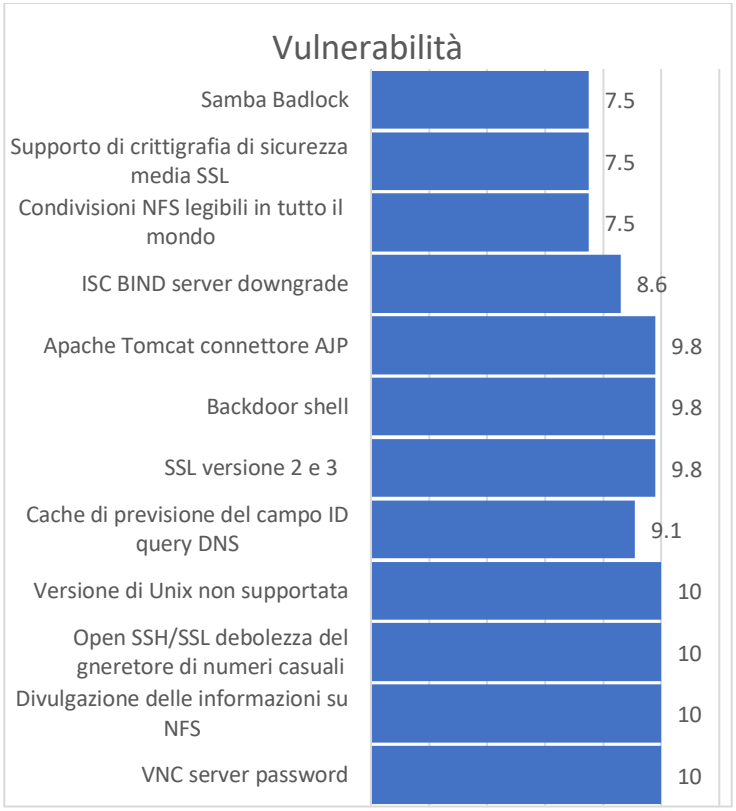
Nella scansione delle vulnerabilità sulla macchina target sono state trovate varie vulnerabilità più o meno gravi, analizzeremo prima quelle con un richio elevato e che quindi vi rendono suscettibili ad attacchi esterni.

Sono state trovate 11 vulnerabilità critiche che richiedono un intervento immediato; le analizzeremo in ordine di rischio decrescente, analizzando di volta in volta le soluzioni consigliate.



- La prima vulnerabilità con rischio 10 riguarda un server VNC (Virtual Network Computing) ovvero un software che consente di condividere e controllare un desktop o un'interfaccia grafica da remoto attraverso una connessione di rete; questo è protetto da una password debole (“password”) e quindi un malintenzionato da remoto potrebbe fruttare questa vulnerabilità per prendere il controllo del sistema. La password va quindi aggiornata e resa più sicura

- La seconda vulnerabilità con rischio 10 è dovuta ad una versione di Unix non più supportata che non riceve più aggiornamenti di sicurezza. Il sistema operativo va quindi aggiornato con una versione recente e supportata.

- La terza vulnerabilità a rischio 10 è causata da un possibile accesso alle condivisioni NFS (caretlle condivise) sull’host remoto, un malintenzionato può leggere informazioni di altri utenti o addirittura modificarle, per risolvere bisogna configurare NFS in modo che solo gli autorizzati possano accedere a determinati file

- La quarta e quinta e sesta vulnerabilità con rischio 10 riguardano il generatore di numeri casuali del sistema Debian dalla libreria Open SSH e SSL. Un utente malintenzionato può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco “man in the middle” (In pratica, l'attaccante si posiziona nel "mezzo" del flusso di comunicazione, facendo apparire come se le comunicazioni stessero procedendo normalmente, ma in realtà tutte le informazioni passano attraverso di lui). Non potendo quindi essere certi che tutto il

materiale crittografato sia realmente protetto tutto il materiale delle chiavi SSH, SSL e OpenVPN dovrebbe essere rigenerato.

- La settima e ottava vulnerabilità con rischio 9.8 riguardano la crittografia usata su una risorsa remota: qualsiasi elemento, informazione o servizio al quale si possa accedere da remoto tramite la rete. La risorsa accetta connessioni crittografate con SSL 2.0 e 3.0 che sono note per avere difetti infatti sono state sostituite da connessioni TSL, per questo come consiglia anche il NIST "National Institute of Standards and Technology" ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. La soluzione è quella di disattivare SSL 2.0 e 3.0 ed utilizzare invece TLS 1.2 o versioni successive.

- La nona vulnerabilità con rischio 9.8 riscontrata riguarda il connettore AJP, ovvero una configurazione errata dello stesso potrebbe consentire a un attaccante di ottenere accesso a file sensibili o di eseguire codice dannoso all'interno del server. Ciò potrebbe inoltre portare all'esecuzione remota di codice (RCE) e mettere a rischio l'integrità del server e dei dati.
  La soluzione consigliata è quindi quella di aggiornare la configurazione di AJP per l'autorizzazione e di aggiornare il server Tomcat noto per le sue vulnerabilità.

- La decima vulnerabilità con rischio 9.8 riguarda una possibile compromissione dell'host remoto ovvero il pc connesso alla rete che diventa così accessibile e controllabile da un'altra rete e quindi da una persona non autorizzata; abbiamo una shell (un'interfaccia che consente agli utenti di interagire con un sistema operativo) in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla connettersi alla porta remota e inviare direttamente i comandi.
  La soluzione richiede innanzitutto la verifica di un eventuale compromissione dell'host remoto e successivamente la reinstallazione del sistema ove necessario.

- L'undicesima vulnerabilità con rischio critico 9.1 il remote name resolver ovvero il servizio che consente di convertire nomi di host o nomi di dominio in indirizzi IP corrispondenti. (ad es. www.esempio.com viene convertito in 192.168.235.3). Il remote DNS resolver non utilizza porte casuali quando esegue una richiesta su server DNS di terze parti e un utente malintenzionato può sfruttare questa situazione per avvelenare il server DNS remoto, consentendogli di deviare il traffico a suo piacimento, bisogna quindi contattare il fornitore del server DNS per un aggiornamento di sicurezza che risolva il bug.

Ci sono poi 5 vulnerabilità con rischio alto che successivamente richiedono anch'esse un rapido intervento.

- La prima con rischio 8,6 rigurda il server dei nomi DNS che utilizza l'istanza di ISC BIND 9, soggetto a vulnerabilità di downgrade del servizio (DoS) riflesso. Il BIND (Berkeley Internet Name Domain) è il software open-source più utilizzato per la gestione di server DNS. La versione 9 di BIND è una delle implementazioni più comuni per i server DNS e offre funzionalità avanzate e sicurezza. Nel vostro caso un malintenzionato potrebbe sfruttare una debolezza nella configurazione o nell'implementazione di BIND 9 per abbassare il livello di servizio offerto dal server DNS. Inoltre il DoS riflesso coinvolge l'invio di query DNS falsificate a server DNS aperti o vulnerabili da parte di un attaccante. Le risposte generate da questi server DNS vengono indirizzate verso il bersaglio dell'attacco (nel caso specifico, il server BIND 9 remoto), causando un sovraccarico delle risorse e potenzialmente interrompendo il servizio. La soluzione per mitigare tali vulnerabilità sarebbe di tenere il software BIND 9 aggiornato con le ultime patch di sicurezza per evitare potenziali vulnerabilità note.

- Ci sono poi due vulnerabilità a rischio alto 7,5 riguardanti il supporto di crittografie SSL di sicurezza media da parte dell'host remoto, esponendovi al rischio che un attaccante possa inviare comando al vostro pc, per questo bisogna riconfigurare l'applicazione interessata per evitare l'uso di crittografie di media complessità.

- La quarta vulnerabilità è causata da Samba, una suite di programmi open-source che consente a sistemi operativi basati su Unix, come Linux, di comunicare con sistemi basati su Windows tramite il protocollo SMB (Server Message Block un server SMB (Server Message Block) in esecuzione sull'host remoto che è interessato dalla vulnerabilità Badlock. Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server può sfruttare questa falla per forzare un abbassamento del livello di autenticazione, che gli consente di visualizzare o modificare dati sensibili di sicurezza nel database o di disabilitare servizi critici. È quindi necessario aggiornare Samba ad una versione 4.2.11 / 4.3.8 / 4.4.2 o successiva.

- La quinta vulnerabilità è causata dal server NFS remoto (permette la condivisione di file) che esporta condivisioni, leggibili da tutto il mondo; il server sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP, o intervallo IP). Vanno quindi messe le opportune restrizioni su tutte le condivisioni NFS per risolvere la vulnerabilità.