

Esercizio W12D1

Svolgiamo l'esercizio tenendo conto della seguente traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable, indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

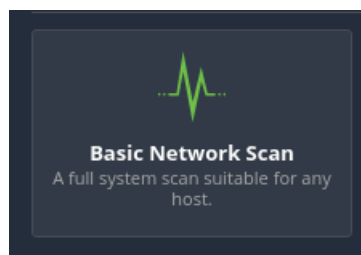
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

- Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.
- Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Preparazione scansione

Visto che andiamo per una basic network scan, non c'è molto da aggiungere se non i dati fondamentali. Le generalità e l'obiettivo della scansione, le common ports.



New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Metasploitable

Description:

Folder: My Scans

Targets: 192.168.50.100

Upload Targets [Add File](#)

Inserimento generalità

Scan Type: Port scan (common ports)

General Settings:

- Always test the local Nessus host
- Use fast network discovery

Port Scanner Settings:

- Scan common ports
- Use netstat if credentials are provided
- Use SYN scanner if necessary

Ping hosts using:

- TCP
- ARP
- ICMP (2 retries)

Scansione su common ports

Risultati

Secondo quanto trovato, andiamo ad analizzare alcune delle vulnerabilità scovate grazie allo scanner.

MEDIUM

HTTP TRACE / TRACK Methods Allowed

< >

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

See Also

<http://www.nessus.org/u?e979b5cb>
<http://www.apacheweek.com/issues/03-01-24>
<https://download.oracle.com/sunalerts/1000718.1.html>

Output

To disable these methods, add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method globally via the 'TraceEnable' [more...](#)

To see debug logs, please visit individual host

Port ▲

Hosts

80 / tcp / www

192.168.50.100

Il metodo HTTP TRACE consente di ottenere una copia di una richiesta HTTP inviata al server. Questo metodo è stato utilizzato in passato per attacchi di tipo Cross-Site Tracing (XST), che consentono a un attaccante di rubare i cookie di autenticazione di un utente. Il metodo HTTP TRACK invece è simile al metodo TRACE, non è supportato da tutti i browser, ma permette di inviare dati al server, rendendolo di fatto più pericoloso. La soluzione migliore è disabilitare i metodi totalmente.

Vulnerabilities 71

< >

CRITICAL

NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

The following NFS shares could be mounted :

```
+ /
+ Contents of / :
- .
- ..
- bin
- boot
- stream
more...
```

To see debug logs, please visit individual host

Port ▲

Hosts

2049 / udp / rpc-nfs

192.168.50.100

Un protocollo NFS(Network File System) malconfigurato può causare diversi problemi di sicurezza. Questo permette ad un utente malintenzionato di accedere a file o directory a cui non dovrebbe avere accesso. Tale protocollo potrebbe essere usato anche per inviare DoS, andando di fatto a saturare il server con richieste di servizio. Per rimuovere questo rischio occorre delegare la parte remota di NFS solo agli utenti autorizzati.

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.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u7b06c7e95>
<http://www.nessus.org/u7247c4540>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<http://www.nessus.org/u75d15ba70>
<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://tools.ietf.org/html/rfc7507>
<https://tools.ietf.org/html/rfc7568>

Output

SSL Version 2 and 3 Protocol Detection part 1

Output

- SSLv2 is enabled and the server supports at least one cipher.

Low Strength Ciphers (<= 64-bit key)

Name	Code	KEX	Auth	Encryption	MAC	
EXP-RC2-CBC-MD5		RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-RC4-MD5		RSA(512)	RSA	RC4(40)	MD5	export

more...

To see debug logs, please visit individual host

Port	Hosts
25 / tcp / smtp	192.168.50.100

- SSLv3 is enabled and the server supports at least one cipher.

Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC	
EXP-RC2-CBC-MD5		RSA(512)	RSA	RC2-CBC(40)	MD5	export
EXP-RC4-MD5		RSA(512)	RSA	RC4(40)	MD5	export

more...

To see debug logs, please visit individual host

Port	Hosts
5432 / tcp / postgresql	192.168.50.100

SSL vulnerability parte 2

In questo caso la vulnerabilità sta nel fatto che la porta 5432 monta il protocollo SSL(secure socket layers) 2.0 e 3.0. Essi sono deprecati per via degli attacchi che li hanno scoperti in passato. Un esempio di quest'ultimi sono il Padding Oracle, che decifra parte del testo cifrato mediante lo sfruttamento del pattern MAC-than-encrypt, oppure semplicemente il BIAS, che sfrutta la debolezza dei cifrari basati su RC4. Per eliminare un tale problema il modo migliore sarebbe sostituire SSL con il ben noto e moderno protocollo di sicurezza TLS(transport layer security) 1.2.

Vulnerabilities 71

CRITICAL Unix Operating System Unsupported Version Detection

Description
According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a version of the Unix operating system that is currently supported.

Output
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server).
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : <https://wiki.ubuntu.com/Releases>

To see debug logs, please visit individual host

Port	Hosts
N/A	192.168.50.100

Dopo lo scan Version Detection del sistema operativo, emerge come la macchina sfoggi una versione non più supportata. Non è solo un fatto di prestazioni, ma anche di carenza di aggiornamenti riguardo la sicurezza del dispositivo. La soluzione a tale vulnerabilità è l'aggiornamento all'ultima versione di Unix.

CRITICAL

UnrealIRCd Backdoor Detection

< >

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output

```
The remote IRC server is running as :  
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port ▲	Hosts
6667 / tcp / irc	192.168.50.100 🔗

UnrealIRCd Backdoor vulnerability

Lo scanner identifica all'interno di UnrealIRCd(un server Internet Relay Chat open source) una backdoor che consente ad un attaccante la possibilità di eseguire comandi arbitrari sul server. Per scongiurare il rischio dobbiamo reinstallare una versione pulita del software.