

Analisi delle vulnerabilità: Porte della metasploitable scanner:

L'obiettivo dell'esercizio è quello di fornire una **Vulnerability Assessment** (Valutazione delle vulnerabilità) che non è altro di una revisione manuale e quindi più approfondita della **Vulnerability Scanner** (Scanner di vulnerabilità) è uno strumento software automatizzato che esegue una scansione di un sistema o di una rete alla ricerca di vulnerabilità conosciute. Quindi si unisce la scansione automatica con l'analisi manuale per valutare la sicurezza di sistema con le specifiche di una determinata azienda e gestire la gravità del pericolo per una eventuale pianificazione delle soluzioni o penetration test.

Vulnerability Scanner

a) Passaggi vulnerability scanner

Come strumento di scanner andremo ad utilizzare Nessus, come da prassi è uno strumento che va sempre aggiornato periodicamente per avere dei database sempre forniti dei nuovi controlli.

Nessus è uno strumento molto usato essendo potente e semplice da usare ci fornisce molte opzioni di utilizzo dei quali i passaggi principali sono:

- 1) port scanning
- 2) service detection
- 3) ricerca nel vulnerability database
- 4) test

b) Architettura Nessus

Nessus ha due componenti principali: un server e un client.

- 1) Il client: configura le scansioni per determinare i target ip e le modalità di scansione e test.
- 2) Il server: si occupa di effettuare i test sugli obiettivi specificati dal client.
- 3) Al termine delle scansioni il server confronta le risposte con il proprio database di vulnerabilità.

c) Struttura della rete

All'interno di una **rete interna** andremo ad utilizzare Nessus con il sistema operativo Kali, per analizzare le vulnerabilità di sicurezza delle porte della macchina metasploitable presente all'interno della stessa rete interna, all'epicentro della quale troviamo la Pfsense che definisce i collegamenti con le macchine interessate.

Vulnerability Assessment

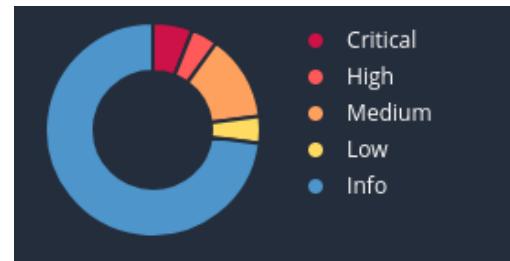
a) report vulnerability scanner

al termine del vulnerability scanner il programma automatizzato ci restituirà un report delle valutazioni grazie all'utilizzo del database delle vulnerabilità, elencando quali vulnerabilità sono più critiche divise per colore di priorità, troviamo i parametri:

- Critical
- High
- Medium
- Low
- Info

Il report che andremo ad analizzare contiene:

- Una soluzione.
- Fattore rischio.
- Score nel sistema CVSS.
- Informazioni sul plugin di Nessus che ha identificato la vulnerabilità.



b) Nessus

Andando a esaminare quella che è la scansione delle vulnerabilità che abbiamo trovato su metasploitable troviamo la il seguente risultato:

Vulnerabilities 71					
Filter ▾ Search Vulnerabilities Q 71 Vulnerabilities				Family ▾	Count ▾
Sev ▾	CVSS ▾	VPR ▾	EPSV ▾	Name ▾	
□ CRITICAL	10.0 *	7.4	0.8622	UnrealIRCd Backdoor Detection	Backdoors 1
□ CRITICAL	10.0			Canonical Ubuntu Linux SEOl (8.04.x)	General 1
□ CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely 1
□ CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection 2
□ CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors 1
□ MIXED	Apache Tomcat (Multiple issues)	Web Servers 4
□ CRITICAL	SSL (Multiple issues)	Gain a shell remotely 3

b0) Rilevamento backdoor UnrealIRCd

Vulnerabilities 71	
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.	

descrizione: ci dice che Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato. Più nel dettaglio è una versione di molto tempo fa e la backdoor consente a chiunque di eseguire qualsiasi comando con i privilegi dell'utente indipendentemente dalle restrizioni. di fatto è una vulnerabilità estremamente pericolosa a cui diamo estrema priorità.

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 192.168.50.12
```

soluzione: infatti consiglia di Scaricare nuovamente il software e verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

b1) Canonical Ubuntu Linux SEoL (8.04.x)

CRITICAL Canonical Ubuntu Linux SEoL (8.04.x)

Description
According to its version, Canonical Ubuntu Linux is 8.04.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.

descrizione: in quest'altra vulnerabilità critica ci dice che la versione di Canonical Ubuntu Linux versione 8.04.x, non è più supportata dal suo fornitore, ciò implica che questa versione non è più all'avanguardia per la sicurezza e potrebbe essere fonte di molte vulnerabilità.

Output

```
OS : Ubuntu Linux 8.04  
Security End of Life : May 9, 2013  
Time since Security End of Life (Est.) : >= 12 years  
  
To see debug logs, please visit individual host  
Port ▾ Hosts  
80 / tcp / www 192.168.50.12
```

soluzione: quindi ci consiglia di aggiornare Canonical Ubuntu Linux con una versione attualmente supportata.

b2) Bind Shell Backdoor Detection

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.

descrizione: qui ci avverte di una shell che è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Quindi un aggressore può utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

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	192.168.50.12 <input checked="" type="checkbox"/>

soluzione: ci consiglia di verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

Conclusione

Il Vulnerability Assessment è una parte essenziale della fase di raccolta informazioni del Penetration Testing, è la parte dove si unisce l'automazione della macchina con la manualità del hacker e ottenere un risultato estremamente dettagliato delle vulnerabilità di interesse. Al termine di questa fase avremo un quadro generale completo della struttura e delle vulnerabilità del nostro target, non che l'inizio della fase successiva, il vero e proprio attacco.