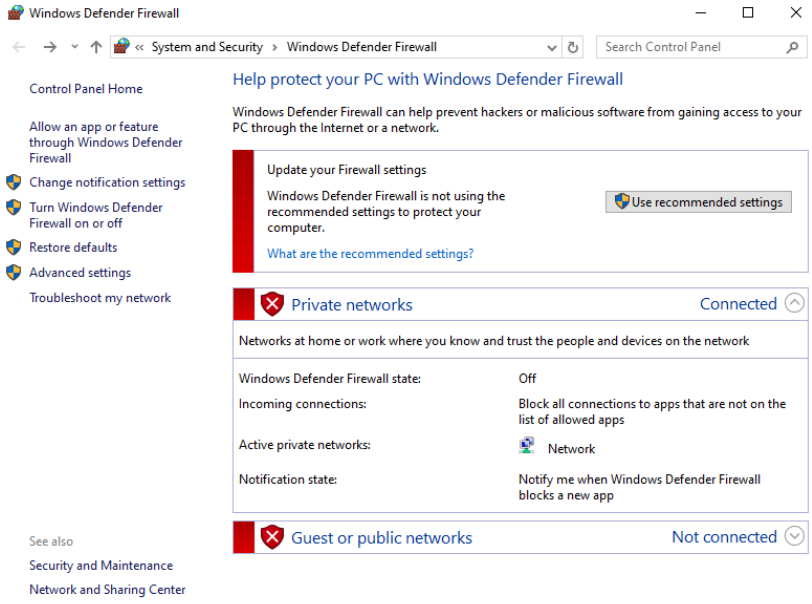
- The initial Nmap scan showed multiple open ports, exposing the VM to potential threats.
- After applying Windows Firewall rules, the number of open ports significantly decreased, strengthening the VM's security.
- KFSensor logs confirmed reduced traffic and fewer connection attempts on previously open ports.

Conclusion

This project demonstrates how to monitor and harden a Windows 10 VM using KFSensor and Nmap. By combining real-time traffic monitoring with targeted firewall configurations, I improved the VM's security posture and reduced its attack surface.

Screenshots

1. Disabling Windows Defender:



2. Initial nmap scan after installing KFSensor, and disabling Windows Firewall:

```
C:\Users\young>nmap -sS -Pn 192.168.1.87
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-19 17:37 Eastern Daylight Time
Nmap scan report for 192.168.1.87
Host is up (0.00058s latency).
Not shown: 893 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  tcpmux
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
119/tcp   open  nntp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
```

3. KFSensor reflection of nmap scan:

119	3/19/2025 2:45:42 PM....	0.000	TCP	139	NBT Session Se...	I
118	3/19/2025 2:45:42 PM....	0.000	TCP	256	TCP Syn Scan	I
117	3/19/2025 2:45:42 PM....	0.000	TCP	1720	TCP Syn Scan	I
116	3/19/2025 2:45:42 PM....	0.000	TCP	25	SMTP	I
115	3/19/2025 2:45:42 PM....	0.000	TCP	6667	TCP Syn Scan	I
114	3/19/2025 2:45:42 PM....	0.000	TCP	8654	TCP Syn Scan	I
113	3/19/2025 2:45:42 PM....	0.000	TCP	993	IMAPS	I
112	3/19/2025 2:45:50 PM....	0.000	TCP	1059	Multi-port Scan	I
111	3/19/2025 2:45:42 PM....	0.000	TCP	23	Telnet	I
110	3/19/2025 2:45:42 PM....	0.000	TCP	8888	Web Proxy	I
109	3/19/2025 2:45:42 PM....	0.000	TCP	8654	TCP Syn Scan	I
108	3/19/2025 2:45:42 PM....	0.000	TCP	6667	TCP Syn Scan	I
107	3/19/2025 2:45:42 PM....	0.000	TCP	25	SMTP	I
106	3/19/2025 2:45:42 PM....	0.000	TCP	1720	TCP Syn Scan	I
105	3/19/2025 2:45:42 PM....	0.000	TCP	256	TCP Syn Scan	I
104	3/19/2025 2:45:42 PM....	0.000	TCP	139	NBT Session Se...	I
103	3/19/2025 2:45:42 PM....	0.000	TCP	445	NBT SMB	I
102	3/19/2025 2:45:42 PM....	0.000	TCP	23	Telnet	I
101	3/19/2025 2:45:42 PM....	0.000	TCP	993	IMAPS	I

4. Nmap Scan after re-enabling Windows Firewall:

```
C:\Users\young>nmap -sS -Pn 192.168.1.87
Starting Nmap 7.93 ( https://nmap.org ) at 2025-03-19 17:45 Eastern Daylight Time
Nmap scan report for 192.168.1.87
Host is up (0.0010s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 00:0C:29:69:3C:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.35 seconds
```