

## **Scansione e rilevamento delle vulnerabilit  tramite l' utilizzo dello scanner NISSUS .**

NISSUS   un Vulnerabilit  scanner che utilizza dei database di vulnerabilit  note e controlli di sicurezza per rilevare le vulnerabilit  di un sistema come :

Servizi in ascolto sulle porte TCP/UDP

Configurazioni di OS e software di gestione

Registri di Windows

Lo scopo principale di questa scansione   quello di identificare le vulnerabilit  e configurazioni errate che potrebbero essere sfruttate da un attaccante.

### **Funzionamento di Nissus**

La scansione avviene in 4 step:

1. Port scanning attraverso il quale il Tool capisce se il host   attivo in rete o meno , qual ora fosse attivo avviene la scansione delle porte per capire quale porta   attiva e quale no.
2. Per ogni porta aperta ,lo scanner attraverso l' analisi del traffico riesce a individuare che tipo di servizio   attivo sulla porta e da quale software e versione   gestito.
3. Per ogni servizio rilevato, lo scanner utilizzando il proprio database , andr  a ricercare le vulnerabilit  note per quel particolare tipo di applicazione / tecnologia.
4. Nella fase finale lo scanner effettua dei test sul target per verificare se sono affetti dalla vulnerabilit  in esame.

Scansione sistema target IP 192.168.1.11

Impostazione esercizio

Entrambi i sistemi (kali) e (meta) devono essere sulla stessa subnet .

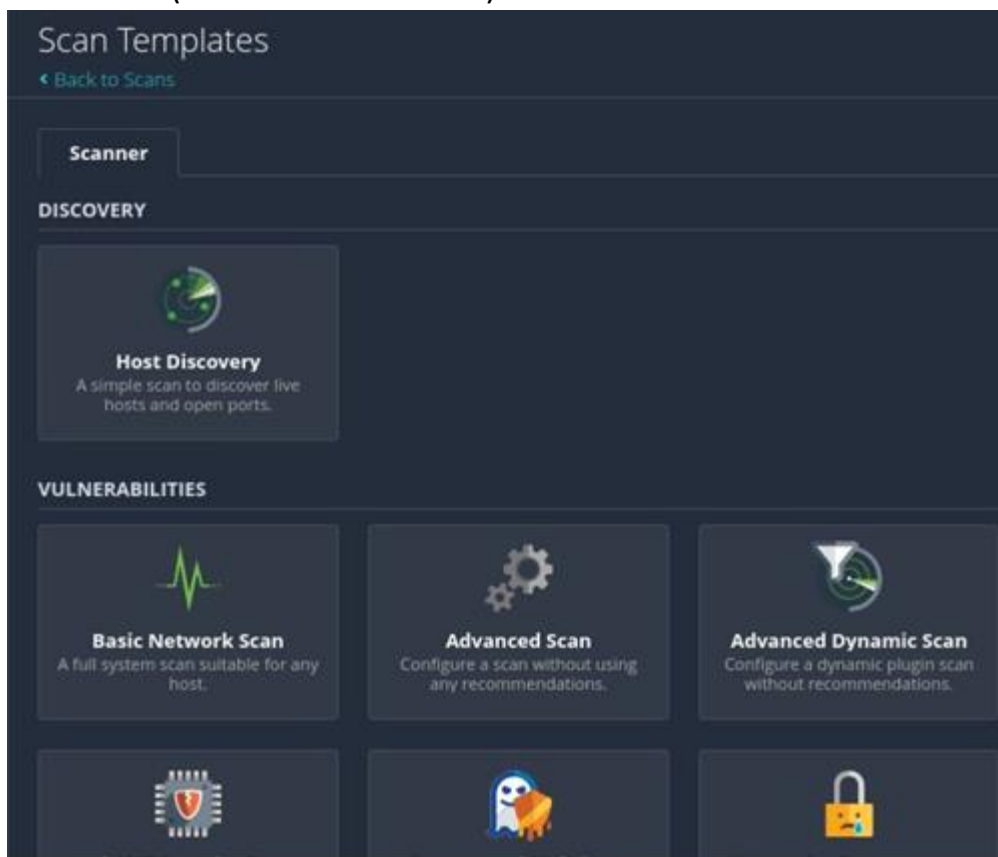
Impostazione di Nissus

Avviare kali ed eseguire il comando per l' attivazione del servizio nissusd

```
(kali@kali)-[~]  
$ systemctl start nessusd.service  
  
(kali@kali)-[~]  
$
```

Il servizio è in ascolto sulla porta 8834 sul localhost

Iniziamo con (create new scan) e selezioniamo il tipo di scansione da effettuare ( Basic Network Scan)



Inseriamo le informazioni richieste all'interno delle schede sulla destra. Il nostro target sarà la macchina Metasploitable. Nella scheda discovery, selezionare «port scan (common ports)»


Completare le altre schede e salvare la scansione

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

### Settings

Credentials

Plugins 

#### BASIC

• General

Schedule

Notifications

#### DISCOVERY

#### ASSESSMENT

#### REPORT

#### ADVANCED

Name

msd scan

Description

Meta 2 Vulnerabilita

Folder

My Scans

Targets

192.168.1.11/24

Upload Targets


[Add File](#)

## New Scan / Basic Network Scan

[← Back to Scan Templates](#)

### Settings

Credentials

Plugins 

#### BASIC

#### DISCOVERY

#### ASSESSMENT

#### REPORT

#### ADVANCED

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

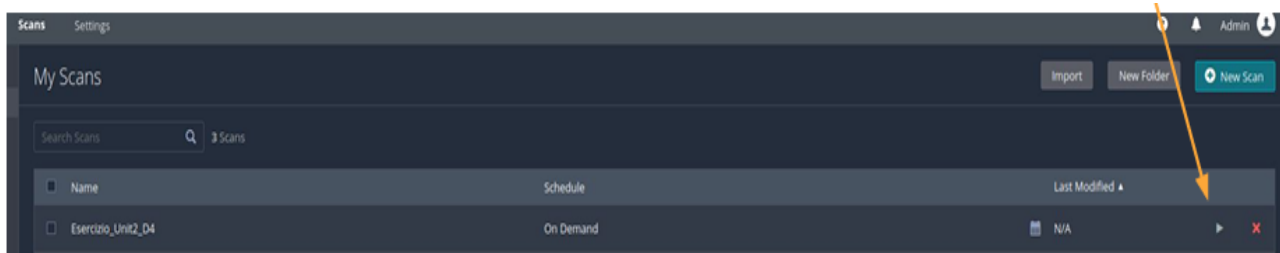
#### Ping hosts using:

TCP

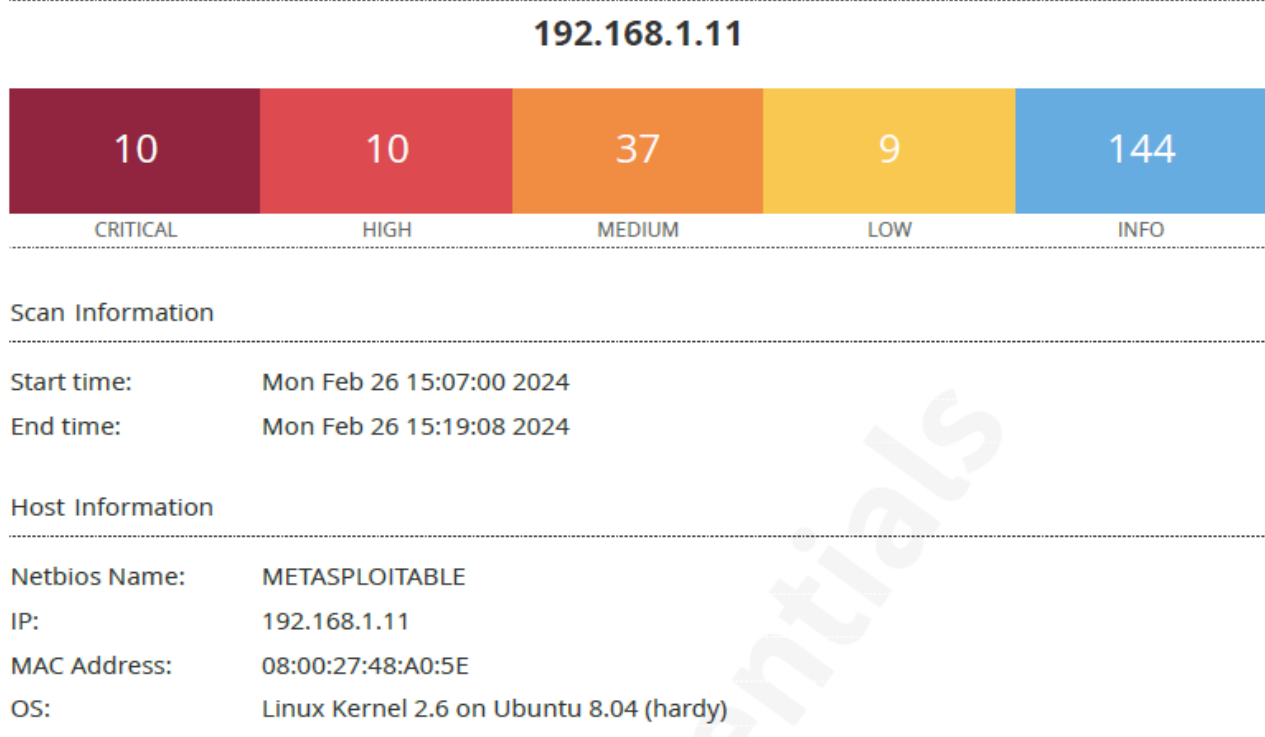
ARP

ICMP (2 retries)

Nella sezione (my scan) avviare la scansione premendo su “play”



Al termine della scansione NESSUS produrrà un report con tutte le vulnerabilità trovate, la descrizione di esse, e il modo di chiuderle.



Nella prima parte del report verranno indicate le info generali sul sistema scansionato e le vulnerabilità identificate e classificate per gravità.

Esempio di vulnerabilità identificate:

-51988 – Bind shell Backdor Detection

Synopsis

Il host può essere compromesso da remoto

Descrizione: la shell può ricevere comandi da remoto senza autorizzazione richiesta in precedenza. Un attaccante può accedere alla porta e inserire comandi da remoto.

Soluzione : verificare se la porta e stata compromessa e reinstallare il sistema se necessario

#### Risk Factor

---

Critical

#### 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 v2.0 Base Score

---

192.168.1.11

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

#### Plugin Information

---

Published: 2011/02/15, Modified: 2022/04/11

#### Plugin Output

---

tcp/1524/wild\_shell

```
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 -----
```

### 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

La chiave SSH e debbole

Descrizione:

La chiave SSH e stata generata da Debian o Ubuntu contiene un bug nella generazione casuale dei numeri nella libreria Open SSL

Questo problema e dovuto al fatto che Debian ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un attaccante puo facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man in the midle.

Fonti:

<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

Considera tutto il materiale crittografico generato sull'host remoto come indovicabile. In particolare, tutti i materiali chiave SSH, SSL e OpenVPN dovrebbero essere rigenerato

#### Risk Factor

---

Critical

#### VPR Score

---

5.1

#### CVSS v2.0 Base Score

---

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

#### CVSS v2.0 Temporal Score

---

8.3 (CVSS2#E:F/RL:OF/RC:C)

#### References

---

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

---

192.168.1.11

Exploitable With

---

Core Impact (true)

Plugin Information

---

Published: 2008/05/14, Modified: 2018/11/15

Plugin Output

---

tcp/22/ssh

## 70728 - Apache PHP-CGI Remote Code Execution

La versione di PHP è datata

Descrizione:

L'installazione di PHP sul server web remoto contiene un difetto che potrebbe consentire il passaggio di un utente malintenzionato remoto

argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Si potrebbe abusare di questo eseguire codice arbitrario, rivelare codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

soluzione:

Aggiornare il PHP alla versione più recente

## 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

---

8.9

## 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)

## References

---

BID	53388
CVE	CVE-2012-1823
CVE	CVE-2012-2311
CVE	CVE-2012-2335
CVE	CVE-2012-2336
XREF	CERT:520827

---

192.168.1.11



XREF EDB-ID:29290  
XREF EDB-ID:29316  
XREF CISA-KNOWN-EXPLOITED:2022/04/15

#### Exploitable With

CANVAS (true) Core Impact (true) Metasploit (true)

#### Plugin Information

Published: 2013/11/01, Modified: 2023/04/25

#### Plugin Output

tcp/80/www

```
Nessus was able to verify the issue exists using the following request :

----- snip -----
POST /cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E HTTP/1.1
Host: PC192.168.1.11
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 115
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
<?php echo "Content-Type:text/html\r\n\r\n"; echo 'php_cgi_remote_code_execution-1708978536';
system('id'); die; ?>
----- snip -----
```

## 10245 - rsh Service Detection

Il servizio rsh e in esecuzione sul remote host

Descrizione:

il servizio rsh e in esecuzione su questo sistema ,il servizio rsh e datato.

Un man in the middle puo sfruttarlo per riuscire a captare i logins con le relative password

Soluzione:

disattivare il servizio rsh da line in /etc/inetd.conf , e passare a SSH.

#### Risk Factor

---

High

#### VPR Score

---

5.9

#### CVSS v2.0 Base Score

---

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

#### References

---

CVE CVE-1999-0651

#### Exploitable With

---

Metasploit (true)

#### Plugin Information

---

Published: 1999/08/22, Modified: 2022/04/11

#### Plugin Output

---

tcp/514/rsh

### 11411 - Backup Files Disclosure

E possibile recuperare i file di backups da un remote web server.

#### Descrizione

Dalle varie terminazioni finali di un file (ie: .old, .bak, ~, etc...)e possibile recuperare il loro contenuto con la possibilita di perdere dati sensibili

#### Fonti

<http://www.nessus.org/u?8f3302c6>

#### Soluzione

Assicurarsi che i file non contengano info sensibili, come credenziali d accesso , cancellare o proteggere (criptografare) questi files .

## Risk Factor

---

Medium

## CVSS v2.0 Base Score

---

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

## Plugin Information

---

Published: 2003/03/17, Modified: 2023/07/10

## Plugin Output

---

tcp/80/www

```
It is possible to read the following backup files :
```

- File : /twiki/bin/view/Main/WebHome~  
URL : http://PC192.168.1.11/twiki/bin/view/Main/WebHome~
- File : /twiki/bin/search/Main/SearchResult~  
URL : http://PC192.168.1.11/twiki/bin/search/Main/SearchResult~