Scansione vulnerabilità

Ho eseguito una scansione per trovare delle vulnerabilità su Metasploitable con il software Nessus,

tenable Nessus

Report generated by Nessus™

Metasploitable

Thu, 09 May 2024 07:21:25 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.50.101

Vulnerabilities by Host

Collapse All | Expand All

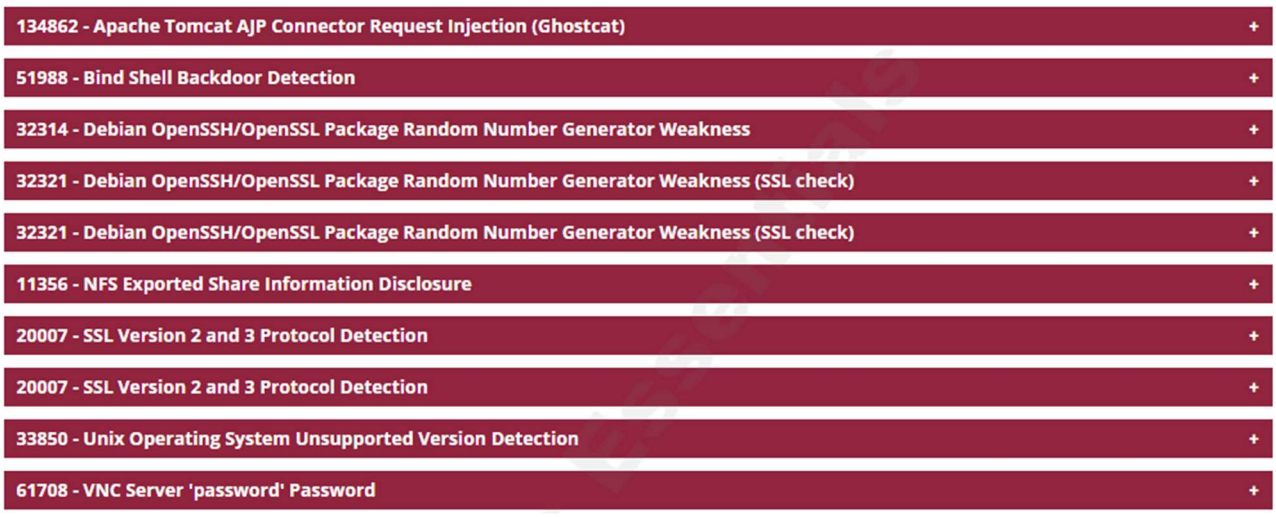
192.168.50.101

10	5	24	8	128
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu May 9 06:55:57 2024
End time:	Thu May 9 07:21:25 2024

e sono state 47 vulnerabilità, tra cui 10 critiche



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

51988 - Bind Shell Backdoor Detection +

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

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) +

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) +

11356 - NFS Exported Share Information Disclosure +

20007 - SSL Version 2 and 3 Protocol Detection +

20007 - SSL Version 2 and 3 Protocol Detection +

33850 - Unix Operating System Unsupported Version Detection +

61708 - VNC Server 'password' Password +

Per ogni vulnerabilità sono presenti delle informazioni che descrivono il problema e propongono soluzioni, adesso andremo ad analizzare le 10 vulnerabilità critiche:

1. Una vulnerabilità di lettura dei file è stata trovata nel connector AJP, un utente remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni Web da un server.
   La soluzione proposta è di modificare le configurazioni di AJP e aggiornare il server Tomcat;

2. È stata trovata una backdoor e il software propone di reinstallare il sistema, però prima di eseguire un'azione drastica sarebbe meglio provare ad installare un software che rimuove in automatico la backdoor come Fortect o SpyHunter5 oppure provare a toglierla manualmente;

3. Le chiavi remote generate sul sistema Ubuntu contiene un bug, e un utente esterno può ottenere la chiave privata e decifrare la sessione remota. È necessario rigenerare le chiavi SSH;

4. Le chiavi remote generate sul sistema Ubuntu contiene un bug, e un utente esterno può ottenere la chiave privata e decifrare la sessione remota. È necessario rigenerare le chiavi SSL;

5. Stesso problema del numero 4;

6. È possibile accedere alle condivisioni NFS da remoto, e potrebbe essere in grado di leggere (e possibilmente scrivere) file, la soluzione è configurare NFS sull'host remoto in modo che solo gli host autorizzati possano accedere;

7. Il servizio remoto crittografa SSL 2.0 o SSL 3.0 usa un protocollo con vulnerabilità note. Bisogna disabilitare SSL 2.0 e SSL 3.0 e usare TLS 1.2 o versioni successive;

8. Stesso problema del numero 7;

9. Il sistema operativo non è più aggiornato quindi non verranno fornite nuove patch ed è molto probabile che ci siano delle vulnerabilità;

10. Un server VNC è protetto da una password debole “password”, ed è molto facile da scoprire con un attacco brute force con dizionari.

La prima cosa da fare è quella di concentrarsi su queste vulnerabilità per risolverle e poi passare man mano a quelle meno gravi.

In allegato lascio un file contenente tutte le vulnerabilità che dovranno essere sistemate dopo quelle critiche.