Security Testing Report

Pace Massimiliano - efmpas@gmail.com

W11 D4

Sommario:

Descrizione lavoro svolto

Eseguito un set di scansioni Nmap per identificare sistema operativo, porte aperte e versioni dei servizi su VM WINDOWS 10. Sono state identificate diverse porte e servizi vulnerabili (FTP, SSH, HTTP, MySQL, ecc.). Di seguito i dettagli tecnici e le raccomandazioni operative per la mitigazione.

Target

Virtual Machine WINDOWS 10 ip 192.168.50.102

Metodologia e comandi utilizzati

OS fingerprint	sudo nmap -O 192.168.50.102
SYN Scan (stealth)	sudo nmap -sS -p- 192.168.50.102
TCP connect scan	sudo nmap -sT -p 1-65535 192.168.50.102
Version detection	sudo nmap -sV -p 21,22,80,3306 192.168.50.102

* in TCP connect abbiamo selezionato un range di porte da 1 a 65535
* in Version detection sono state scelte la porta 21,22,80,3306

Risultati ottenuti

Stato della macchina e scansioni:

La macchina Windows 10 su VirtualBox è stata sottoposta a scansione Nmap da Kali Linux, prima con il firewall disattivato e poi con il firewall attivo.

Nel caso di firewall disattivato, Nmap ha rilevato numerose porte TCP aperte, mostrando chiaramente servizi attivi come FTP (21), Telnet (23), HTTP (80), NetBIOS/SMB (139, 445), MS RPC (135), RDP (3389) e altri servizi associati a Windows. Queste porte e servizi erano accessibili e ben visibili nella scansione.

Nel caso con firewall attivo, molte porte risultavano “filtered” (filtrate) oppure non rispondevano, con un elenco di servizi molto limitato o assente. Il firewall ha bloccato la visibilità dei servizi, nascondendoli dalla scansione di rete

Sicurezza :

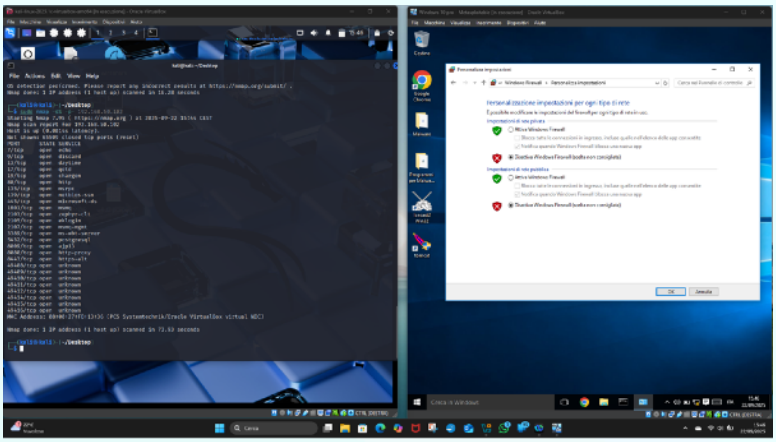
La differenza tra le due situazioni mostra chiaramente come il firewall sia essenziale per la sicurezza: quando disattivato permette facilmente il rilevamento di servizi e potenziali vulnerabilità, quando attivo protegge la macchina nascondendo la maggior parte delle porte e limitando le informazioni accessibili dall’esterno.

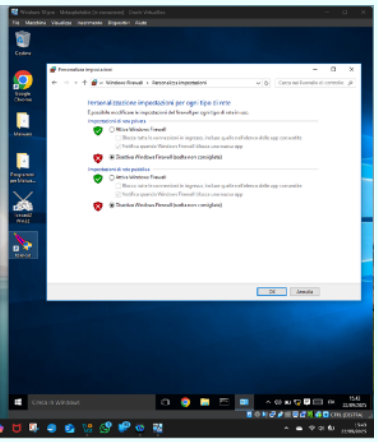
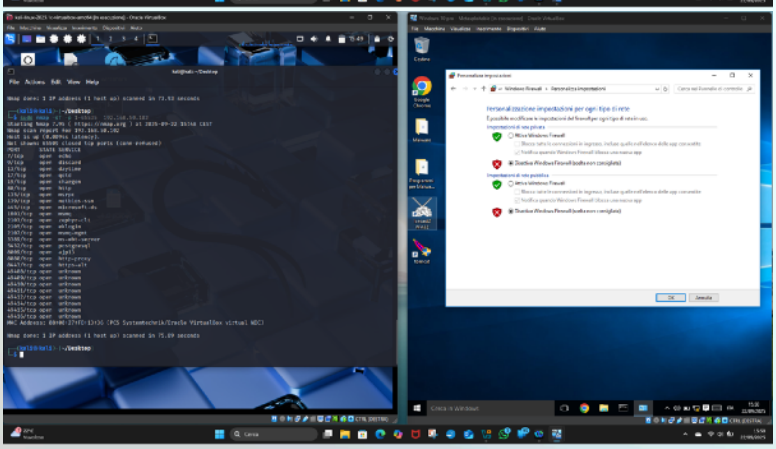
In tutte le scansioni, Nmap ha identificato il sistema operativo come “Windows 10”, e nella configurazione senza firewall sono presenti molte informazioni che potrebbero essere sfruttate per attacchi.

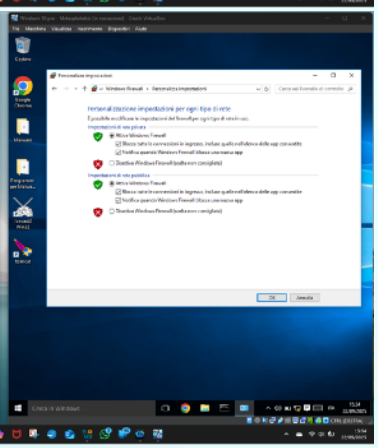
Report di scansione Nmap — 192.168.50.101

Autore: Pace Massimiliano
Data scansione: 2025-09-22
Host target: 192.168.50.102
MAC:08:00:27:FD:13:36(Oracle VirtualBox virtual NIC)
OS stimato: WINDOWS (risultato Nmap `-O`)
Note ambiente: WINDOWS in VirtualBox (scanner). L'host target e' una macchina vulnerabile/ di laboratorio

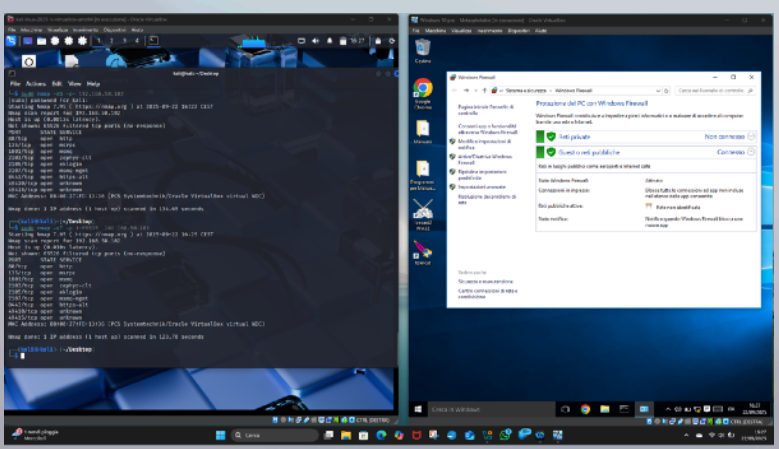
Prove fotografiche e comparazione con Firewall attivo

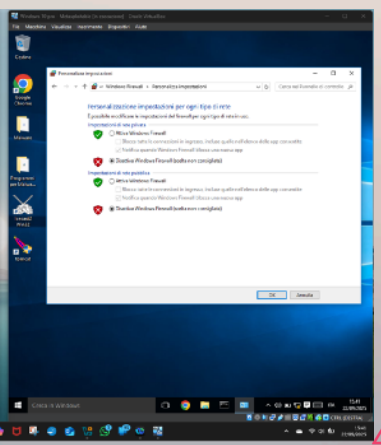


Firewall attivo



Differenze con Firewall attivo/spento

Sono state effettuate due scansioni Nmap su una macchina Windows 10 con indirizzo IP 192.168.50.102, prima con firewall disattivato e poi attivato. Entrambe le scansioni sono state eseguite da una macchina Kali Linux sulla stessa rete virtuale

Situazione con Firewall Disattivato

Numerose porte risultano aperte e visibili alla scansione, tra cui: 21 (FTP), 23 (Telnet), 80 (HTTP), 135 (MS RPC), 139 e 445 (NetBIOS), 3389 (RDP) e altre.

I servizi associati a queste porte sono elencati in modo dettagliato, evidenziando la loro esposizione alla rete.

Il sistema operativo viene identificato correttamente come Windows 10 e Nmap espone numerose informazioni sul target.

Situazione con Firewall Attivato

Diverse porte risultano non rispondere (“filtered”), e molti servizi non sono più visibili durante la scansione.

Le poche porte accessibili sono quelle permesse dalla policy del firewall (in molti casi nessuna).

Il sistema operativo Windows 10 resta identificabile, ma le informazioni sui servizi disponibili sono fortemente limitate.

Considerazioni finali

Firewall disattivato: la macchina espone numerosi servizi sensibili e risulta facilmente attaccabile.

Firewall attivato: l'esposizione è fortemente ridotta, Nmap non rivela quasi nulla, quindi la sicurezza della macchina è notevolmente aumentata.

La differenza tra le due situazioni dimostra come il firewall sia uno strumento fondamentale per la sicurezza delle reti e dei sistemi operativi Windows.

Rimedi e Consigli	Descrizione
Attivare sempre il firewall	Tenere attivo il firewall di Windows per bloccare traffico indesiderato
Regole firewall restrittive	Permettere solo traffico necessario e bloccare tutto il resto
Limitare servizi esposti	Disabilitare servizi non necessari, specialmente FTP, Telnet, NetBIOS/SMB
Aggiornare sistema e software	Installare patch di sicurezza e aggiornamenti regolari
Segmentare la rete	Usare VLAN o sottoreti per isolare macchine critiche
Usare VPN o tunnel cifrati	Proteggere l'accesso ai servizi sensibili con connessioni sicure
Monitorare log e attività	Analizzare regolarmente log firewall, sistema e servizi per attività sospette
Implementare IDS/IPS	Sistemi di rilevamento/prevenzione intrusioni per monitorare la rete
Gestione patch e backup	Utilizzare strumenti di gestione patch e backup per mantenere sicurezza