S5L4,

BENVENUTI LUIGI, 22/02/2024

Traccia:

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo).

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

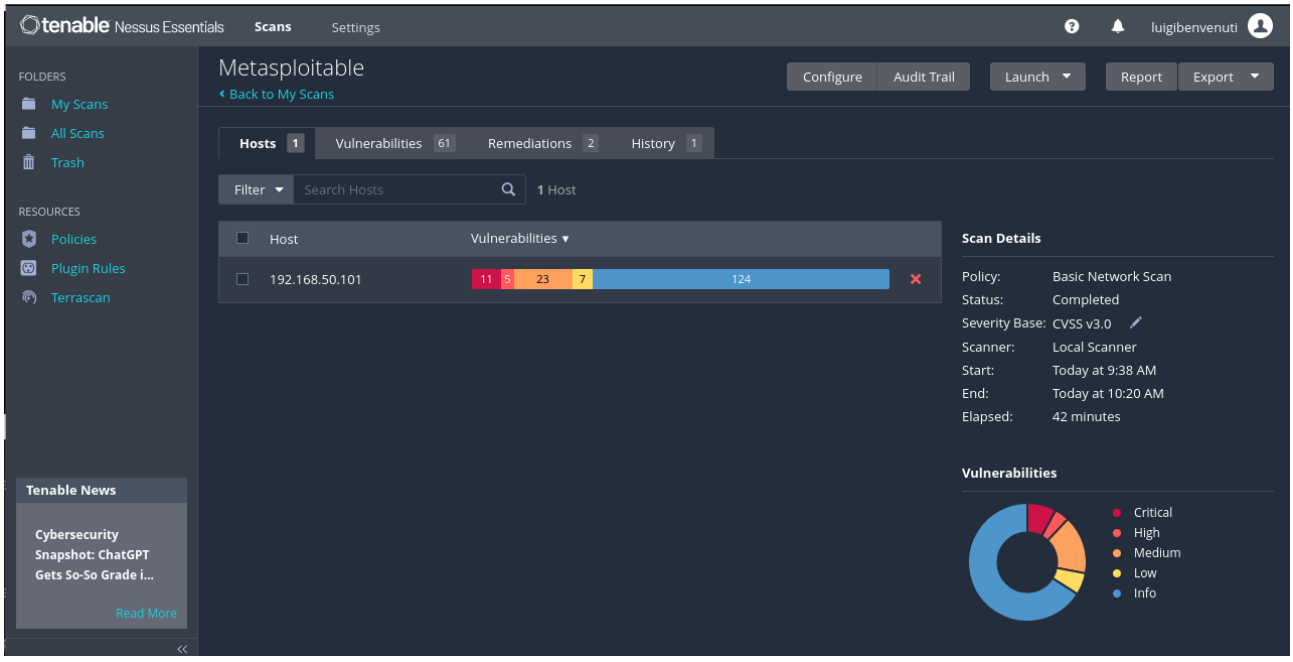
● Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni.

● Familiarizzare con alcune delle vulnerabilità note che troverete spesso sul vostro percorso da penetration tester.

Una volta terminata l'installazione di Nessus, andiamo a sfruttarne le capacità di scansione verso la macchina Metasploitable, come precedentemente richiesto. Per fare ciò, selezioniamo la voce "Basic Network Scan", che ci fornisce una scansione con funzioni base di default, ed inseriamo come IP target quello della macchina Metasploitable.

Selezioniamo poi l'opzione <<port scan common ports>>, per andare a scansionare soltanto le porte più frequenti.

Il risultato della scansione è il seguente:



Scarichiamo il report in formato PDF utilizzando la funzione <<Report>> in alto a destra.

192.168.50.101

9	4	17	6	70
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 106

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	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	9.1	-	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

Nella prima parte del report generato, ci vengono ricapitolate le vulnerabilità rilevate sulla macchina scansionata.

Vediamo nel dettaglio il significato di alcune voci:

- Severity: indica il grado di pericolosità di una vulnerabilità, ed ha 5 voci. Oltre a critical, high, medium e low, fornisce una voce info, che sta ad indicare che la macchina espone alcune possibili informazioni interessanti per un eventuale attaccante.
- CVSS: Common Vulnerability Scoring System, metodo standard di valutazione della gravità di una vulnerabilità.
- VPR score: Vulnerability Priority Rating, è uno score fornito direttamente da Nessus che consiglia un'indice di priorità nell'applicazione delle patch.
- Plugin: indica l'ID plugin di Nessus che ha scovato la vulnerabilità.
- Name: indica il nome della vulnerabilità rilevata.

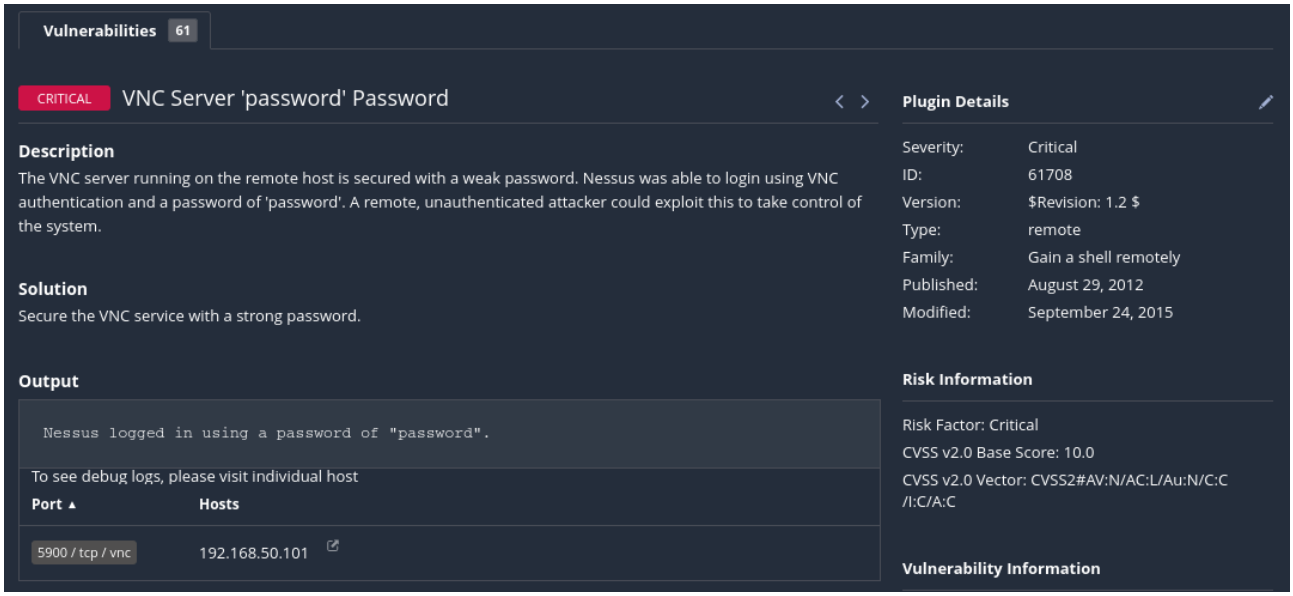
Analizziamo una criticità per ogni severity, cercando di capirne il significato.

1- Critical

Prendiamo in esame la criticità con pericolosità Critical di nome “VNC Server Password password”;

Questa vulnerabilità ha CVSS 10, quindi massimo. Essa sta ad indicare che una virtual network computing app ha come password di accesso “password”, facilmente reperibile da un potenziale attaccante. Si potrebbe sfruttare la vulnerabilità per lanciare una shell e prendere il comando del server.

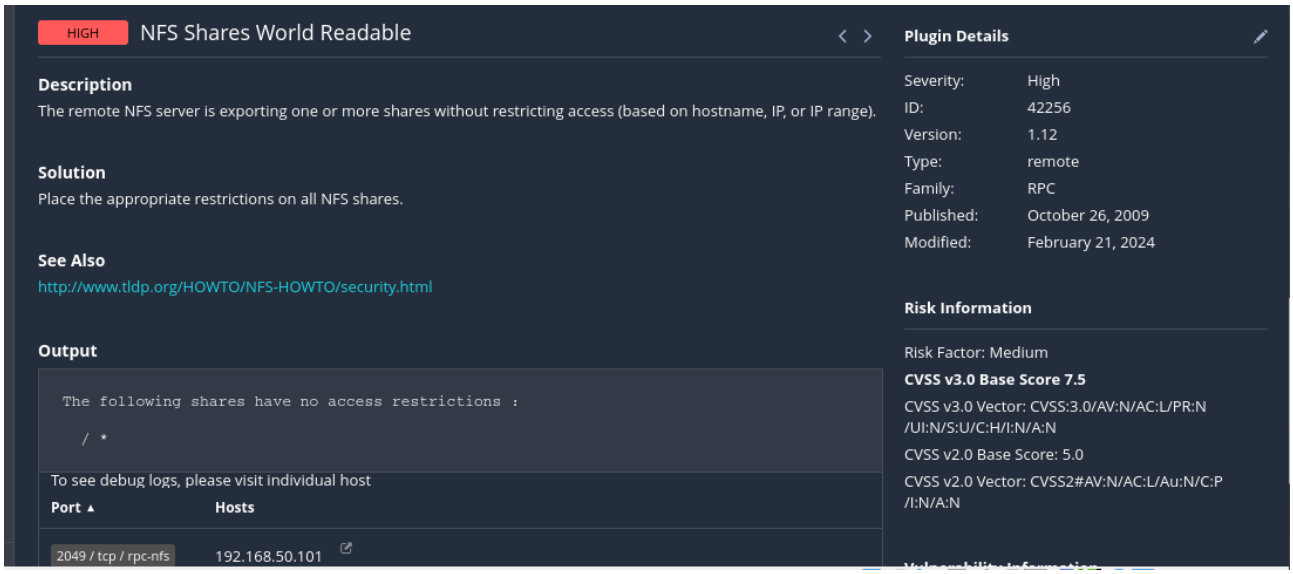
Vediamo le specifiche della voce fornite da Nessus:



2- High

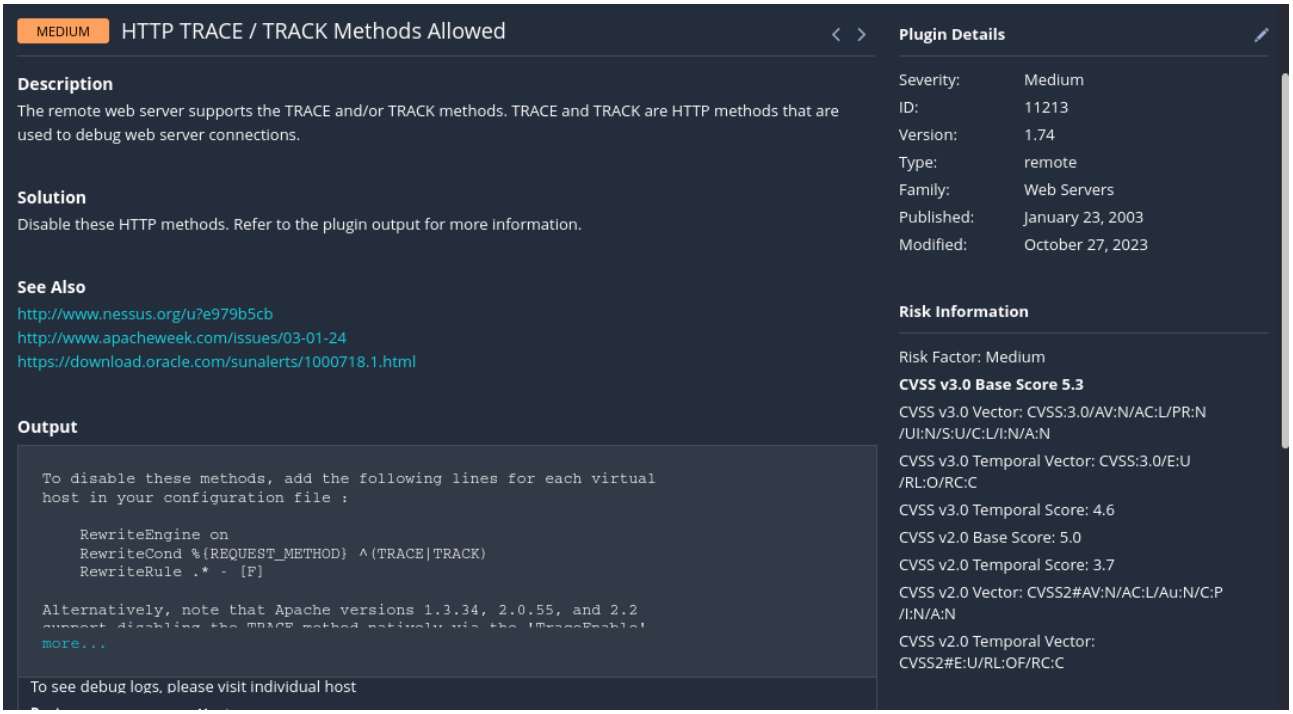
Prendiamo in esame la criticità con pericolosità High di nome NFS Shares World Readable.

Si riferisce alla famiglia delle RPC (chiamate di procedura remota), ovvero la capacità di avviare un programma da un computer diverso da quello host. In particolare, un server NFS trasmette esportazioni di rete sensibili in maniera leggibile. Nessus consiglia di raffinare le restrizioni applicate allo sharing del file system in questione. Questa debolezza ha CVSS 7.5.



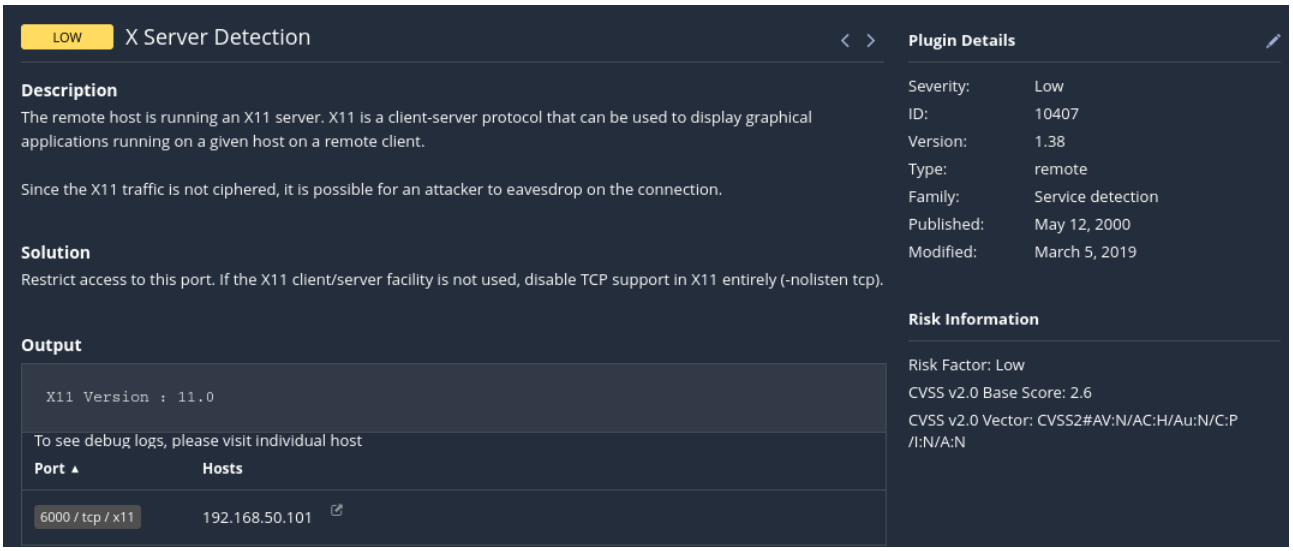
3- Medium

Prendiamo in esame la criticità con pericolosità Medium di nome “HTTP TRACE/TRACK METHOD ALLOWED”. La vulnerabilità ha uno score 5.3 e riguarda l’abilitazione del metodo HTTP trace; esso consente di inviare al server un messaggio loopback per tracciare il path e fornire un meccanismo di debugging. Anche questa vulnerabilità è di tipo RPC.
Il tool consiglia di disabilitare il metodo.



4- Low

Prendiamo in esame la criticità con pericolosità Low di nome “X Server Detection”.
La vulnerabilità è della famiglia “Service detection” ed indica che sulla porta 6000 è attivo un servizio X11 in ascolto per la visualizzazione grafica di applicazioni da client remoto, ed il traffico non è cifrato. Il tool consiglia di restringere l’accesso alla suddetta porta.



5- Info

Prendiamo infine in esame la criticità con pericolosità INFO di nome “Unknown Service Detection: Banner Retrieval”.
Questa debolezza è relativa a delle informazioni esposte da un banner di uno script; il tool non ha rilevato a quale script esse possano far riferimento. Le informazioni esposte potrebbero comunque fare gola ad un aspirante intruso.