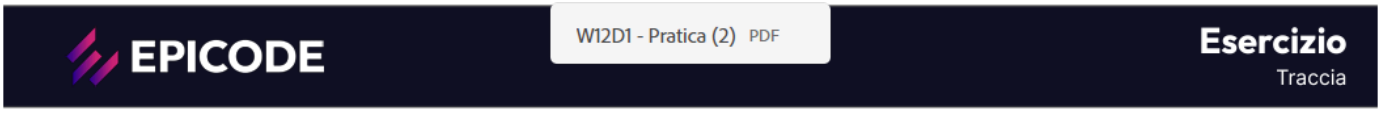
W12D1 - Pratica 2

Giacomo di Giacinto



Traccia
A partire dal report di ieri:

- Analisi/studio delle vulnerabilità (PDF) - servirà sia per exploit che remediation

- Report PDF per «dirigente»
- Inteso come riassunto che va presentato ai dirigenti per l'approvazione a livello finanziario ecc. Non contiene troppi dettagli tecnici ma soltanto l'indicazione della vulnerabilità e soprattutto i grafici con la pericolosità delle varie vulnerabilità riscontrate

A seguito della vostra fase di ingaggio sono a portare su carta i risultati del vulnerability assessment.

Lo scopo principale di questo test è stato quello di identificare e valutare le potenziali vulnerabilità che potrebbero compromettere l'integrità, la disponibilità e la riservatezza delle risorse informatiche critiche della vostra organizzazione.

Ho identificato una serie di punti di debolezza che richiedono immediata attenzione e azione.

Il presente rapporto è stato redatto con l'intento di fornire un quadro chiaro e sintetico delle vulnerabilità individuate, delle relative implicazioni per l'organizzazione e delle contromisure consigliate per mitigare i rischi.

Per eseguire l'analisi delle vulnerabilità è stato utilizzato il software Nessus e come bersaglio della scansione è stata individuata la macchina Metasploitable (IP 192.168.1.246). La scansione adottata è stata una basic network scan.

Sono state rilevate diverse criticità che richiedono un'attenzione immediata e proporzionata a seconda della macro categoria alla quale appartengono.

Le categorie sono le seguenti:

Critical:
- Le vulnerabilità categorizzate come "Critical" rappresentano le minacce più gravi per la sicurezza del sistema, con un elevato potenziale di sfruttamento da parte di attaccanti.

High:
- Le vulnerabilità classificate come "High" indicano rischi significativi per la sicurezza del sistema, sebbene non siano necessariamente così gravi come quelle "Critical".

Medium:
- Le vulnerabilità di livello "Medium" rappresentano minacce di sicurezza rilevanti che potrebbero essere sfruttate da attaccanti per compromettere la sicurezza del sistema. Sebbene il loro impatto possa non essere così immediato o grave come le vulnerabilità di livello superiore, è comunque essenziale affrontarle per ridurre il rischio complessivo.

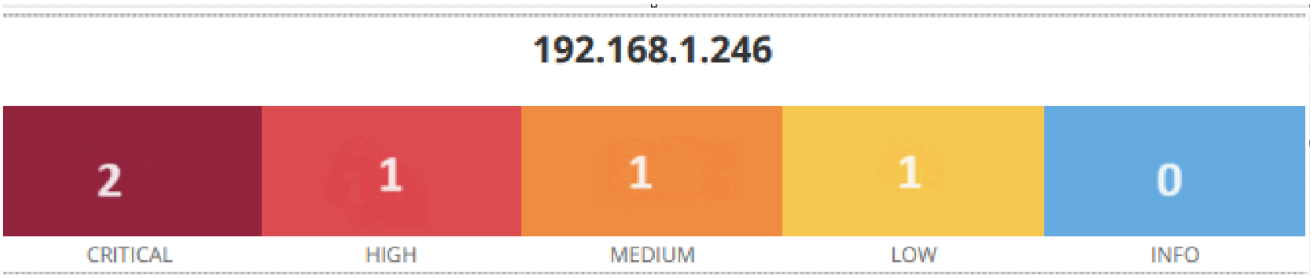
Low:

- Le vulnerabilità classificate come "Low" indicano rischi di sicurezza minori, che potrebbero non rappresentare una minaccia immediata per il sistema ma che comunque richiedono attenzione e monitoraggio per evitare eventuali problemi futuri o l'escalation a livelli di criticità più elevati.

Info:

- Le informazioni di livello "Info" sono segnalazioni di sicurezza che forniscono dati rilevanti ma non rappresentano necessariamente una vulnerabilità attiva o un rischio immediato per il sistema.

Di seguito elenco le criticità emerse con la loro descrizione



CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un attaccante potrebbe utilizzarla collegandosi alla porta remota e inviando comandi direttamente. La sistemazione della criticità prevede la reinstallazione del sistema

CRITICAL	10.0	10.0	156115	Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)

Una vulnerabilità di esecuzione remota del codice esiste in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si gestisce l'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questo, tramite una richiesta web, per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione. La sistemazione della criticità prevede l'aggiornamento della applicazione.

HIGH	7.5	5.9	90509	Samba Badlock Vulnerability

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è interessata da una falla, nota come Badlock, che esiste nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD). La sistemazione della criticità prevede l'aggiornamento della applicazione.

MEDIUM	6.5	-	42263	Unencrypted Telnet Server

L'host remoto sta eseguendo un server Telnet su un canale non crittografato. L'utilizzo di Telnet su un canale non crittografato non è consigliato poiché i login, le password e i comandi vengono trasferiti in testo non cifrato. Ciò consente a un attaccante remoto uomo-in-the-middle di intercettare una sessione Telnet per ottenere credenziali o altre informazioni sensibili e di modificare il traffico scambiato tra un client e un server. La sistemazione della criticità prevede il cambio di strumento utilizzato, la mia proposta è quella di utilizzare SSH

LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials

Il server web remoto contiene diversi campi di modulo HTML che contengono un input di tipo 'password' che trasmettono le loro informazioni a un server web remoto in chiaro.Un attaccante che intercetta il traffico tra il browser web e il server potrebbe ottenere i nomi utente e le password degli utenti validi. La sistemazione della criticità prevede di controllare che ogni modulo sensibile trasmetta il contenuto attraverso il protocollo HTTPS.

In conclusione, il vulnerability assessment ha evidenziato diverse criticità che richiedono una pronta attenzione e azione correttiva da parte dell'organizzazione. Le vulnerabilità identificate spaziano da problemi di autenticazione non sicura a gravi falle di sicurezza in applicazioni e protocolli critici.

La presenza di una shell in ascolto su una porta remota senza autenticazione rappresenta un rischio significativo per la sicurezza del sistema, mentre la vulnerabilità di esecuzione remota del codice in Apache Log4j e la falla Badlock in Samba possono consentire agli attaccanti di compromettere l'integrità e la riservatezza dei dati.

L'utilizzo non sicuro di Telnet e la trasmissione non crittografata di informazioni sensibili tramite campi di modulo HTML sono vulnerabilità che espongono il sistema a rischi di intercettazione e manipolazione da parte di attaccanti malevoli.

Per affrontare queste criticità, è fondamentale adottare misure correttive immediate, che includono la reinstallazione del sistema, l'aggiornamento delle applicazioni interessate, l'adozione di protocolli di comunicazione sicuri come SSH e l'implementazione del protocollo HTTPS per la trasmissione sicura di informazioni sensibili.

Sottolineiamo l'importanza della sicurezza informatica e l'urgente necessità di affrontare le vulnerabilità identificate per garantire la protezione e l'integrità delle risorse informatiche critiche dell'organizzazione.