VULNERABILITY SCANNING

Nel seguente report si spiega come si effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni.
Fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Configurazione della scansione:

○ Target: Metasploitable

○ Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389★ Tipo di

○ Scansione: Basic Network Scan: Configurazione predefinita per una scansione di rete.

Analisi del Report:

○ Una volta completata la scansione, si analizzera il report generato da Nessus.

○ Per ogni vulnerabilità verrra' riportato approfondimenti ulteriori utilizzando i link e le risorse suggerite nel report.

7-JAN-26
CYBER SECURITY

AMIN EL KASSIMI
PAOLO RAMPINO

CONFIGURAZIONE SCANSIONE

Nei seguenti screen sono mostrate le configurazioni deelle varie sezioni:

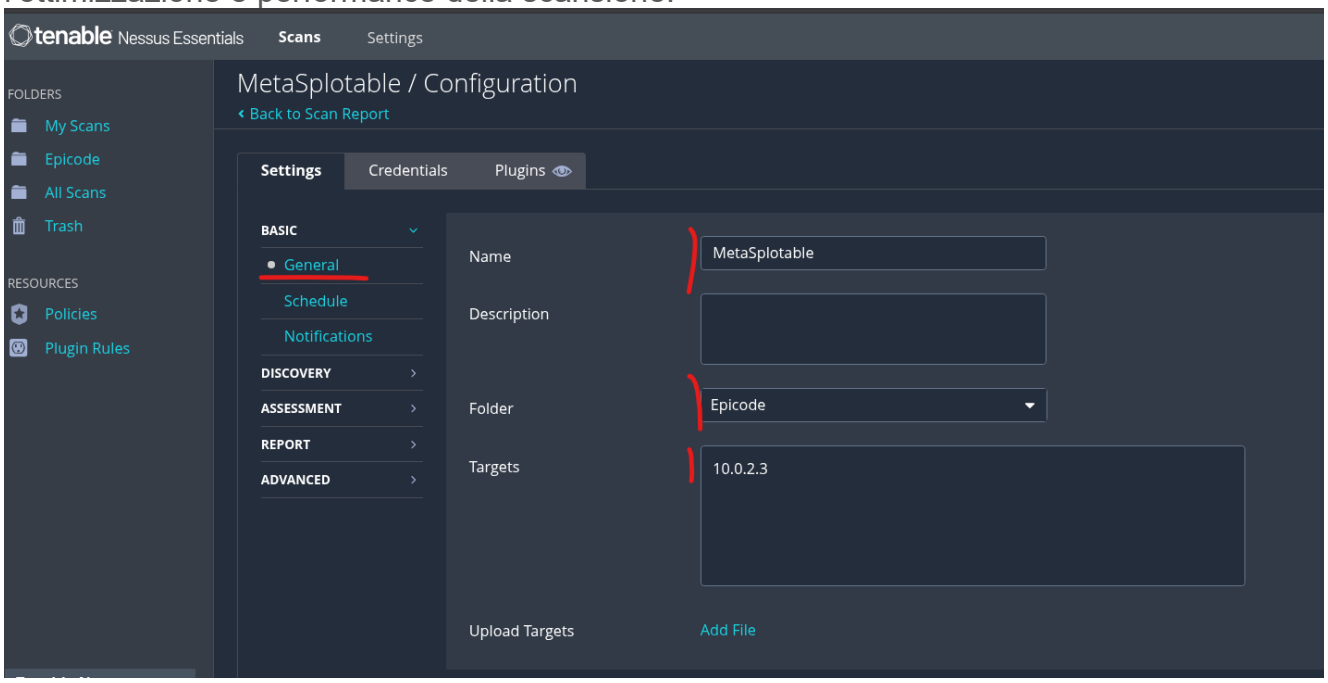
Basic: in questa sezione si inserisconoinformazioni di carattere generale sulla scansione come nome, descrizione, sistemi.

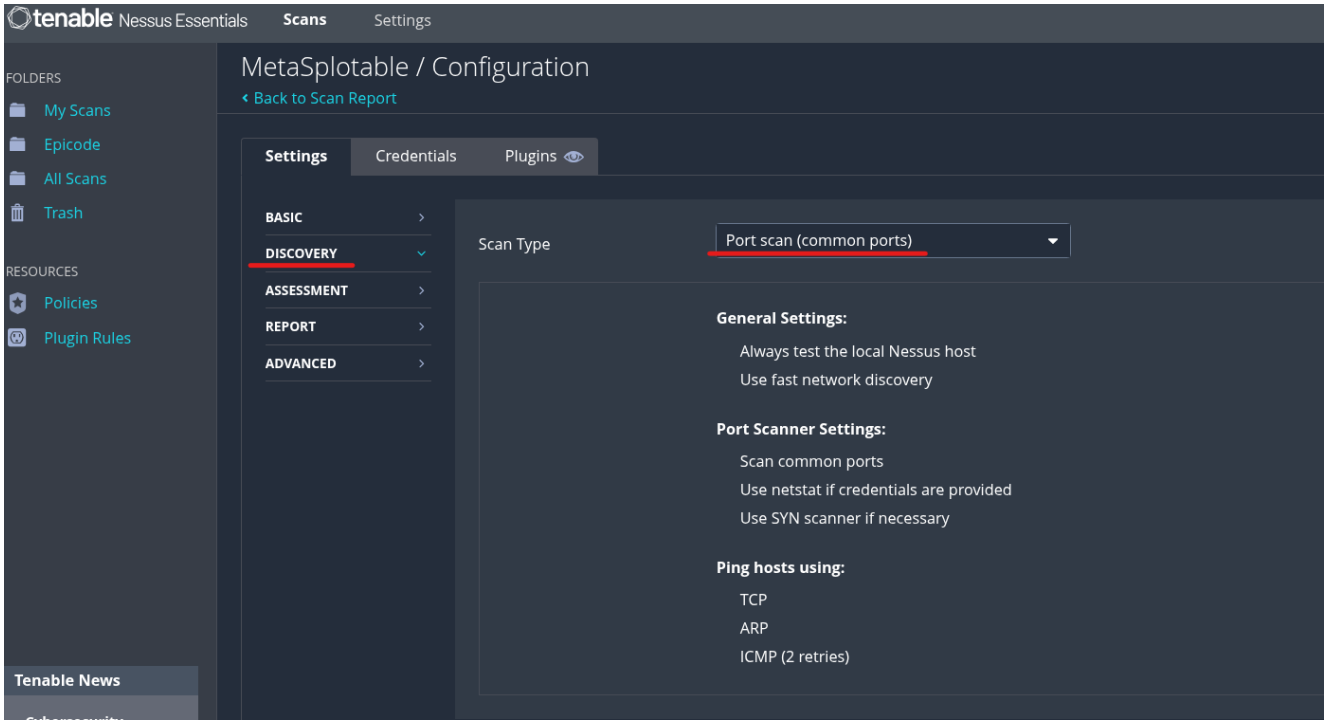
Discovery: in questa sezione si inseriscono le modalità per effettuare l'host discovery ed il port scanner.

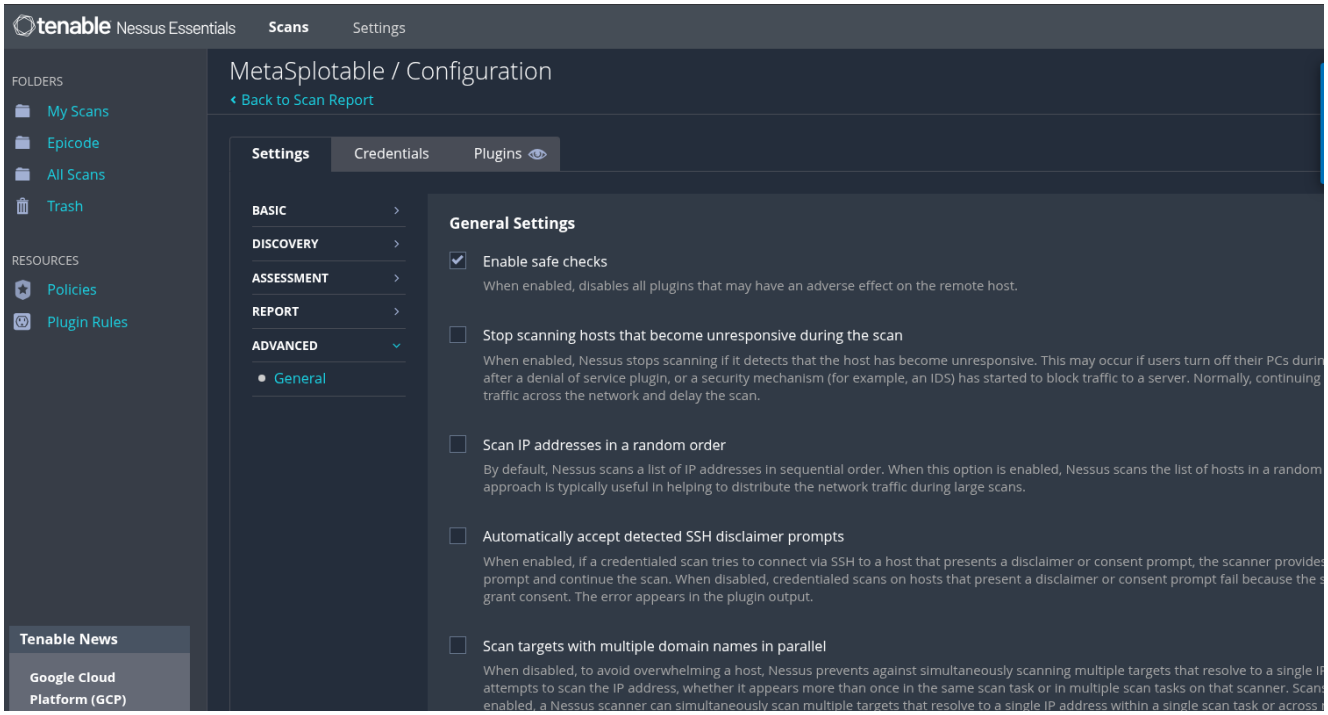
Assessment: in questa sezione si inseriscono le modalità per effettuare la valutazione delle vulnerabilità.

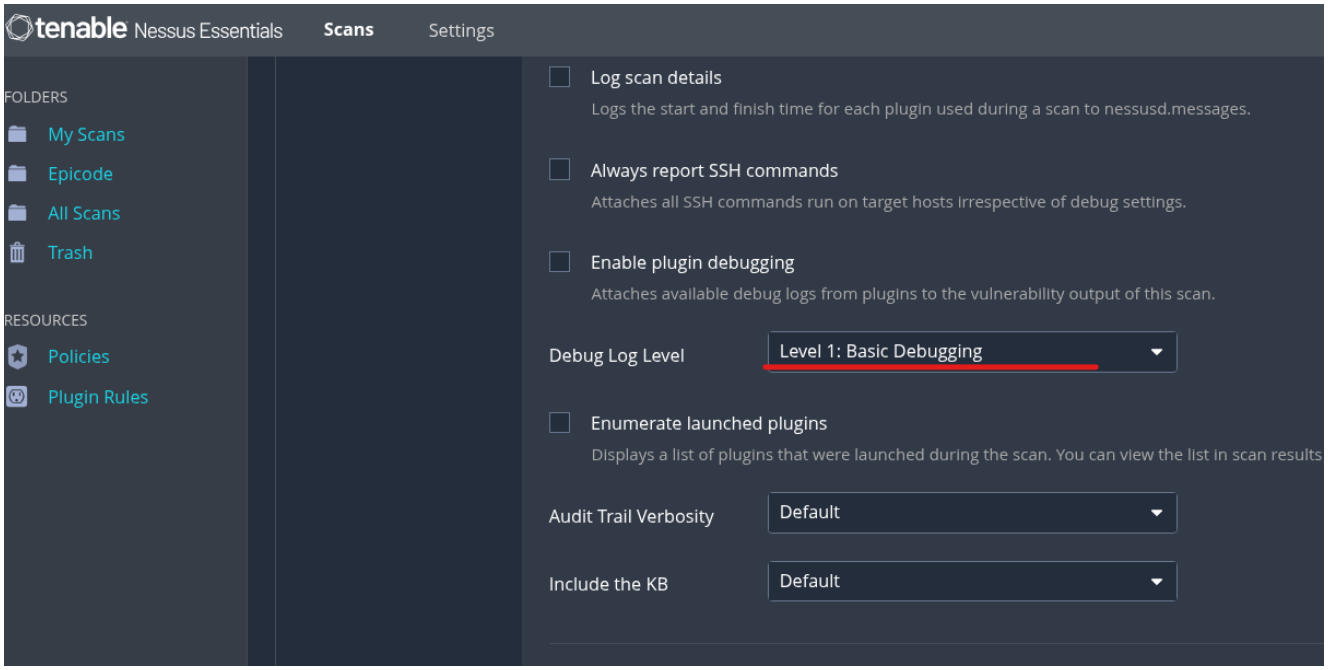
Report: in questa sezione si inseriscono le linee guida che utilizzerà lo strumento per creare i report.

Advanced: in questa sezione si possono scegliere delle impostazioni avanzate circa l'ottimizzazione e performance della scansione.




tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
Epicode
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
MetaSplotable / Configuration
Back to Scan Report
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (common ports)
General Settings:
Always test the local Nessus host
Use fast network discovery
Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)


tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
Epicode
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Tenable News
Google Cloud Platform (GCP)
MetaSplotable / Configuration
Back to Scan Report
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
General
General Settings
Enable safe checks
When enabled, disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become unresponsive during the scan
When enabled, Nessus stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs durin
after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing
traffic across the network and delay the scan.
Scan IP addresses in a random order
By default, Nessus scans a list of IP addresses in sequential order. When this option is enabled, Nessus scans the list of hosts in a random
approach is typically useful in helping to distribute the network traffic during large scans.
Automatically accept detected SSH disclaimer prompts
When enabled, if a credentialed scan tries to connect via SSH to a host that presents a disclaimer or consent prompt, the scanner provides
prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer or consent prompt fail because the s
grant consent. The error appears in the plugin output.
Scan targets with multiple domain names in parallel
When disabled, to avoid overwhelming a host, Nessus prevents against simultaneously scanning multiple targets that resolve to a single IP
attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans
enabled, a Nessus scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across

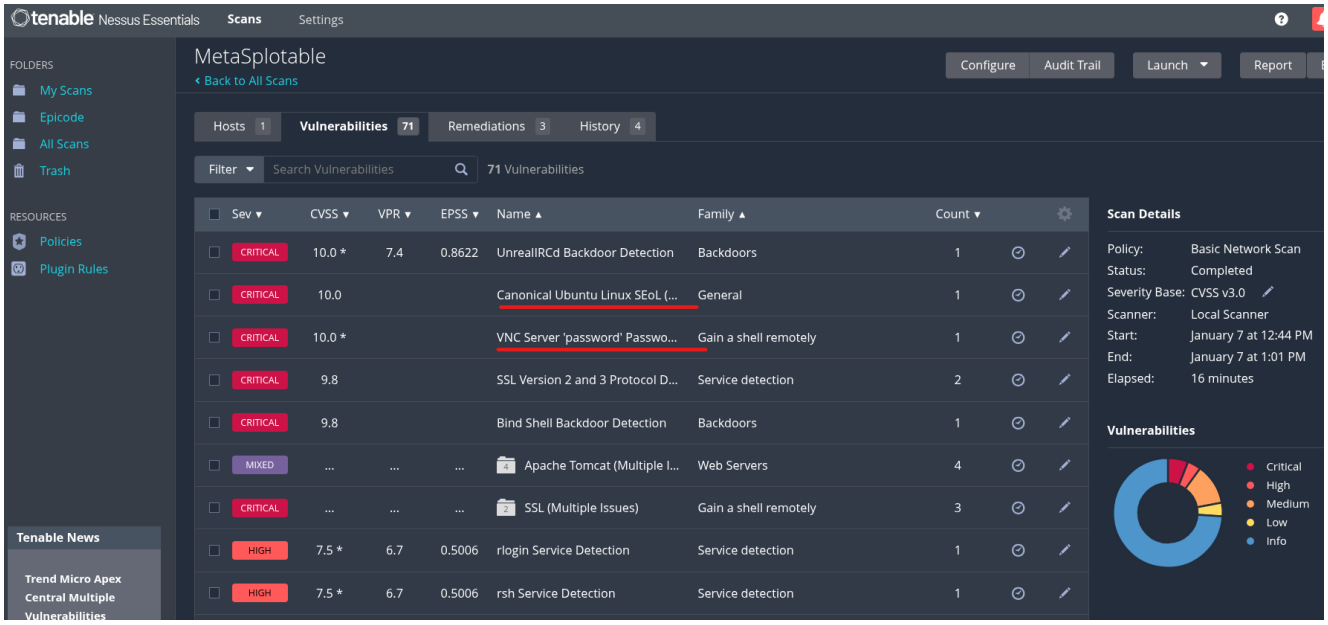

tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
Epicode
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Log scan details
Logs the start and finish time for each plugin used during a scan to nessusd.messages.
Always report SSH commands
Attaches all SSH commands run on target hosts irrespective of debug settings.
Enable plugin debugging
Attaches available debug logs from plugins to the vulnerability output of this scan.
Debug Log Level
Level 1: Basic Debugging
Enumerate launched plugins
Displays a list of plugins that were launched during the scan. You can view the list in scan results
Audit Trail Verbosity
Default
Include the KB
Default

ANALISI VULNERABILITA' TROVATE

Questa è la vista "Vulnerabilities" di una scansione Basic Network Scan eseguita contro Metasploitable con Nessus.

Tradotto:

- 1 host scansionato
- 71 vulnerabilità trovate
- Nessus ha già fatto port scan + service detection + matching con il database
- Qui si vede il risultato grezzo del Vulnerability Assessment, noon è ancora exploit. È intelligence tecnica.



La tabella centrale: come leggerla senza perdersi

Ogni riga = una vulnerabilità (o una famiglia di vulnerabilità)."
Qui vedi **molti CRITICAL**: Metasploitable è volutamente vulnerabile.

Colonne importantiSev (Severity)
Colore + livello:

- Critical → compromissione quasi certa
- High → rischio serio
- Medium → sfruttabile in contesti specifici
- Low → debolezza minore
- Info → informazione utile, non una falla

CVSS
Numero da 0 a 10: È una **misura tecnica della gravità**, 10.0 = scenario peggiore possibile

Esempio:
UnrealIRCd Backdoor Detection → **CVSS 10.0**, Vuol dire: servizio backdoored noto → compromissione immediata

VPR / EPSS
Servono per prioritizzare, non per fare exploit.
VPR: rischio "contestualizzato" secondo Tenable
EPSS: probabilità che quella vulnerabilità venga sfruttata nel mondo reale

Name
Il nome della vulnerabilità rilevata.
Qui trovi cose molto esplicite, tipo:
- *Bind Shell Backdoor Detection*
- *VNC Server 'password' Password*
- *SSL Version 2 and 3 Protocol Detected*

Family
Categoria tecnica, Serve a **capire la superficie d'attacco**, non solo la singola falla:
- Backdoors
- Service Detection
- Web Servers
- RPC
- General

Scan Details
Pannello di destra: Qui Nessus ti dice come ha lavorato.
Informazioni chiave:

Policy: Basic Network Scan
→ scan standard, non aggressiva

Status: Completed
→ finita correttamente

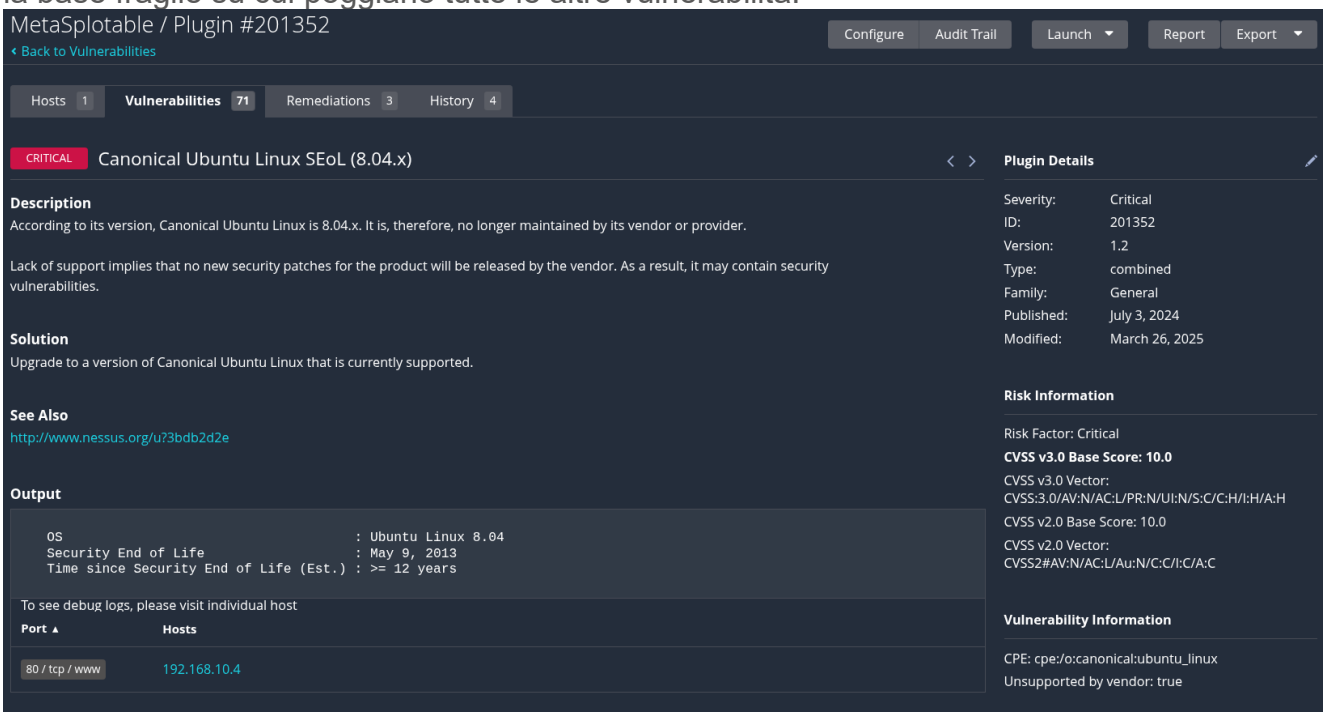
Scanner: Local Scanner
→ Nessus gira sulla tua Kali

Elapsed: 16 minuti
→ tempo realistico per una macchina piena di servizi

Questa sezione è fondamentale nei report professionali: dimostra metodologia e ripetibilità.

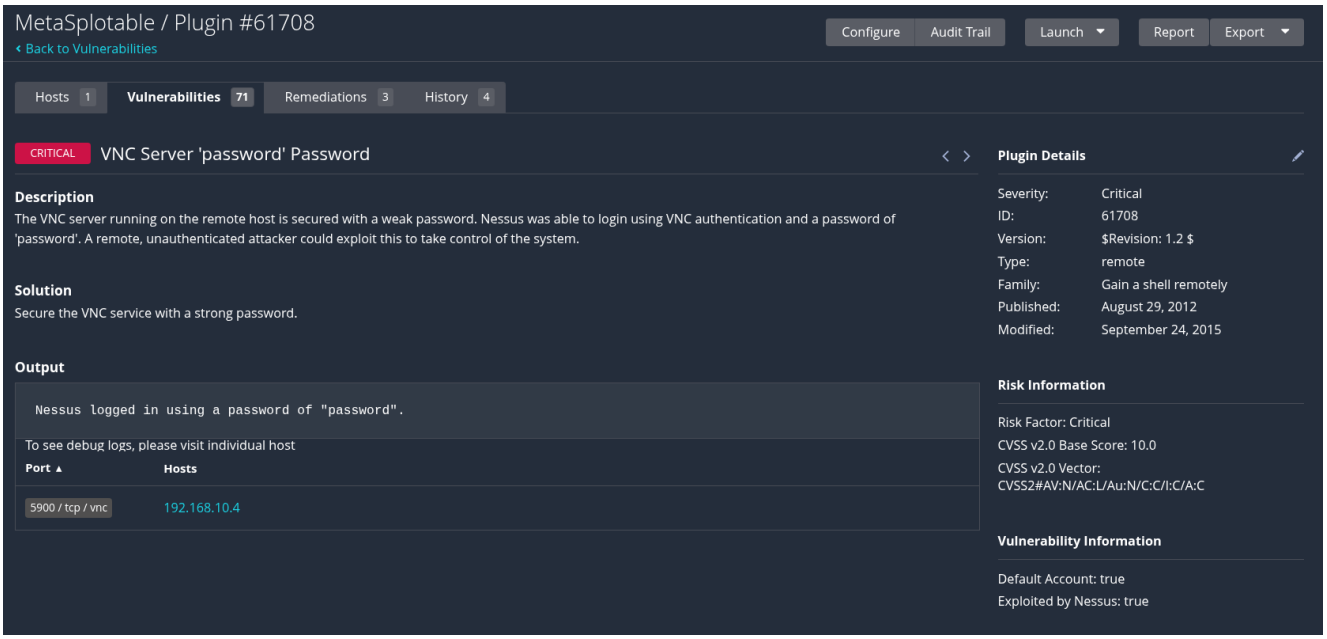
Canonical Ubuntu Linux SEoL (8.04.x):

La vulnerabilità Canonical Ubuntu Linux SEoL (8.04.x) non riguarda un bug specifico ma lo stato stesso del sistema. Metasploitable gira su una versione di Ubuntu che è fuori supporto da più di dieci anni, il che significa che da quel momento in poi nessuna vulnerabilità scoperta è mai stata corretta. Questo trasforma il sistema in un bersaglio permanente: ogni servizio che espone, ogni libreria che usa e persino il kernel possono contenere falle note e pubblicamente documentate. Nessus la classifica come critica non perché “rompe qualcosa” direttamente, ma perché stabilisce un contesto in cui la sicurezza non è più recuperabile. È la base fragile su cui poggiano tutte le altre vulnerabilità.



VNC Server 'password' Password:

La vulnerabilità VNC Server con password “password” invece è l’esatto opposto: qui non parliamo di contesto, ma di accesso reale. Il servizio VNC accetta una credenziale banale e Nessus è riuscito ad autenticarsi senza alcuno sforzo, dimostrando che chiunque sulla rete può ottenere il controllo remoto della macchina. Non serve exploit, non serve catena di attacco, non serve escalation iniziale: la porta è già aperta. È per questo che nel report compare “Exploited by Nessus: true”: lo scanner non sta ipotizzando un rischio, sta documentando un ingresso riuscito.



EXPLOIT DELLE VULNERABILITA

Nel seguente paragrafo andremo a vedere come sono state sfruttate le due vulnerabilita analizate in precedenza

Canonical Ubuntu Linux SEoL (8.04.x)

L'accesso mostrato nello screenshot è stato ottenuto sfruttando una **backdoor in ascolto su una porta TCP**, precedentemente identificata durante la fase di Vulnerability Assessment. Il sistema Metasploitable espone infatti diversi servizi malevoli o deliberatamente insicuri, tra cui una **shell bind** che rimane in ascolto su una porta non standard.

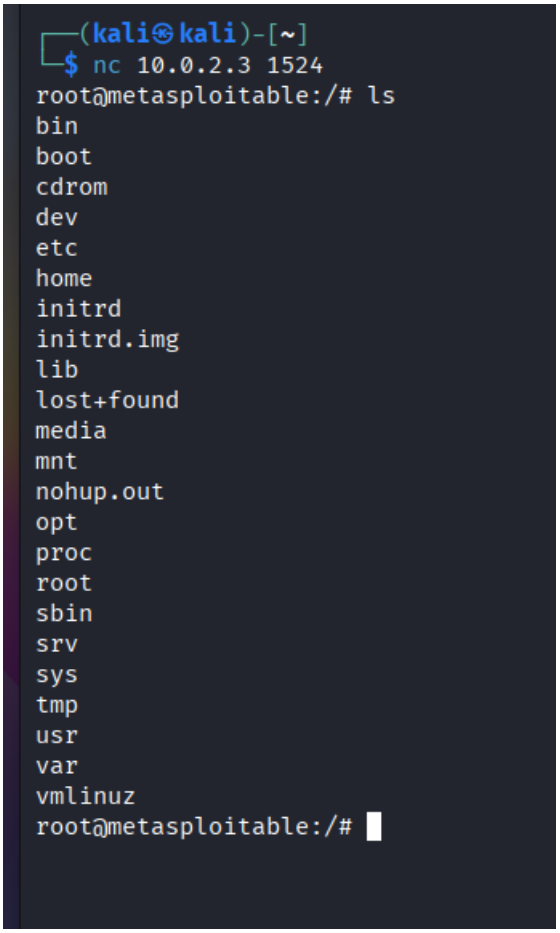
Dopo l'identificazione della porta aperta, è stata stabilita una connessione diretta utilizzando un semplice client di rete (netcat). La connessione non ha richiesto alcuna autenticazione, poiché il servizio era configurato per fornire immediatamente una shell all'host che si collegava. Questo comportamento indica la presenza di una **backdoor attiva**, non di una vulnerabilità potenziale.

Una volta stabilita la connessione, il sistema ha restituito direttamente un prompt di shell con privilegi **root**, come dimostrato dal prompt root@metasploitable:/#. L'esecuzione del comando di listing (ls) mostra la struttura completa del filesystem di sistema, confermando il pieno accesso all'host compromesso. Non è stata necessaria alcuna fase di privilege escalation, poiché l'accesso iniziale era già fornito con i massimi privilegi.

Questo risultato rappresenta una **compromissione completa del sistema** ottenuta tramite accesso remoto diretto. Dal punto di vista metodologico, il passaggio dimostra la validazione pratica di una vulnerabilità critica segnalata in fase di scansione: ciò che inizialmente era stato classificato come rischio elevato viene qui confermato come **controllo effettivo del sistema**.

In un contesto reale, una backdoor di questo tipo consentirebbe a un attaccante di operare indisturbato sull'host, installare malware persistente, muoversi lateralmente nella rete e compromettere ulteriori sistemi. L'esempio evidenzia l'importanza di distinguere tra vulnerabilità teoriche e vulnerabilità che offrono **accesso immediato e non autenticato**, le quali rappresentano il livello massimo di criticità in un'analisi di sicurezza.

Screen risultato:



VNC Server 'password' Password:

L’accesso remoto al sistema è stato ottenuto sfruttando una configurazione debole del servizio VNC in esecuzione sulla macchina target Metasploitable. Durante la fase di Vulnerability Assessment, lo scanner ha identificato che il servizio VNC esponeva un meccanismo di autenticazione estremamente debole, accettando come credenziale la password letterale *“password”*. Questa condizione è stata classificata come vulnerabilità critica perché consente l’accesso remoto senza alcuna forma di protezione reale.

A differenza di molte vulnerabilità che richiedono exploit specifici o catene di attacco complesse, in questo caso il servizio era direttamente accessibile sulla rete e non richiedeva alcuna autenticazione robusta. La connessione è avvenuta utilizzando un normale client VNC, che ha eseguito il protocollo di autenticazione standard e ha ricevuto una risposta positiva dal server. Questo conferma che la vulnerabilità non era solo teorica, ma attivamente sfruttabile.

Una volta completata l’autenticazione, il server VNC ha esposto la sessione grafica associata all’utente root. Questo aspetto è particolarmente critico: l’accesso non avviene come utente limitato, ma direttamente con i massimi privilegi di sistema. Di conseguenza, l’attaccante ottiene pieno controllo della macchina, con possibilità di eseguire comandi, modificare configurazioni, accedere ai file e compromettere completamente il sistema.

Questo risultato dimostra il passaggio netto dalla fase di analisi delle vulnerabilità alla compromissione effettiva del sistema. Il finding riportato dallo scanner viene validato manualmente, trasformandosi da segnalazione di rischio a prova concreta di accesso non autorizzato. In un contesto reale, una vulnerabilità di questo tipo rappresenterebbe un *initial access* immediato e definitivo, rendendo superflue ulteriori tecniche di escalation dei privilegi.

L’esempio evidenzia come una singola configurazione errata, specialmente su un sistema già obsoleto e fuori supporto, sia sufficiente a compromettere completamente un’infrastruttura esposta in rete.

Screen risultato: