Traccia:

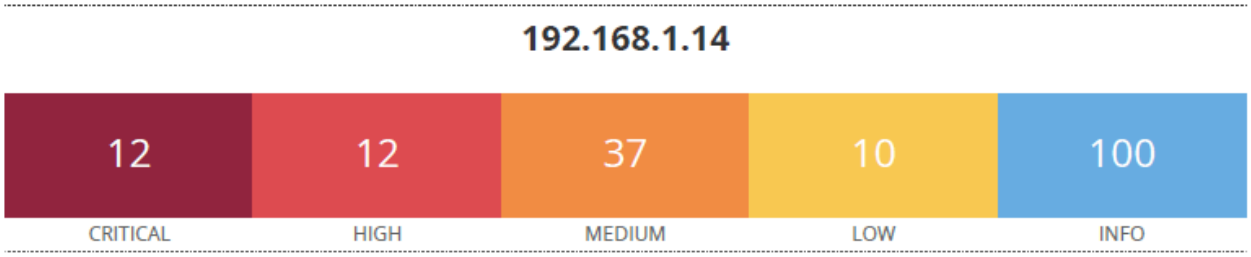
Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.

Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Come da immagine, una volta effettuato lo scan tramite nessus su macchina metasploitable, il report generato ha evidenziato una serie di vulnerabilità sfruttabili. Precisamente 12 critiche, 12 alte, 37 medie, 10 basse e 100 informative.



La prima vulnerabilità analizzata è la seguente:

51988 - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una backdoor bind shell è un tipo di vulnerabilità di sicurezza in cui un aggressore ha creato una shell, o interfaccia a riga di comando, legata a una porta specifica su un sistema compromesso. Nel caso della vulnerabilità con ID 51988, la backdoor è in ascolto sulla porta 1524/tcp. Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Exploit:

Per sfruttare questa vulnerabilità e ottenere l'accesso alla shell, è possibile utilizzare uno strumento come Netcat o Telnet per connettersi al sistema remoto sulla porta 1524/tcp. Una volta connessi, sarà possibile inviare comandi alla shell e riceverne l'output.

Soluzione

Per mitigare il rischio di una backdoor bind shell, è possibile implementare diverse soluzioni:

1. **Regole del firewall**: Configurare le regole del firewall per bloccare il traffico in entrata sulla porta 1524/tcp, che è la porta predefinita utilizzata dalla backdoor. In questo modo si impedisce agli aggressori esterni di connettersi alla shell.
2. **Aggiornamenti software**: Assicurarsi che tutto il software del sistema sia aggiornato e che siano state applicate tutte le patch di sicurezza.
3. **Sistemi di rilevamento delle intrusioni (IDS)**: implementare un IDS per monitorare il traffico di rete e rilevare qualsiasi attività sospetta.
4. **Utilizzare connessioni sicure**: Utilizzate connessioni sicure, come SSH, per connettervi ai sistemi remoti. Questo aiuta a proteggere dagli attacchi man-in-the-middle e da altri tipi di attacchi basati sulla rete.
5. **Modificare le porte predefinite**: Modificare le porte predefinite utilizzate da servizi e applicazioni per impedire agli aggressori di identificare e sfruttare facilmente le vulnerabilità.

Seconda vulnerabilità:

11356 - NFS Exported Share Information Disclosure

Sinossi

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

La vulnerabilità NFS (Network File System) Exported Share Information Disclosure, identificata da CVE-1999-0170, CVE-1999-0211 e CVE-1999-0554, si riferisce al rischio associato alle condivisioni NFS non correttamente configurate. Quando le condivisioni NFS non sono adeguatamente protette, un utente malintenzionato può essere in grado di accedere e potenzialmente manipolare dati sensibili sull'host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Alcune soluzioni per mitigare la vulnerabilità NFS Exported Share Information Disclosure:

1. **Limitare le esportazioni NFS a client specifici:** Nel file /etc/exports, specificare gli indirizzi IP dei client che possono accedere alle condivisioni NFS. In questo modo si limiterà l'accesso alla condivisione NFS al client con indirizzo IP specificato.
2. **Utilizzare NFSv4**: NFSv4 ha caratteristiche di sicurezza integrate che possono aiutare a prevenire la divulgazione di informazioni. Ad esempio, NFSv4 utilizza un meccanismo di autenticazione sicuro chiamato GSS-API (Generic Security Services Application Program Interface) che può impedire l'accesso non autorizzato alle condivisioni NFS.
3. **Utilizzare le regole del firewall:** È possibile utilizzare le regole del firewall per limitare l'accesso al servizio NFS. Ad esempio, su Linux, si può usare iptables per bloccare tutto il traffico in entrata alla porta NFS (2049) e consentire solo il traffico da client affidabili.
4. **Utilizzare l'autenticazione Kerberos:** Kerberos è un protocollo di autenticazione di rete che può fornire autenticazione e crittografia sicure per NFS. Utilizzando l'autenticazione Kerberos, è possibile garantire che solo i client autorizzati possano accedere alle condivisioni NFS.

5. **Utilizzare NFS su SSH:** È possibile utilizzare NFS su SSH per crittografare il traffico NFS e prevenire le intercettazioni. Ciò può essere fatto utilizzando SSH per creare un tunnel sicuro tra il client e il server NFS.

La terza vulnerabilità:

61708 - VNC Server 'password' Password

Sinossi

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

L'opzione "password" del server VNC 61708 serve a proteggere l'accesso remoto al server richiedendo l'inserimento di una password prima di stabilire una connessione. Si tratta di un'importante funzione di sicurezza, in quanto aiuta a prevenire l'accesso non autorizzato al server e ai sistemi collegati.

Per impostare una password nel server VNC 61708, è possibile utilizzare lo strumento di configurazione del server VNC o l'interfaccia a riga di comando del server VNC. Quando si imposta la password, è importante sceglierne una forte e unica che non possa essere facilmente indovinata o forzata. È inoltre buona norma cambiare regolarmente la password per aumentare ulteriormente la sicurezza.

Una volta impostata la password, a qualsiasi utente che tenti di connettersi al server VNC verrà richiesto di inserire la password. Se non viene inserita la password corretta, la connessione viene rifiutata.

La funzione "password" del Server VNC 61708 è uno strumento essenziale per garantire l'accesso remoto ai sistemi e proteggere i dati.

Exploit:

Innanzitutto, è necessario identificare il sistema di destinazione che esegue la versione vulnerabile del server VNC 61708, in questo caso metasploitable. È possibile utilizzare vari strumenti come Nmap, Nessus o qualsiasi altro scanner di rete per identificare il server VNC e la sua versione.

Una volta identificato il sistema di destinazione, è possibile utilizzare uno strumento come **Hydra** per forzare la password VNC. Hydra è un potente strumento di cracking delle password che può essere utilizzato per eseguire un **attacco a dizionario sul server VNC**. Ecco un esempio di comando per utilizzare Hydra per forzare la password VNC:

hydra -L usernames.txt -P passwords.txt vnc://target_ip -s 5900 -t 4

In questo comando, *usernames.txt* è un file contenente un elenco di nomi utente da provare, *passwords.txt* è un file contenente un elenco di password da provare, *target_ip* è l'indirizzo IP del sistema di destinazione e *5900* è la porta predefinita del server VNC. L'opzione *-t* specifica il numero di thread da utilizzare per l'attacco.

Se il server VNC utilizza una password debole, Hydra dovrebbe essere in grado di decifrarla in pochi minuti. Una volta ottenuta la password, potete utilizzare un client VNC come **TightVNC** o **RealVNC** per connettervi al server VNC e ottenere l'accesso remoto al sistema di destinazione.

Una volta ottenuto l'accesso al sistema di destinazione, è possibile eseguire diverse azioni come installare malware, rubare dati sensibili o spostarsi lateralmente all'interno della rete.

Soluzione

Proteggere il servizio VNC con una password forte.

Quarta vulnerabilità:

33850 - Unix Operating System Unsupported Version Detection

Sinossi

Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione

Secondo il numero di versione dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Exploit:

Per sfruttare questa vulnerabilità, un utente malintenzionato dovrebbe creare un payload dannoso che si rivolge alla versione specifica del sistema operativo Unix non supportata. Questo payload verrebbe inviato al sistema interessato attraverso un servizio vulnerabile, come SSH.

1. **Identificare il sistema di destinazione**: L'attaccante deve identificare il sistema di destinazione che esegue la versione non supportata del sistema operativo Unix. Questo può essere fatto scansionando la rete alla ricerca di sistemi che eseguono versioni vulnerabili note di Unix.
2. **Creare il payload dannoso**: L'aggressore deve creare un payload che si rivolga alla versione specifica del sistema operativo Unix. Questo payload potrebbe includere comandi per aumentare i privilegi, eseguire codice arbitrario o ottenere un accesso non autorizzato al sistema.
3. **Inviare il payload al sistema di destinazione**: L'aggressore deve inviare il payload dannoso al sistema di destinazione attraverso un servizio vulnerabile, come SSH. Questo può essere fatto utilizzando uno strumento come Metasploit o creando manualmente un comando SSH.
4. **Eseguire il payload**: Una volta che il payload è stato ricevuto dal sistema di destinazione, deve essere eseguito. Ciò potrebbe essere fatto sfruttando una vulnerabilità di iniezione di comandi nel servizio SSH.
5. **Ottenere un accesso non autorizzato o aumentare i privilegi**: Dopo aver eseguito il payload, l'aggressore otterrebbe l'accesso non autorizzato al sistema o l'escalation dei privilegi, a seconda del payload utilizzato.

Soluzione

La soluzione a questa vulnerabilità consiste nell'aggiornare il sistema operativo Unix a una versione supportata. L'aggiornamento a una versione supportata garantisce che il sistema riceva le patch di sicurezza e gli aggiornamenti più recenti dal fornitore, riducendo il rischio di sfruttamento.

Quinta vulnerabilità:

Sinossi

Sull'host remoto è installata una versione non supportata di Apache Tomcat.

Descrizione

Secondo la sua versione, Apache Tomcat è inferiore o uguale a 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Exploit:

Per sfruttare Apache Tomcat SEoL (<= 5.5.x), è possibile utilizzare il framework Metasploit per sfruttare una vulnerabilità nota (CVE-2010-1157) che consente il caricamento e l'esecuzione di file arbitrari.

Soluzione

Aggiornare a una versione di Apache Tomcat attualmente supportata.