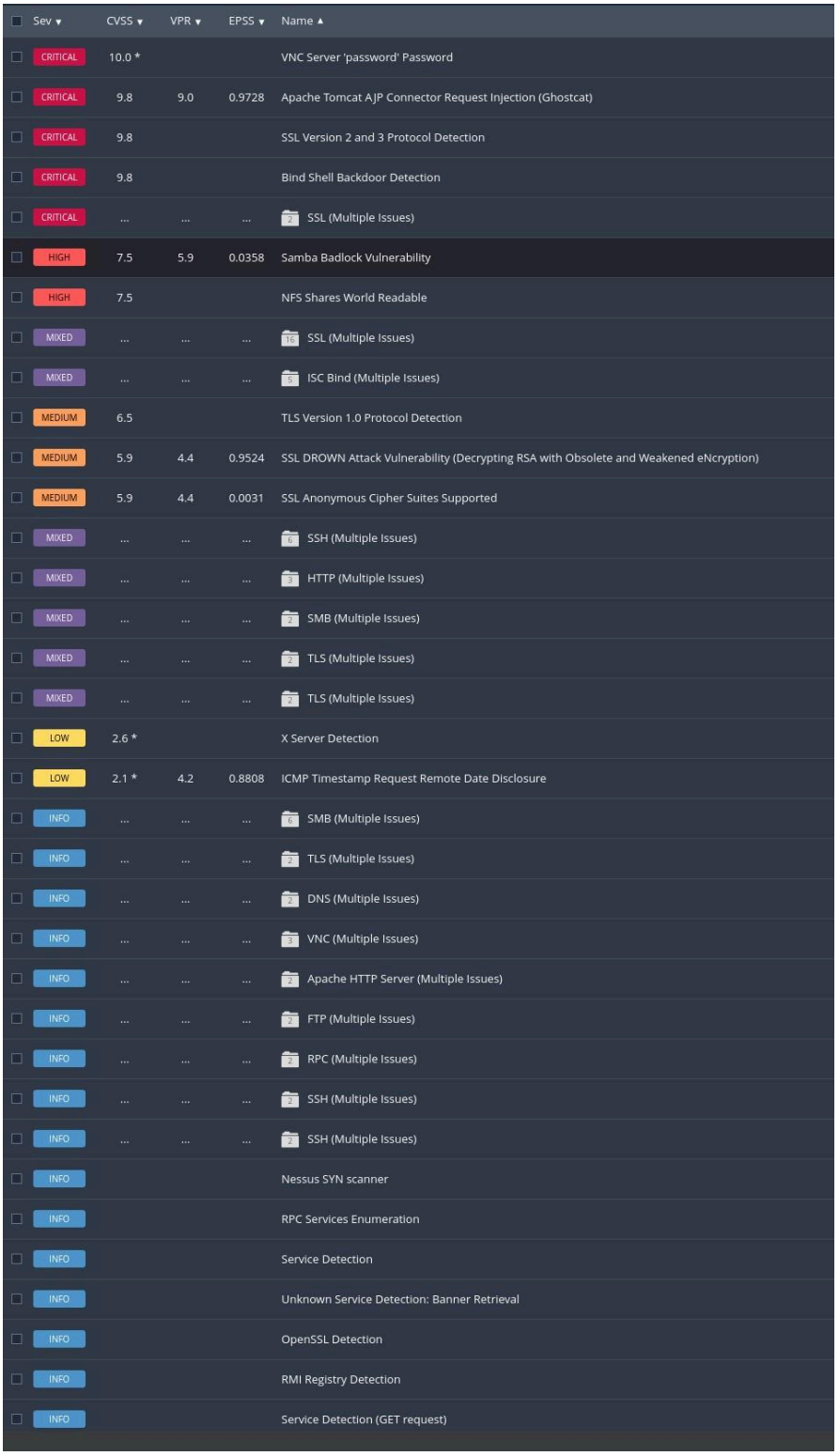
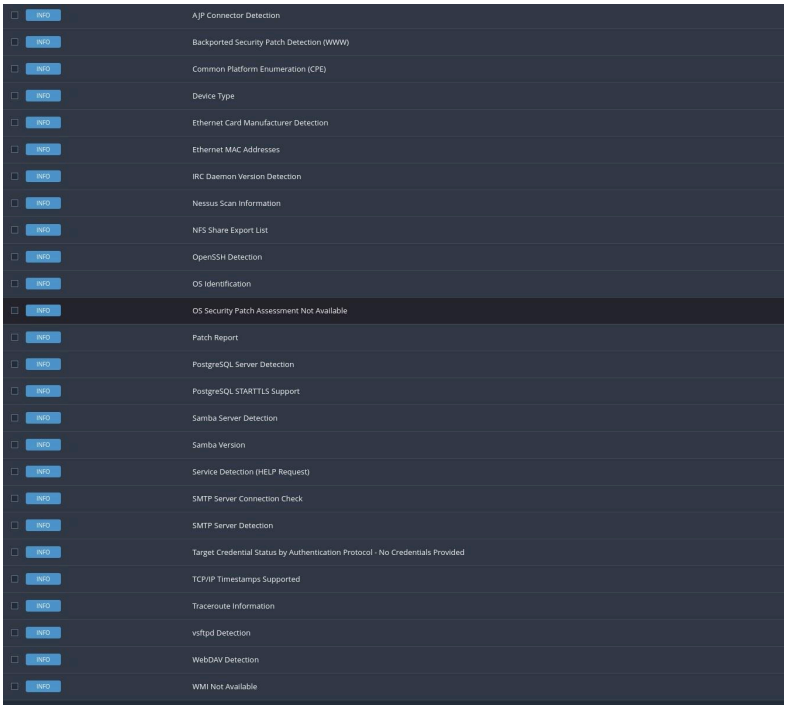
Esercizio S5L3 - Nessus e scansione di rete

L’esercizio di oggi prevedeva la scansione di Metasploitable2 (volutamente vulnerabile, quindi) per impratichirci con l’utilizzo di Nessus e vedere un primo esempio di report.
Qui la lista delle 61 vulnerabilità individuate:



Sev	CVSS	VPR	EPSS	Name
CRITICAL	10.0 *			VNC Server 'password' Password
CRITICAL	9.8	9.0	0.9728	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8			Bind Shell Backdoor Detection
CRITICAL	...	...	...	SSL (Multiple Issues)
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability
HIGH	7.5			NFS Shares World Readable
MIXED	...	...	...	SSL (Multiple Issues)
MIXED	...	...	...	ISC Bind (Multiple Issues)
MEDIUM	6.5			TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites Supported
MIXED	...	...	...	SSH (Multiple Issues)
MIXED	...	...	...	HTTP (Multiple Issues)
MIXED	...	...	...	SMB (Multiple Issues)
MIXED	...	...	...	TLS (Multiple Issues)
MIXED	...	...	...	TLS (Multiple Issues)
LOW	2.6 *			X Server Detection
LOW	2.1 *	4.2	0.8808	ICMP Timestamp Request Remote Date Disclosure
INFO	...	...	...	SMB (Multiple Issues)
INFO	...	...	...	TLS (Multiple Issues)
INFO	...	...	...	DNS (Multiple Issues)
INFO	...	...	...	VNC (Multiple Issues)
INFO	...	...	...	Apache HTTP Server (Multiple Issues)
INFO	...	...	...	FTP (Multiple Issues)
INFO	...	...	...	RPC (Multiple Issues)
INFO	...	...	...	SSH (Multiple Issues)
INFO	...	...	...	SSH (Multiple Issues)
INFO				Nessus SYN scanner
INFO				RPC Services Enumeration
INFO				Service Detection
INFO				Unknown Service Detection: Banner Retrieval
INFO				OpenSSL Detection
INFO				RMI Registry Detection
INFO				Service Detection (GET request)



Vulnerabilità critiche e breve descrizione:

1) **Apache Tomcat AJP Connector Request Injection**: Vulnerabilità che consente l'invio di JSP malevole per effettuare esecuzione di codice da remoto. Nessus ci suggerisce di aggiornare il server Tomcat a una versione successiva.
2) **SSL Version 2 and 3 Protocol Detection**: Individua l'uso di protocolli SSL 2 e 3, considerati insicuri e vulnerabili agli attacchi. Nessus suggerisce di disabilitare SSL 2 e 3, e passare a TLS.
3) **Debian Open SSL/SSH**: La vulnerabilità riguarda il generatore di numeri casuali di Debian OpenSSL, che compromette le chiavi crittografiche. Il controllo SSL verifica questa debolezza per mitigare rischi di compromissione delle chiavi. Nessus ci suggerisce di rigenerare tutto ciò che è stato generato originariamente con questi, in quanto potrebbero essere facilmente indovinabili con un attacco di tipo brute force.
4) **Bind Shell Remote Protection**: Indica la presenza di una backdoor di tipo "bind shell" che consente accesso remoto non autorizzato al sistema. Nessus ci suggerisce di verificare se l'host remoto è stato compromesso, e di reinstallare il sistema qualora necessario.
5) **VNC Server Password 'Password'**: la password di accesso è "password", essendo piuttosto debole Nessus ci suggerisce di modificarla.

CRITICAL

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

See Also

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

Output

```
Nessus was able to exploit the issue using the following request :

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040:  00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050:  63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060:  0F 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00    .en-US,en;q=0.5.
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
8009 / tcp / ajp13	192.168.1.5

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/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

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	192.168.1.5

```
- 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
    ---------------------        ----------       ---           ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA                          DH            RSA      3DES-CBC(168)          SHA1
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.1.5

CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.1.5
25 / tcp / smtp	192.168.1.5

CRITICAL

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
22 / tcp / ssh	192.168.1.5

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.

Output

```
Nessus was able to execute the command "id" using the
following request :


This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.5

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	192.168.1.5