

# S5E3

## Vulnerability Scanning

L'obiettivo dell'esercizio è effettuare un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

### Cosa è Nessus?

Nessus è un vulnerability scanner.

Vulnerability scanner utilizzano dei database di vulnerabilità note e controlli di sicurezza per rilevare le vulnerabilità di un sistema.

Gli scanner effettuano le verifiche delle vulnerabilità su:

- Servizi in ascolto su porte TCP / UDP.
- Configurazioni di sistemi operativi, software e piattaforme.
- Registri di Windows.

Lo scopo principale del VA è identificare le vulnerabilità e configurazioni errate che potrebbero essere sfruttate da un malintenzionato.

### Fase 1 della scansione : configurazione

In questa fase andrò a specificare su Nessus il Target, le porte da scannerizzare, e il tipo di scansione.

- Target = Metasploitable, IP 192.168.1.161/24
- Porte = 0 - 1024 (porte note)
- Tipo di scansione = Basic Network Scan (una scansione basica ma ricca di informazioni)

### Fase 2 della scansione : esecuzione

Dopo aver configurato la scansione non ci resta che attendere i risultati. Nessus impiegherà una decina di minuti per scannerizzare l'IP dato, ovviamente questo tempo salirà nel caso dovessimo scannerizzare un'intera rete.

### Fase 3 della scansione : Analisi

Ora che la scansione è terminata possiamo chiedere a Nessus di fornirci un report delle vulnerabilità. In questo caso da Pentester il nostro lavoro non finisce qui, una parte importante del lavoro è approfondire le vulnerabilità più critiche.

### Fase 4 della scansione : approfondimento

Ora andremo ad approfondire 5 vulnerabilità critiche trovate da Nessus sulla macchina metasploitable.

## Vulnerabilità 1 : Backdoor

The screenshot shows a Nessus vulnerability report for 'UnrealIRCd Backdoor Detection'. The report is categorized as 'CRITICAL'. It includes a description of the vulnerability, a solution to fix it, and a table of affected hosts. The 'Plugin Details' section provides technical information about the vulnerability, including its ID, version, type, family, and publication date. The 'VPR Key Drivers' section lists factors like threat recency and intensity. The 'Risk Information' section provides a vulnerability priority rating (VPR) and other risk metrics.

Port	Hosts
6667 / tcp / irc	192.168.1.161

Come si può vedere dall'immagine, Nessus ci fornisce una **descrizione** della vulnerabilità.

In questo caso ci dice che è stata trovata una backdoor che può permettere ad un attaccante di controllare la macchina a suo piacimento.

La **soluzione** consigliata è di scaricare nuovamente la macchina virtuale da un sito certificato, controllando che la macchina in questo caso non sia infetta.

## Vulnerabilità 2 : VNC server password

CRITICAL

VNC Server 'password' Password

< >

**Description**  
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.  
  
**Solution**  
Secure the VNC service with a strong password.  
  
**Output**  
Nessus logged in using a password of "password".  
  
To see debug logs, please visit individual host  

Port	Hosts
5900 / tcp / vnc	192.168.1.161

**Plugin Details**  
  
Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015  
  
**Risk Information**  
  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  
  
**Vulnerability Information**  
  
Default Account: true  
Exploited by Nessus: true

La seconda vulnerabilità trovata da Nessus è che la password del server VNC è la parola 'password'. Si consiglia di risolvere mettendo a protezione del server VNC una password più potente.

## Vulnerabilità 3 : versioni SSL poco sicure

CRITICAL

SSL Version 2 and 3 Protocol Detection

< >

**Description**  
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:  
  
- An insecure padding scheme with CBC ciphers.  
  
- Insecure session renegotiation and resumption schemes.  
  
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.  
  
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.  
  
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.  
  
**Solution**  
Consult the application's documentation to disable SSL 2.0 and 3.0.  
Use TLS 1.2 (with approved cipher suites) or higher instead.

**Plugin Details**  
  
Severity: Critical  
ID: 20007  
Version: 1.34  
Type: remote  
Family: Service detection  
Published: October 12, 2005  
Modified: April 4, 2022  
  
**Risk Information**  
  
Risk Factor: Critical  
CVSS v3.0 Base Score: 9.8  
CVSS v3.0 Vector: CVSS3.0#AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  
  
**Vulnerability Information**  
  
In the news: true

La terza vulnerabilità è un uso di versioni poco affidabili. In questo caso Nessus ha trovato delle vulnerabilità del servizio SSL in versione 2 e 3.

Il consiglio è di risolvere disabilitando le due versioni del servizio SSL e utilizzare il servizio TLS in versione 1.2 o più recente.

## Vulnerabilità 4 : Backdoor n2

CRITICAL

Bind Shell Backdoor Detection

< >

**Description**  
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.  
  
**Solution**  
Verify if the remote host has been compromised, and reinstall the system if necessary.

**Plugin Details**  
  
Severity: Critical  
ID: 51988  
Version: 1.10  
Type: remote  
Family: Backdoors  
Published: February 15, 2011  
Modified: April 11, 2022

È stata trovata una seconda backdoor, per risolvere si consiglia di guardare la **vulnerabilità 1**

## Vulnerabilità 5 : Versione Apache poco sicura

CRITICAL

Apache Tomcat SEoL (<= 5.5.x)

>

**Description**  
According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.  
  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.  
  
**Solution**  
Upgrade to a version of Apache Tomcat that is currently supported.

**Plugin Details**  
  
Severity: Critical  
ID: 171340  
Version: 1.5  
Type: combined  
Family: Web Servers  
Published: February 10, 2023  
Modified: May 6, 2024  
  
**Risk Information**

In questo caso la versione Apache non è aggiornata, non ha a disposizione supporto o patch per contrastare gli attacchi più moderni.