

# Nessus Scan su Metasploitable - Report

Nel report di oggi illustrerò l'utilizzo di Nessus per eseguire una scansione di vulnerabilità sul sistema Metasploitable, con l'obiettivo di identificare porte aperte e servizi potenzialmente vulnerabili.

## 1. Impostazione dell'ambiente

Per questa attività è stato utilizzato un ambiente virtuale composto da:

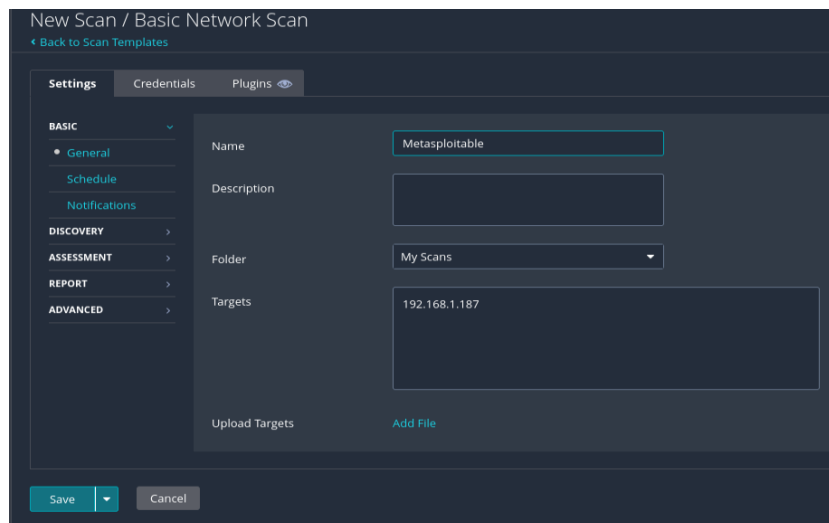
- **Macchina attaccante:** Kali Linux con Nessus installato e configurato.
- **Macchina bersaglio:** Metasploitable2, una VM vulnerabile usata a scopo didattico e di test.

Entrambe le macchine sono state collegate alla stessa rete Bridged per garantire la visibilità reciproca.

## 2. Configurazione di Nessus

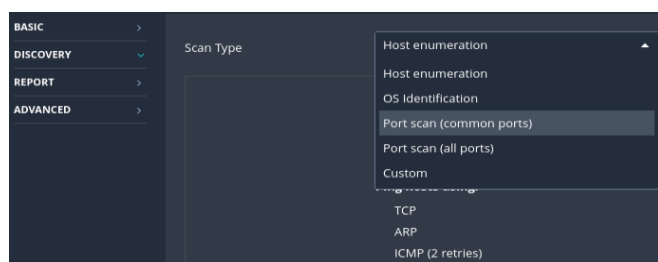
Dopo aver avviato Nessus, è stata creata una nuova scansione con i seguenti parametri:

- **Tipo di scansione:** Basic Network Scan
- **Target:** Indirizzo IP della macchina Metasploitable
- **Opzioni avanzate:** attivata la rilevazione di porte TCP/UDP e plugin completi per la valutazione di vulnerabilità.



Iniziamo creando il nostro Scan che chiameremo per comodità Metasploitable. Inserendo la Descrizione (giusto per precisione) E il **target**, che è la parte importante per raggiungere il nostro obiettivo. Inseriamo l'ip della nostra Metasploitable: 192.168.1.187

Aggiungiamo adesso una regola, andiamo su → Discovery → Scan Type → Port scan (common ports)





Questa opzione indica a Nessus di effettuare una **scansione delle porte comuni** (cioè le più frequentemente utilizzate) sul sistema bersaglio.

Informazioni Generali IP Target: 192.168.1.187

Totale vulnerabilità rilevate: 122

Critiche: 9      Alte: 6      Medie: 20      Basse: 8      Informative: 79

Filter	Search Vulnerabilities	72 Vulnerabilities						
Sev	CVSS	VPR	EPSS	Name	Family	Count	Host Details	
<input type="checkbox"/>	CRITICAL	10.0 *	8.4	0.6132	UnrealIRCd Backdoor Detection	Backdoors	1	<div>IP: 192.168.1.187</div> <div>MAC: 08:00:27:25:AC:14</div> <div>OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)</div> <div>Start: Today at 8:12 AM</div> <div>End: Today at 8:21 AM</div> <div>Elapsed: 9 minutes</div> <div>KB: <a href="#">Download</a></div> <div><b>Vulnerabilities</b></div> <div></div>
<input type="checkbox"/>	CRITICAL	10.0			Canonical Ubuntu Linux SEOL (8.04.x)	General	1	
<input type="checkbox"/>	CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1	
<input type="checkbox"/>	CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
<input type="checkbox"/>	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1	
<input type="checkbox"/>	MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4	<div>IP: 192.168.1.187</div> <div>MAC: 08:00:27:25:AC:14</div> <div>OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)</div> <div>Start: Today at 8:12 AM</div> <div>End: Today at 8:21 AM</div> <div>Elapsed: 9 minutes</div> <div>KB: <a href="#">Download</a></div> <div><b>Vulnerabilities</b></div> <div></div>
<input type="checkbox"/>	CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3	
<input type="checkbox"/>	HIGH	7.5 *	7.4	0.4664	rlogin Service Detection	Service detection	1	
<input type="checkbox"/>	HIGH	7.5 *	7.4	0.4664	rsh Service Detection	Service detection	1	
<input type="checkbox"/>	HIGH	7.5	5.9	0.7865	Samba Badlock Vulnerability	General	1	
<input type="checkbox"/>	HIGH	7.5			NFS Shares World Readable	RPC	1	
<input type="checkbox"/>	MIXED	...	...	...	SSL (Multiple Issues)	General	28	
<input type="checkbox"/>	MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5	
<input type="checkbox"/>	MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	
<input type="checkbox"/>	MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1	
<input type="checkbox"/>	MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1	
<input type="checkbox"/>	MEDIUM	5.9	3.6	0.8991	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	

## Principali Vulnerabilità Critiche

Plugin Name CVSS v3 Descrizione

(CVSS v3: indica il punteggio massimo di gravità secondo il sistema Common Vulnerability Scoring System)

1. **CVSS v3: 9.8** - Apache Tomcat AJP Connector Request Injection (Ghostcat) 9.8 - Permette accesso arbitrario a file interni e RCE tramite AJP.

**Descrizione:** Vulnerabilità nel protocollo AJP (Apache JServ Protocol) che consente a un attaccante non autenticato di leggere file interni del server o eseguire codice remoto (RCE), sfruttando l'esposizione di questo connettore.

**Impatto:** Gravissimo. Rischio di pieno controllo del server.

2. **CVSS v3: 9.8** - Bind Shell Backdoor Detection 9.8 - Rileva presenza di una backdoor con shell in ascolto.

**Descrizione:** Identifica una backdoor attiva sul sistema che apre una "bind shell", ovvero una porta di rete in ascolto che accetta connessioni remote, spesso usata da attaccanti per mantenere l'accesso.

**Impatto:** Critico. Indica una compromissione già avvenuta.

3. **CVSS v3: 9.8** - SSL Version 2 and 3 Protocol Detection 9.8 - Supporto a protocolli SSL insicuri.

**Descrizione:** Il server supporta le versioni SSL 2.0 o 3.0, che sono protocolli crittografici obsoleti e vulnerabili a numerosi attacchi (come POODLE).

**Impatto:** Elevato. Consente potenziali attacchi Man-in-the-Middle o decrittazione del traffico.

4. **CVSS v3:** 10.0 - Apache Tomcat SEoL ( $\leq 5.5.x$ ) 10.0 - Versione non più supportata con molteplici vulnerabilità note.

**Descrizione:** Versione "SEoL" (Software End of Life) di Apache Tomcat. Non riceve più aggiornamenti o patch di sicurezza, esponendo il sistema a molte vulnerabilità note.

**Impatto:** Critico. Uso di software abbandonato.

5. **CVSS v3:** 10.0 - Canonical Ubuntu Linux SEoL (8.04.x) 10.0 - Fine vita del sistema operativo, non riceve più patch.

**Descrizione:** Sistema operativo obsoleto e non più supportato da Canonical. Nessuna patch di sicurezza viene rilasciata, rendendo il sistema vulnerabile a nuovi exploit.

**Impatto:** Critico. Rischio molto alto in ambienti di produzione.

6. **CVSS v3:** 10.0 - Debian OpenSSH/OpenSSL RNG Weakness (x2 plugin) 10.0 - Generazione debole di chiavi crittografiche

**Descrizione:** Bug storico (2006-2008) in Debian che causava la generazione di chiavi crittografiche prevedibili. Due plugin possono rilevare questa debolezza sia lato client che lato server.

**Impatto:** Critico. Chiavi SSH possono essere facilmente indovinate o replicate.

7. **CVSS v3:** 10.0 - UnrealIRCd Backdoor Detection 10.0 IRC - compromesso da una backdoor nota.

**Descrizione:** Una versione compromessa del software UnrealIRCd (IRC server) venne distribuita ufficialmente con una backdoor installata. Se rilevata, indica che il sistema è già compromesso.

**Impatto:** Critico. Accesso completo da parte dell'attaccante.

8. **CVSS v3:** 10.0 - VNC Server con password predefinita 10.0 - Accesso remoto non autenticato via VNC

**Descrizione:** Un server VNC configurato con la password di default o senza password consente l'accesso remoto non autenticato.

**Impatto:** Critico. Accesso non autorizzato completo al sistema remoto.

## **Altre vulnerabilità degne di nota**

- Samba Badlock (CVE-2016-2118): vulnerabilità DoS ed escalation di privilegi.

**Descrizione:** Questa vulnerabilità interessa Samba (l'implementazione open source del protocollo SMB/CIFS usato per la condivisione file in rete).

### **Rischi principali:**

Vulnerabilità critica in Samba che consente DoS e escalation di privilegi, compromettendo la condivisione file nei sistemi aziendali.

- NFS Shares World Readable: condivisione file non protetta.

**Descrizione:** Le condivisioni NFS (Network File System) sono configurate in modo che chiunque sulla rete possa accedervi senza restrizioni di lettura.

### Rischi principali:

Le condivisioni NFS risultano accessibili a chiunque in rete, esponendo dati sensibili a lettura non autorizzata e furto di informazioni.

- rlogin/rsh detection: protocolli obsoleti e insicuri ancora attivi.

**Descrizione:** Il sistema rileva la presenza dei servizi **rlogin** e **rsh**, protocolli obsoleti per l'accesso remoto tra sistemi UNIX.

### Rischi principali:

Servizi remoti **obsoleti e non cifrati** rilevati sul sistema. Espongono **credenziali in chiaro** e vanno sostituiti con SSH.

- SSL DROWN e FREAK: protocolli e cipher deboli, potenzialmente soggetti a decrittazione.

**Descrizione:** Queste sono due **vulnerabilità crittografiche** che sfruttano configurazioni errate o protocolli obsoleti su server HTTPS o SSL/TLS.

- **DROWN** (Decrypting RSA with Obsolete and Weakened eNcryption): sfrutta la presenza di SSLv2 per decrittare connessioni TLS.
- **FREAK** (Factoring RSA Export Keys): attacca server che supportano le deboli **export cipher suites**, forzando l'uso di chiavi RSA deboli.

### Rischi principali:

Vulnerabilità che sfruttano protocolli SSL obsoleti e cifrature deboli per decrittare il traffico cifrato, con rischio di attacchi MITM e furto dati.

---

## Servizi e Protocolli Esposti

- Apache
- Tomcat
- VNC
- Telnet
- FTP
- SSH
- SMB
- MySQL, PostgreSQL
- RPC, NFS, SMTP, IRC

### Rischi Principali

- **Apache / Tomcat:** Servizi web esposti. Se non aggiornati, possono contenere vulnerabilità RCE o di accesso non autorizzato.
- **VNC:** Accesso remoto al desktop. Se non protetto da password robuste o cifratura, è facilmente attaccabile.
- **Telnet / FTP:** Protocolli non cifrati. Trasmettono credenziali in chiaro, facilitando attacchi MITM.
- **SSH:** Accesso remoto sicuro, ma da monitorare per bruteforce o configurazioni deboli.
- **SMB:** Condivisione file di rete. Espone dati sensibili e può essere vettore per worm come Wannacry.
- **MySQL / PostgreSQL:** Database accessibili da rete. Espongono dati critici se non ben configurati.
- **RPC / NFS / SMTP / IRC:** Servizi vari che, se non protetti, possono essere sfruttati per attacchi DoS, data leak o movimento laterale nella rete.

## Conclusioni del Report di Sicurezza

L'analisi ha rilevato diverse vulnerabilità critiche e configurazioni rischiose che compromettono la sicurezza complessiva dell'infrastruttura.

In particolare, è stata riscontrata la presenza di **software obsoleto o non più supportato**, come versioni legacy di Apache Tomcat e Samba, che espongono il sistema a numerosi exploit noti.

Sono attivi **servizi e protocolli insicuri** (es. Telnet, FTP, rlogin/rsh, VNC senza cifratura), che mettono a rischio la trasmissione di dati e le credenziali, favorendo potenziali accessi non autorizzati.

Alcune **vulnerabilità crittografiche**, come DROWN e FREAK, indicano l'uso di protocolli SSL obsoleti e cifrature deboli, con conseguente possibilità di **decriptazione del traffico cifrato** e attacchi Man-in-the-Middle.

È stata inoltre rilevata la **condivisione di risorse di rete senza adeguati controlli di accesso** (NFS world-readable, SMB), esponendo dati sensibili a potenziali letture non autorizzate.

Infine, la presenza di **backdoor e servizi con credenziali deboli o predefinite** rappresenta un rischio concreto di compromissione già in atto o facilmente realizzabile.

In sintesi, il livello di esposizione rilevato è elevato e richiede una revisione urgente delle configurazioni e delle tecnologie impiegate per garantire un adeguato livello di sicurezza.

In un contesto digitale sempre più ostile, ogni vulnerabilità trascurata è una porta aperta sul perimetro aziendale: la sicurezza non è un'opzione, è una priorità strategica.