Report di Vulnerability Assesment -Tecnico-

Azienda commissionante: JetStorm, SPA

Redatto da: Federico Presti

Data: 20 Novembre 2024

Obiettivo del Report:

Identificare le vulnerabilità di sicurezza nel Sistema Metsploitable da voi incaricatomi di analizzare, valutarne I rischi e proporre soluzioni.

Indice

1. Sommario delle Vulnerabilità Critiche

Critical Vulnerabilities Overview: indirizzo ip 192.168.50.1 (Metasploitable 2)

Queste le 5 vulnerabilità critiche poste alla cortese attenzione del team tecnico:

1) Nella porta : tcp/8009 con il servizio ajp13 è stata individuata la vulnerabilità nota come Ghostcat che sfrutta l'Apache Tomcat AJP service.

Questa vulnerabilità se sfruttata esegue codice da remoto che può anche installare una backdoor sul Sistema operativo

2) Nella porta: tcp/8180 con il servizio www, è stata riscontrata una versione non più supportata di Apache Tomcat SEoL (<= 5.5.x) pertanto occorre fare un upgrade alla versione più recente ASAP.

3) Nella porta tcp/1524 risulta attivo il servizio wild_shell; un servizio non riconosciuto che se sfruttato può eseguire direttamente comandi nel Sistema operativo (backdoor)

4) Sulla porta TCP/5900, risulta attivo vnc, su cui è stato completato il login per un problema di password.

5) Sulla porta 6667 il servizio irc server contiene una backdoor identificata come UnrealIRCd capace di eseguire codice sul sistema

2. Informazioni sul Test effettuato

Per l'analisi è stato utilizzato l'applicativo Nessus Essentials, Version 10.8.3 (#10) su ambiente operativo Kali Linux, con criterio CVSS 3.0

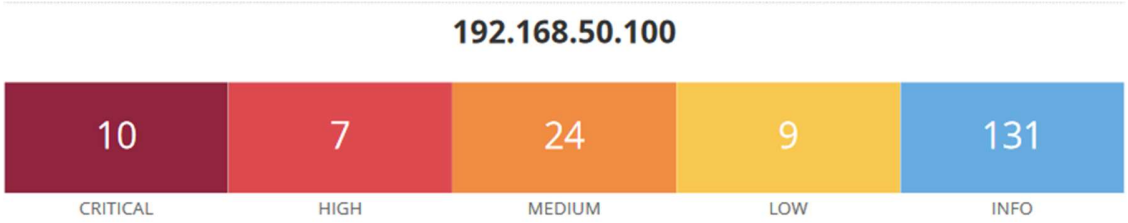
3. Porte e Servizi Scansionati

Il Sistema nessus ha scansionato circa 7000 porte tra le più comuni ed identificato I servizi attivi tramite le fonti autorevoli di National Institute of Standards and Technology (NIST) e CVE (Common Vulnerabilities and Exposures).

4. Vulnerabilità complessive Identificate

Premettendo che Nessus ha preventivamente testato le vulnerabilità eseguendo degli script, queste sono le vulnerabilità complessive riscontrate nel Sistema Metasploitable 2

10 Vulnerabilità critiche; 7 Vulnerabilità Alte; 24 vulnerabilità medie; 9 vulnerabilità basse.



5. Soluzioni Possibili da adottare

Tutte le soluzioni proposte da Nessus vengono preventivamente testate con un automatismo dal programma ma sono da verificare accuratamente da un Pentester.

Vulnerabilità n.1

Fai un'update della configurazione AJP in modo che essa richieda l'autorizzazione oppure, fai un'upgrade del server alle versioni 7.0.100, 8.5.51,9.0.31 o successive.

Vulnerabilità n.2

Effettua l'upgrade ad una versione di Apache Tomcat supportata ed in uso.

Vulnerabilità n.3

Verifica che Metasploitable non sia stato compromesso, dopodichè reinstalla il Sistema Operativo.

Vulnerabilità n.4

Cambiare la password del VNC server e provare che il server sia effettivamente sicuro con la nuova password.

Vulnerabilità n.5

Scarica nuovamente il software e verifica la correttezza dell'installazione con i checksum MD5/SHA1; dopodichè reinstallalo nuovamente.

6. Conclusioni

Le vulnerabilità identificate rappresentano un rischio significativo per la sicurezza del sistema, poiché molte di esse permettono l'esecuzione di codice da remoto o l'accesso non autorizzato al sistema.

Report di Vulnerability Assessment - per Dirigente-

Vulnerabilità	Gravità	Costo di Risoluzione (stimato)	Impatto Finanziario (stimato)	Tempo di Risoluzione (stimato)
1. Ghostcat (TCP/8009)	**Critica**	€5,000 (aggiornamento e configurazione)	€200,000 (esfiltrazione dati, RCE)	1-2 giorni
2. Apache Tomcat Obsoleto (TCP/8180)	**Critica**	€8,000 (aggiornamento e testing)	€150,000 (compromissione server)	2-3 giorni
3. Backdoor "wild_shell" (TCP/1524)	**Critica**	€6,000 (analisi forense e bonifica)	€300,000 (controllo completo OS)	2 giorni
4. VNC Password Debole (TCP/5900)	**Critica**	€4,000 (revisione accessi e hardening)	€100,000 (controllo remoto)	1 giorno
5. Backdoor UnrealIRCd (TCP/6667)	**Critica**	€6,000 (rimozione e reinstallazione)	€250,000 (esecuzione codice remoto)	2 giorni