VULNERABILITY SCAN E RISK ASSESTMENT

- **Host:**
  Metasploitable 192.168.50.120

- **Macchina di scan:**
  Kali Linux

- **Strumenti usati:**
  Nessus
  Nmap

PORTA	TIPO	**CVSS SCORE**	VPR	**RISCHIO**	**DESCRIZIONE**	**SOLUZIONE**
2049 /udp/rpc-nfs	RPC	10.0	5.9	CRITICO	Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un attaccante potrebbe sfruttare ciò per leggere (e eventualmente scrivere) file sull'host remoto.	Configura NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.
NON DISPONIBILE	GENERALE	10.0	/	CRITICO	Secondo il numero di versione autodichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuovi patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.	Aggiorna a una versione del sistema operativo Unix attualmente supportata.
5900 /tcp/vnc	GAIN A SHELL REMOTE -					

LY	10.0	/	CRITICO	Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito a effettuare l'accesso utilizzando l'autenticazione VNC e una password 'password'. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per prendere il controllo del sistema.	Proteggi il servizio VNC con una password forte.
8000 tcp/ajp13	WEB SERVER	9.8	9.0	CRITICO	È stata trovata una vulnerabilità di lettura/inclusione file nel connettore AJP. Un attaccante remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un attaccante

potrebbe caricare codice malizioso JavaServer Pages (JSP) in una varietà di tipi di file e ottenere l'esecuzione remota del codice (RCE).	Aggiornare la configurazione AJP per richiedere autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versioni successive.

25 /tcp/smtp	SERVICE DETECTION	9.8	/	CRITICO	Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diverse vulnerabilità crittografiche, tra cui: • Uno schema di padding non sicuro con cifrari CBC. • Schemi non sicuri di rinegoziazione e ripresa della sessione. Un attaccante può sfruttare queste vulnerabilità per condurre attacchi di tipo man-in-the-middle o per decifrare le comunicazioni tra il servizio interessato e i client. Anche se SSL/TLS dispone di un modo sicuro per scegliere la versione più supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano nulla di meglio), molti browser web implementano questo in modo non sicuro, consentendo a un attaccante di declassare una connessione (come nel caso di POODLE). Pertanto, è consigliabile disabilitare completamente questi protocolli. Il NIST ha stabilito che SSL	Consulta la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di cifratura approvate) o versioni superiori.

1524 tcp/wild_shell	**Bind Shell Backdoor Detection**	9.8	/	CRITICO	Una shell è in ascolto sulla porta remota senza richiedere alcuna autenticazione. Un attaccante potrebbe utilizzarla collegandosi alla porta remota e inviando comandi direttamente.	Verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.
25 tcp/postgresql		5.1	/	CRITICO	Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un pacchettizzatore Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un attaccante può facilmente ottenere la parte privata della chiave remota e usarla per decifrare la sessione remota o impostare un attacco di tipo man-in-the-middle.	Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato.

22 tcp/ssh		9.8	5.1	CRITICO	La chiave host remota SSH è stata generata su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL. Il problema è dovuto a un pacchettizzatore Debian che ha rimosso quasi tutte le fonti di entropia nella versione remota di OpenSSL. Un attaccante può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco di tipo "uomo nel mezzo".	Considerare tutto il materiale crittografico generato sull'host remoto come indovinabile. In particolare, tutto il materiale chiave SSH, SSL e OpenVPN dovrebbe essere rigenerato.
445 tcp/cifs	**Samba Badlock Vulnerabi**	-				

lity	7.5	5.9	ELEVATO-MEDIO	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) a causa di un'impropria negoziazione del livello di autenticazione sui canali Remote Procedure Call (RPC). Un attaccante man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, consentendo l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati sensibili di sicurezza nel database Active Directory (AD) o la disabilitazione di servizi critici.	Upgrade a Samba version 4.2.11 / 4.3.8 / 4.4.2 o più recenti.

2049 / tcp / rpc-nfs	**NFS Shares World Readable**	7.5	/	ELEVATO-MEDIO	Il server remoto NFS sta esportando una o più condivisioni senza limitare l'accesso (in base all'hostname, all'IP o all'intervallo di IP).	Imporre le restrizioni appropriate su tutte le condivisioni NFS.
5432 /						

tcp / postgresql 25 / tcp / smtp	**TLS Version 1.0 Protocol Detection**	6.5 /	MEDIO	Il servizio remoto accetta connessioni crittografate utilizzando TLS 1.0. TLS 1.0 presenta una serie di difetti di progettazione crittografica. Le moderne implementazioni di TLS 1.0 attenuano questi problemi, ma le versioni più recenti di TLS come 1.2 e 1.3 sono progettate per contrastare tali difetti e dovrebbero essere utilizzate ogni volta che possibile.	Dal 31 marzo 2020, gli endpoints che non utilizzano TLS 1.2 e versioni superiori avranno problemi con i principali browser web e fornitori. Il PCI DSS v3.2 richiede la completa disabilitazione di TLS 1.0 entro il 30 giugno 2018, ad eccezione di determinati terminali POS POI e dei relativi punti di terminazione SSL/TLS. Questo requisito è dovuto alla suscettibilità di TLS 1.0 a exploit conosciuti. L'uso di

25 / tcp / smtp	**SSL Anonymous Cipher Suites Supported**	5.9	ELEVATO-MEDIO	L'host remoto supporta l'uso di cifrari SSL anonimi. Sebbene ciò consenta a un amministratore di configurare un servizio che crittografa il traffico senza dover generare e configurare certificati SSL, non offre alcun modo per verificare l'identità dell'host remoto e rende il servizio vulnerabile a un attacco man-in-the-middle. Nota: Questo è notevolmente più facile da sfruttare se l'attaccante si trova sulla stessa rete fisica.	Riconfigurare l'applicazione interessata, se possibile, per evitare l'uso di cifrature deboli.
25 / tcp / smtp	**SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and**				

Weakened eNcryption)	5.9	MEDIO	L'host remoto supporta SSLv2 e potrebbe quindi essere vulnerabile a un attacco di Bleichenbacher padding oracle cross-protocol noto come DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Questa vulnerabilità esiste a causa di un difetto nell'implementazione del Secure Sockets Layer Version 2 (SSLv2) e consente di decifrare il traffico TLS catturato. Un attaccante man-in-the-middle può sfruttare ciò per decifrare la connessione TLS utilizzando il traffico precedentemente catturato e una crittografia debole insieme a una serie di connessioni appositamente create verso un server SSLv2 che utilizza la stessa chiave privata.	Disabilitare SSLv2 e le suite crittografiche con crittografia di esportazione . Assicurarsi che le chiavi private non vengano utilizzate in nessun punto con software server che supporta connessioni SSLv2.

22 / tcp / ssh	**SSH Weak Algorithms Supported**	4.3	MEDIO	Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario a flusso Arcfour o nessun cifrario affatto. L'RFC 4253 sconsiglia l'uso di Arcfour a causa di un problema legato alle chiavi deboli.	Contattare il fornitore o consultare la documentazione del prodotto per rimuovere le cifrature deboli.
6000 / tcp / x11	**X Server Detection**	2.6	BASSO	L'host remoto sta eseguendo un server X11. X11 è un protocollo client-server che può essere utilizzato per visualizzare applicazioni grafiche in esecuzione su un determinato host su un client remoto. Poiché il traffico X11 non è cifrato, è possibile per un attaccante intercettare la connessione.	Limitare l'accesso a questa porta. Se non viene utilizzato il servizio client/server X11, disabilitare completamente il supporto TCP in X11 (-nolisten tcp).
0 / icmp	**ICMP Timestamp Request Remote Date Disclosure**	4.2	BASSO	L'host remoto risponde a una richiesta di timestamp ICMP. Questo consente a un attaccante di conoscere la data impostata sulla macchina bersaglio, il che potrebbe aiutare un attaccante remoto non autenticato a sconfiggere i protocolli	

di autenticazione basati sul tempo.

Filtra le richieste di timestamp ICMP (13) in uscita e le risposte di timestamp ICMP (14) in uscita.

VERIFICA CON NMAP

SCRIPT USATO:

sudo nmap --script vuln 192.168.50.120 -v

PORTE APERTE RILEVATE:

Discovered open port 22/tcp on 192.168.50.120
Discovered open port 5900/tcp on 192.168.50.120
Discovered open port 445/tcp on 192.168.50.120
Discovered open port 25/tcp on 192.168.50.120
Discovered open port 53/tcp on 192.168.50.120
Discovered open port 80/tcp on 192.168.50.120
Discovered open port 111/tcp on 192.168.50.120
Discovered open port 23/tcp on 192.168.50.120
Discovered open port 21/tcp on 192.168.50.120
Discovered open port 139/tcp on 192.168.50.120
Discovered open port 3306/tcp on 192.168.50.120
Discovered open port 2049/tcp on 192.168.50.120
Discovered open port 513/tcp on 192.168.50.120
Discovered open port 8180/tcp on 192.168.50.120
Discovered open port 6000/tcp on 192.168.50.120
Discovered open port 514/tcp on 192.168.50.120
Discovered open port 6667/tcp on 192.168.50.120
Discovered open port 8009/tcp on 192.168.50.120
Discovered open port 5432/tcp on 192.168.50.120
Discovered open port 512/tcp on 192.168.50.120
Discovered open port 2121/tcp on 192.168.50.120
Discovered open port 1524/tcp on 192.168.50.120
Discovered open port 1099/tcp on 192.168.50.120

PORT STATE SERVICE

21/tcp open ftp
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor

```
|    State: VULNERABLE (Exploitable)
|    IDs:  CVE:CVE-2011-2523  BID:48539
|      vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|    Disclosure date: 2011-07-03
|    Exploit results:
|      Shell command: id
|      Results: uid=0(root) gid=0(root)

22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp  open  domain
80/tcp  open  http
|_http-trace: TRACE is enabled
| http-slowloris-check:
|  VULNERABLE:
|  Slowloris DOS attack
|    State: LIKELY VULNERABLE
|    IDs:  CVE:CVE-2007-6750
|      Slowloris tries to keep many connections to the target web server open and hold
|      them open as long as possible.  It accomplishes this by opening connections to
|      the target web server and sending a partial request. By doing so, it starves
|      the http server's resources causing Denial Of Service.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-sql-injection

111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|  VULNERABLE:
|  RMI registry default configuration remote code execution vulnerability
|    State: VULNERABLE
|      Default configuration of RMI registry allows loading classes from remote URLs which
can lead to remote code execution.
```

```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
| ssl-dh-params:
|  VULNERABLE:
|  Diffie-Hellman Key Exchange Insufficient Group Strength
|    State: VULNERABLE
|      Transport Layer Security (TLS) services that use Diffie-Hellman groups
|      of insufficient strength, especially those using one of a few commonly
|      shared groups, may be susceptible to passive eavesdropping attacks.
|    Check results:
|      WEAK DH GROUP 1
|            Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|            Modulus Type: Safe prime
|            Modulus Source: Unknown/Custom-generated
|            Modulus Length: 1024
|            Generator Length: 8
|            Public Key Length: 1024

| ssl-poodle:
|  VULNERABLE:
|  SSL POODLE information leak
|    State: VULNERABLE
|    IDs:  CVE:CVE-2014-3566  BID:70574
|          The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|          products, uses nondeterministic CBC padding, which makes it easier
|          for man-in-the-middle attackers to obtain cleartext data via a
|          padding-oracle attack, aka the "POODLE" issue.
|    Disclosure date: 2014-10-14
|    Check results:
|      TLS_RSA_WITH_AES_128_CBC_SHA
|    References:
|      https://www.imperialviolet.org/2014/10/14/poodle.html
|      https://www.openssl.org/~bodo/ssl-poodle.pdf
|      https://www.securityfocus.com/bid/70574
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
| ssl-ccs-injection:
|  VULNERABLE:
```

```
|  SSL/TLS MITM vulnerability (CCS Injection)
|    State: VULNERABLE
|    Risk factor: High
|      OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|      does not properly restrict processing of ChangeCipherSpec messages,
|      which allows man-in-the-middle attackers to trigger use of a zero
|      length master key in certain OpenSSL-to-OpenSSL communications, and
|      consequently hijack sessions or obtain sensitive information, via
|      a crafted TLS handshake, aka the "CCS Injection" vulnerability.


5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See
http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown

Host script results:
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

NSE: Script Post-scanning.
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Initiating NSE at 14:33
Completed NSE at 14:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 312.13 seconds
        Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```