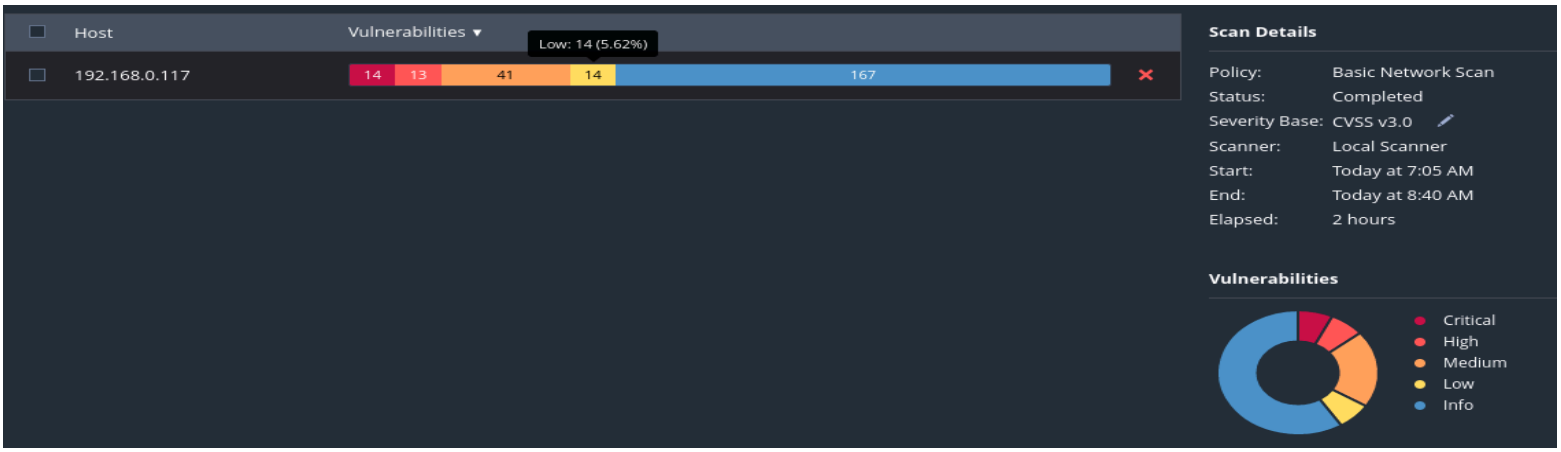
S5.L4 VULNERABILITY ASSESSTMENT-NESSUS:

In questo esercizio, ho deciso di condurre un Vulnerability Assessment utilizzando Nessus sulla macchina Metasploitable, limitando il target alle porte comuni. Dopo aver completato la scansione, mi sono dedicato all'analisi dettagliata del rapporto per ogni vulnerabilità individuata, consultando i link forniti nel rapporto e cercando ulteriori informazioni sul web quando necessario. L'intento principale dell'esercizio era acquisire familiarità con l'uso di Nessus, dalla configurazione all'avvio delle scansioni, e approfondire la mia conoscenza sulle vulnerabilità più frequenti che un penetration tester può incontrare.
Dopo aver installato Nessus, ho sfruttato le sue funzionalità di base per eseguire una scansione sulla macchina Metasploitable come specificato. Ho selezionato l'opzione "Basic Network Scan", che fornisce una scansione con le impostazioni di default, e ho inserito l'IP della macchina Metasploitable come target. questi sono i risultati



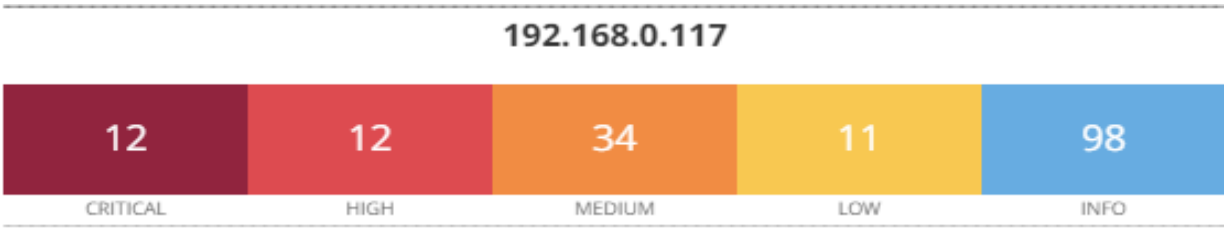
Dalla scansione effettuata sulla macchina con indirizzo IP 192.168.0.117, usando Nessus e impostando la politica di "Basic Network Scan", ho ottenuto i seguenti risultati:

- Ora di inizio della scansione: Oggi alle 7:05 AM
- Ora di fine della scansione: Oggi alle 8:40 AM
- Durata della scansione: 2 ore
- Stato della scansione: Completata
- Base della severità: CVSS v3.0
- Tipo di scanner utilizzato: Scanner locale

Riepilogo delle vulnerabilità rilevate:

- Vulnerabilità critiche: 14
- Vulnerabilità ad alto rischio: 13
- Vulnerabilità a medio rischio: 41
- Vulnerabilità a basso rischio: 14
- Informazioni aggiuntive: 167

Tabella vulnerabilità trovate:



Report PDF vulnerabilità:

Vulnerabilities Total: 167

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	8.3	-	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	90509	Samba Badlock Vulnerability

Nessus Scanner

MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	5.3	2.9	58751	SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)
MEDIUM	5.3	-	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0*	-	11411	Backup Files Disclosure
MEDIUM	5.0*	-	46195	CGI Generic Path Traversal (extended test)
MEDIUM	4.3*	-	47831	CGI Generic XSS (comprehensive test)
MEDIUM	5.0*	-	46803	PHP expose_php Information Disclosure
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	5.0*	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3*	3.8	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	5.0*	-	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	4.3*	3.0	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.1	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	4.2	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	N/A	-	42057	Web Server Allows Password Auto-Completion

HIGH	7.5*	-	39465	CGI Generic Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5*	5.9	10205	rlogin Service Detection
HIGH	7.5*	5.9	10245	rsh Service Detection
MEDIUM	6.8	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	6.1	3.8	10815	Web Server Generic XSS
MEDIUM	5.9	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories
MEDIUM	5.3	-	39467	CGI Generic Path Traversal
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry

LOW	2.6*	-	26194	Web Server Transmits Cleartext Credentials
LOW	2.6*	-	34850	Web Server Uses Basic Authentication Without HTTPS
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39446	Apache Tomcat Detection
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	40406	CGI Generic Tests HTTP Errors
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	49704	External URLs

INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection

INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection

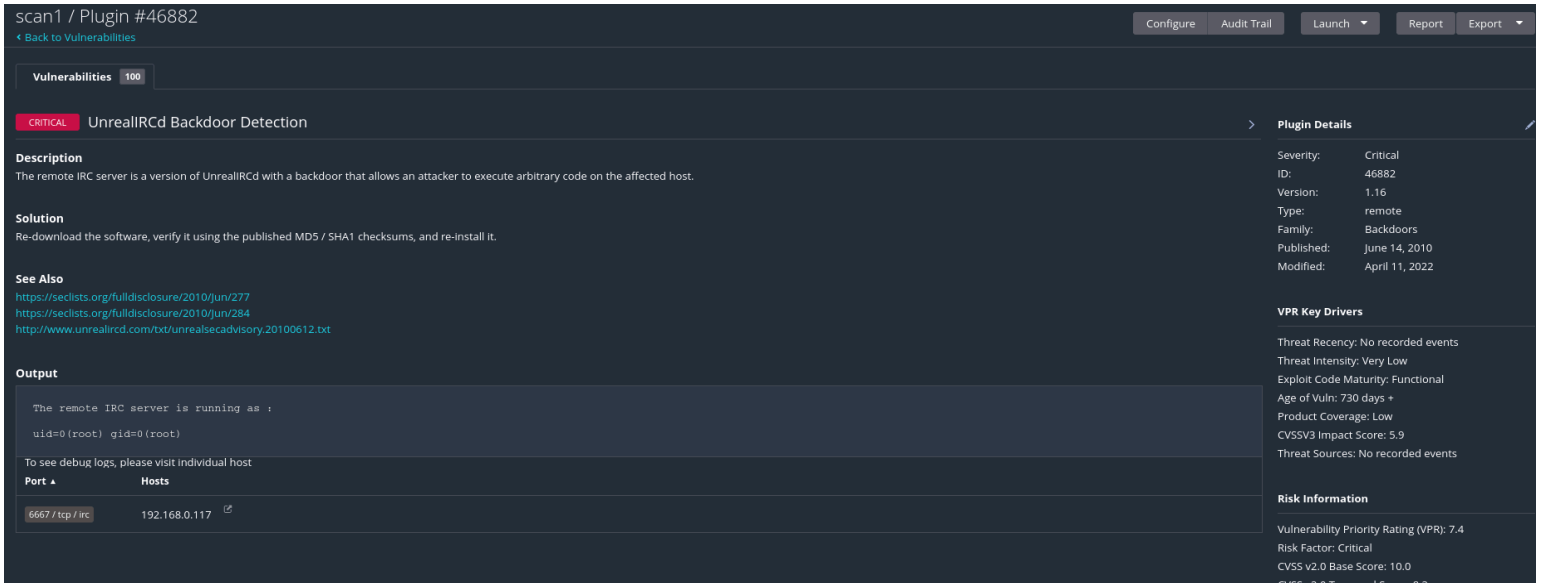
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	14788	IP Protocols Scan
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	181418	OpenSSH Detection
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection

INFO	N/A	-	17219	phpMyAdmin Detection
INFO	N/A	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Analisi, risoluzione e livelli di vulnerabilità:

Livello critico:



Descrizione vulnerabilità:

Il servizio IRC remoto eseguito è una versione di UnrealIRCd che contiene una backdoor. Questo difetto di sicurezza consente a un attaccante di eseguire codice arbitrario sull'host colpito. Questo tipo di vulnerabilità è particolarmente pericoloso

poiché dà agli attaccanti la capacità di prendere il controllo completo della macchina compromessa.

Dettagli Tecnici:

- Severità: Critica
- CVSS v2.0 Base Score: 10.0 (il punteggio massimo, indicando un rischio estremamente elevato)
- CVSS v2.0 Temporal Score: 8.3
- Vulnerability Priority Rating (VPR): 7.4
- CVSS v2.0 Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) - Indica che la vulnerabilità è sfruttabile da remoto, con bassa complessità, senza autenticazione, e ha un impatto completo su confidenzialità, integrità, e disponibilità.

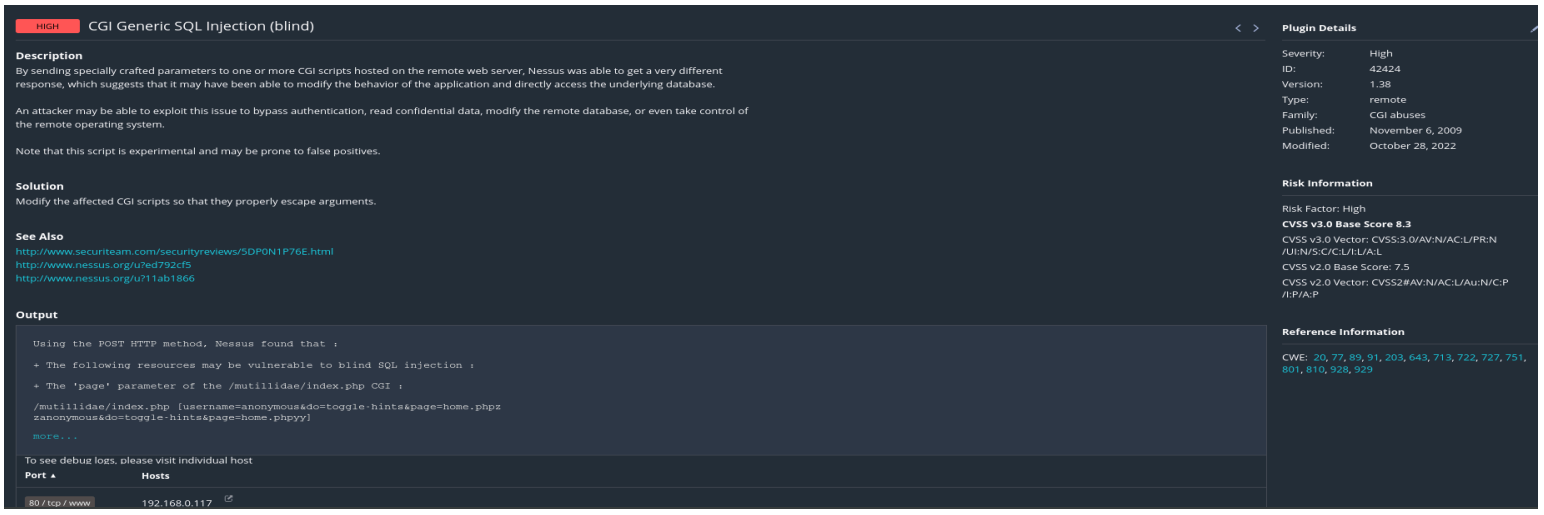
Soluzione Proposta:

La soluzione raccomandata è riscaricare il software, verificando l'integrità del file scaricato usando gli hash MD5 o SHA1, e quindi reinstallarlo. Questo dovrebbe sostituire la versione compromessa con una che non include la backdoor.

Ulteriori Azioni:

- Monitoraggio continuo: Dato che la backdoor era attiva, è fondamentale monitorare l'host per altre attività sospette che potrebbero indicare che gli attaccanti avevano già sfruttato la backdoor prima della sua rimozione.
- Aggiornamento delle politiche di sicurezza: Verificare e aggiornare le politiche di sicurezza per prevenire installazioni di software non verificato o modificato.

Livello Alto:



La vulnerabilità che ho identificato è una "CGI Generic SQL Injection (blind)" di livello alto. Ecco un'analisi dettagliata e la soluzione proposta per mitigarla:

Descrizione della Vulnerabilità:

La vulnerabilità di SQL Injection cieca è stata rilevata in uno o più script CGI eseguiti su un server web remoto. Tramite parametri appositamente manipolati, Nessus ha ottenuto una risposta significativamente diversa dall'atteso, indicando che potrebbe essere stata modificata la condotta dell'applicazione e, potenzialmente, acceduto al database sottostante. Questo tipo di attacco potrebbe permettere a un malintenzionato di bypassare l'autenticazione, leggere dati confidenziali, modificare il database remoto o persino prendere il controllo del sistema operativo remoto.

Dettagli Tecnici:

- Severità: Alta
- CVSS v3.0 Base Score: 8.3
- CVSS v2.0 Base Score: 7.5
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L - Indica che l'attacco è sfruttabile da remoto con bassa complessità, senza necessità di privilegi o interazioni utente, con impatti limitati sulla confidenzialità, integrità e disponibilità.

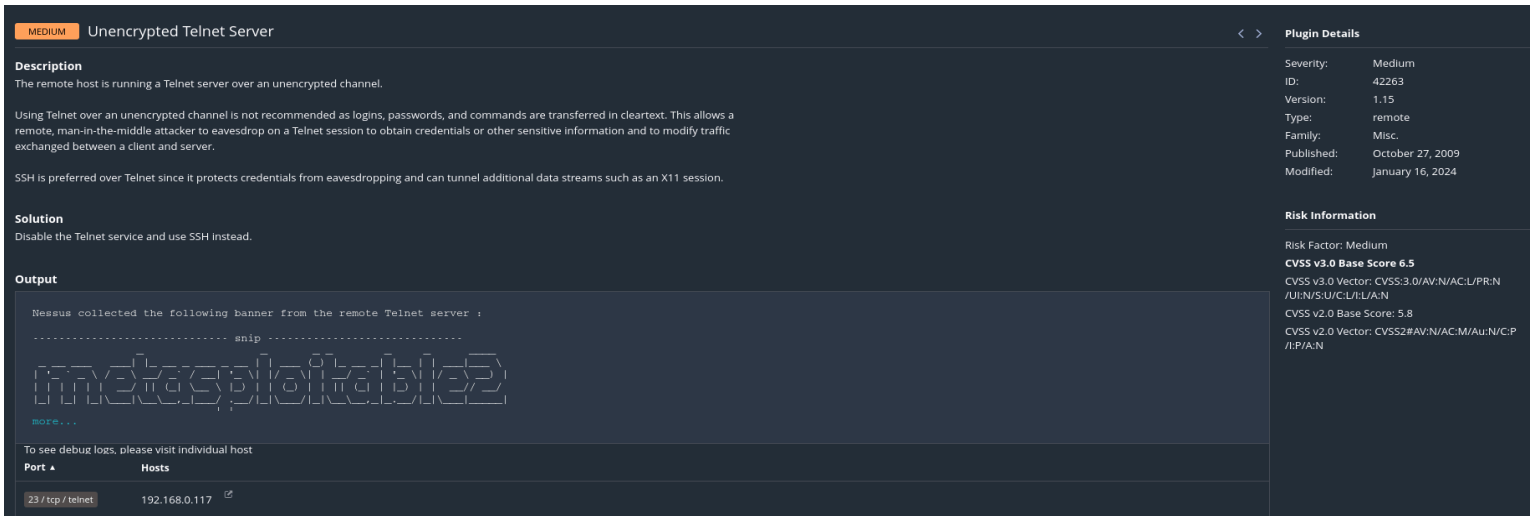
Soluzione Proposta:

Per mitigare questa vulnerabilità, è necessario modificare gli script CGI affetti in modo che eseguano un'adeguata sanificazione degli input, evitando così l'iniezione di SQL. Questo generalmente implica l'uso di funzioni di escaping degli argomenti o l'implementazione di prepared statements che separano chiaramente i dati dai comandi SQL.

Ulteriori Azioni:

- Validazione e sanificazione degli input: Assicurarsi che tutti gli input provenienti dagli utenti siano adeguatamente validati e sanificati prima di essere processati dagli script.
- Aggiornamenti regolari del software: Mantenere aggiornato il software server e gli script per proteggersi dalle vulnerabilità note.

Livello Medio:



La vulnerabilità identificata è relativa a un "Server Telnet non criptato" con una severità media. Ecco l'analisi dettagliata e la soluzione proposta per questa vulnerabilità:

Descrizione della Vulnerabilità:

Il server remoto sta eseguendo un servizio Telnet su un canale non criptato. Utilizzare Telnet su un canale non criptato è altamente sconsigliato perché i login, le password e i comandi vengono trasmessi in chiaro. Questo permette agli attaccanti, attraverso attacchi di tipo "man-in-the-middle", di intercettare facilmente queste informazioni sensibili e modificare i dati trasmessi tra un client e il server.

Dettagli Tecnici:

- Severità: Media
- CVSS v3.0 Base Score: 6.5
- CVSS v2.0 Base Score: 5.8
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N - Indica che l'attacco può essere eseguito da remoto con bassa complessità, non richiede privilegi né interazione dall'utente, e ha un impatto limitato sulla confidenzialità e integrità, senza impatti sulla disponibilità.

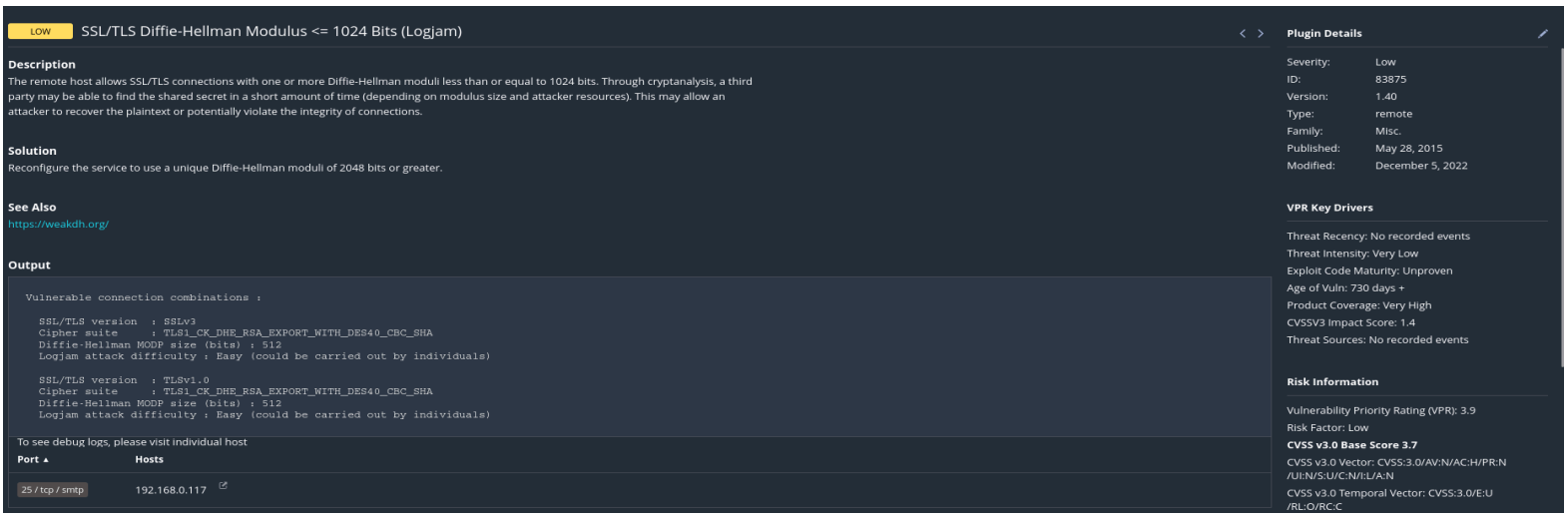
Soluzione Proposta:

Disattivare il servizio Telnet e utilizzare SSH come alternativa. SSH è preferibile perché protegge le credenziali e altri dati sensibili dall'intercettazione e, inoltre, può incanalare flussi di dati aggiuntivi come una sessione X11, offrendo così una maggiore sicurezza.

Ulteriori Azioni:

- Revisione delle configurazioni di rete: Controllare e aggiornare tutte le configurazioni di rete per garantire che nessun servizio non sicuro come Telnet sia abilitato.
- Monitoraggio della rete: Implementare strumenti di monitoraggio della rete per rilevare e rispondere a tentativi di accesso non autorizzati tramite servizi non sicuri.

Livello Basso:



La vulnerabilità identificata riguarda una configurazione non sicura dei moduli Diffie-Hellman utilizzati per le connessioni SSL/TLS, classificata come di severità bassa. Ecco un'analisi dettagliata e la soluzione proposta:

Descrizione della Vulnerabilità:

Il server remoto permette connessioni SSL/TLS che utilizzano uno o più moduli Diffie-Hellman con una dimensione inferiore o uguale a 1024 bit. L'utilizzo di moduli di dimensioni ridotte può rendere più facile, tramite tecniche di crittoanalisi, per una parte terza scoprire il segreto condiviso in un breve periodo di tempo, a seconda delle dimensioni del modulo e delle risorse dell'attaccante. Questo potrebbe permettere all'attaccante di recuperare il testo in chiaro o potenzialmente violare l'integrità delle connessioni.

Dettagli Tecnici:

- Severità: Bassa
- CVSS v3.0 Base Score: 3.7
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N - Indica che l'attacco è possibile da remoto, ma con alta complessità, senza privilegi necessari né interazioni dall'utente, e ha un impatto limitato sull'integrità senza influenzare la confidenzialità o la disponibilità.

Soluzione Proposta:

Riconfigurare il servizio per utilizzare un modulo Diffie-Hellman unico di 2048 bit o maggiore. L'aumento delle dimensioni del modulo migliora significativamente la sicurezza della crittografia a chiave pubblica utilizzata nelle connessioni SSL/TLS, rendendole più resistenti contro attacchi di crittoanalisi.

Ulteriori Azioni:

- Revisione e aggiornamento dei protocolli di crittografia: Verificare e aggiornare regolarmente i protocolli di crittografia e le configurazioni per assicurarsi che rispettino le migliori pratiche di sicurezza.
- Monitoraggio delle connessioni SSL/TLS: Utilizzare strumenti di monitoraggio della sicurezza per identificare e rispondere a potenziali abusi o configurazioni non sicure.

IN CONCLUSIONE:

Nel corso di questa sessione di Vulnerability Assessment con Nessus sulla macchina Metasploitable, ho potuto ottenere una visione chiara delle vulnerabilità presenti, classificandole in base alla loro gravità e rischio. Dopo aver eseguito una scansione completa utilizzando il "Basic Network Scan", sono emerse numerose vulnerabilità che variano da critiche a basse, necessitando di un'analisi attenta e di interventi specifici.
Ogni vulnerabilità identificata è stata documentata dettagliatamente, con le soluzioni appropriate che ho pianificato di implementare. Questo processo non solo migliora la sicurezza della macchina Metasploitable ma rafforza anche le mie competenze e conoscenze come penetration tester. La continua revisione e aggiornamento delle politiche e delle configurazioni di sicurezza saranno essenziali per mantenere la resilienza contro le minacce emergenti.