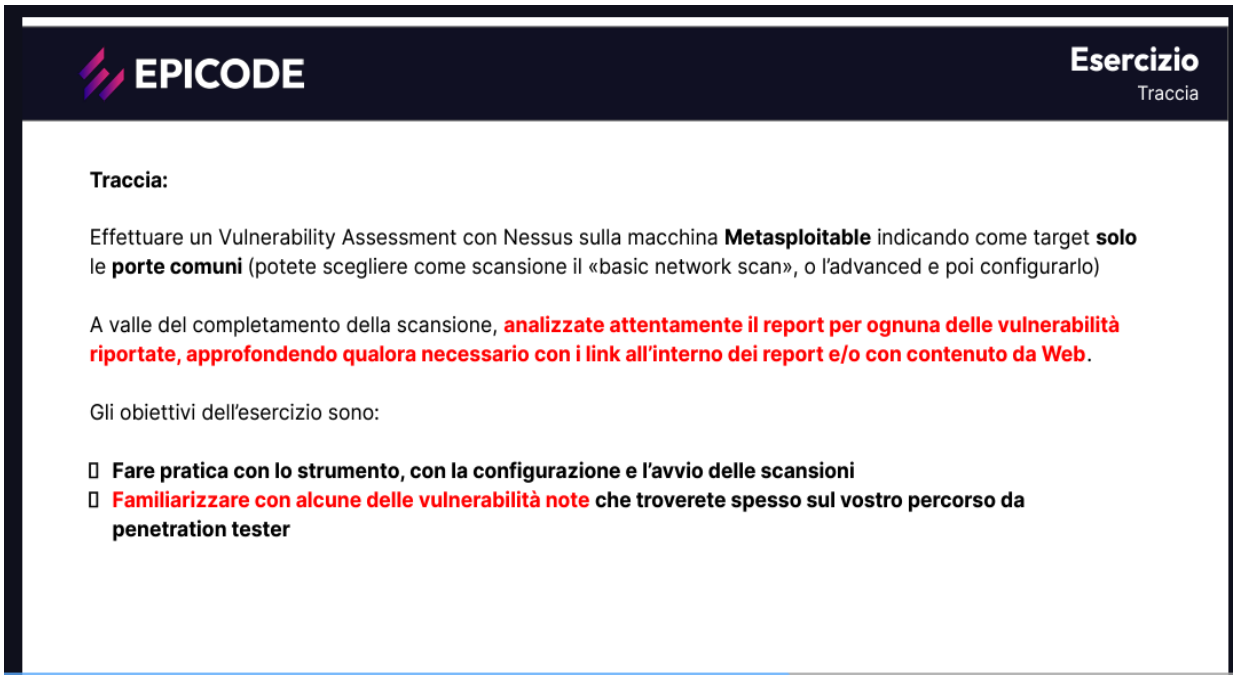
ESERCITAZIONE W12 D1(1)



192.168.1.15

6	1	21	7	68
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
MEDIUM	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	7.5	-	42256	NFS Shares World Readable
MEDIUM	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	-	136808	ISC BIND Denial of Service

SSL Version 2 and 3 Protocol Detection

Il servizio remoto crittografa il traffico utilizzando SSL 2.0 e SSL 3.0, che hanno punti deboli noti come schemi di riempimento insicuri e rinegoziazione non sicura delle sessioni. Queste vulnerabilità possono essere sfruttate per attacchi man-in-the-middle o decrittazione delle comunicazioni. Si raccomanda di disattivare SSL 2.0 e SSL 3.0 e passare a TLS 1.2 o versioni successive con suite di crittografia sicure.

Unix Operating System Unsupported Version Detection

Il sistema operativo dell'host remoto ha raggiunto la fine del supporto.L'host remoto esegue un sistema operativo Unix che non è più supportato, come indicato dal numero di versione. Questo significa che il fornitore non rilascerà ulteriori patch di sicurezza per questo sistema operativo. Pertanto, è probabile che il sistema presenti vulnerabilità di sicurezza.Soluzione:Per affrontare questa situazione, è consigliabile eseguire l'aggiornamento a una versione supportata del sistema operativo Unix.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Le chiavi dell'host SSH remoto sono deboli a causa di un bug nel generatore di numeri casuali della libreria OpenSSL su sistemi Debian o Ubuntu. Questo è dovuto alla rimozione di fonti di entropia da parte di un packager Debian, rendendo la parte privata della chiave facilmente ottenibile da un utente malintenzionato. Si consiglia di rigenerare tutto il materiale crittografico, inclusi le chiavi SSH, SSL e OpenVPN, sull'host remoto.

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

Il certificato SSL remoto utilizza una chiave debole a causa di un bug nel generatore di numeri casuali della libreria OpenSSL su sistemi Debian o Ubuntu. Questo problema è dovuto alla rimozione di fonti di entropia da parte di un packager Debian, rendendo la parte privata della chiave facilmente ottenibile da un utente malintenzionato. Si raccomanda di rigenerare tutto il materiale crittografico, inclusi i certificati SSL, sul server remoto per garantire la sicurezza delle comunicazioni.

UnrealIRCd Backdoor Detection

Il server IRC remoto è compromesso da una backdoor.Il server IRC remoto utilizza una versione di UnrealIRCd che contiene una backdoor. Questo permette a un utente malevolo di eseguire codice arbitrario sull'host interessato.Per risolvere il problema, è necessario scaricare nuovamente il software da una fonte affidabile, verificare l'integrità utilizzando i checksum MD5/SHA1 pubblicati e quindi reinstallarlo sul server remoto.

VNC Server 'password' Password

Il server VNC remoto è vulnerabile a causa di una password debole impostata come "password", consentendo a un attaccante non autenticato di assumere il controllo del sistema.Per proteggere il server VNC, è fondamentale utilizzare una password complessa e sicura. Si consiglia di creare una nuova password che contenga una combinazione di caratteri alfanumerici e speciali, garantendo una lunghezza adeguata per aumentare la sicurezza. Subito dopo, è importante sostituire la vecchia password debole con la nuova.

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Un connettore AJP vulnerabile è in ascolto sull'host remoto, esponendo il sistema a una vulnerabilità di lettura/inclusione di file. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questa vulnerabilità per accedere ai file delle applicazioni Web o eseguire codice dannoso.Per

risolvere il problema, è necessario aggiornare la configurazione del connettore AJP per richiedere l'autenticazione e/o aggiornare il server Tomcat a una versione sicura, come la 7.0.100, 8.5.51, 9.0.31 o successive. Ciò contribuirà a mitigare il rischio di sfruttamento della vulnerabilità.

ISC BIND Service Downgrade / Reflected DoS

Il server dei nomi remoto, eseguendo ISC BIND 9, è vulnerabile a un downgrade delle prestazioni e alle vulnerabilità di DoS riflesse. Questo è dovuto alla mancanza di limitazioni sufficienti nei recuperi di risposte di riferimento, consentendo a un utente non autenticato di causare degrado del servizio o utilizzare il server come riflettore in un attacco di riflessione.Per risolvere il problema, è necessario aggiornare ISC BIND alla versione specificata nell'avviso del fornitore. Questo aggiornamento contribuirà a mitigare la vulnerabilità e migliorare la sicurezza del server dei nomi.

NFS Shares World Readable

Il server NFS remoto esporta condivisioni leggibili da tutto il mondo. Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).Posizionare le opportune restrizioni su tutte le condivisioni NFS.

SSL Medium Strength Cipher Suites Supported (SWEET32)

Il servizio remoto supporta l'uso di crittografie SSL di media potenza.L'host remoto supporta l'utilizzo di crittografie SSL che forniscono una crittografia di livello medio. Questo include l'utilizzo di chiavi con lunghezza compresa tra almeno 64 bit e meno di 112 bit, o l'utilizzo della suite di crittografia 3DES. È importante notare che la crittografia di livello medio è più vulnerabile all'elusione, specialmente se l'aggressore si trova sulla stessa rete fisica.Per mitigare il rischio, è consigliabile riconfigurare l'applicazione interessata per evitare l'utilizzo di crittografie di media complessità. Questo aiuterà a migliorare la sicurezza delle comunicazioni SSL sul servizio remoto.