EPICODE S5-L4

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

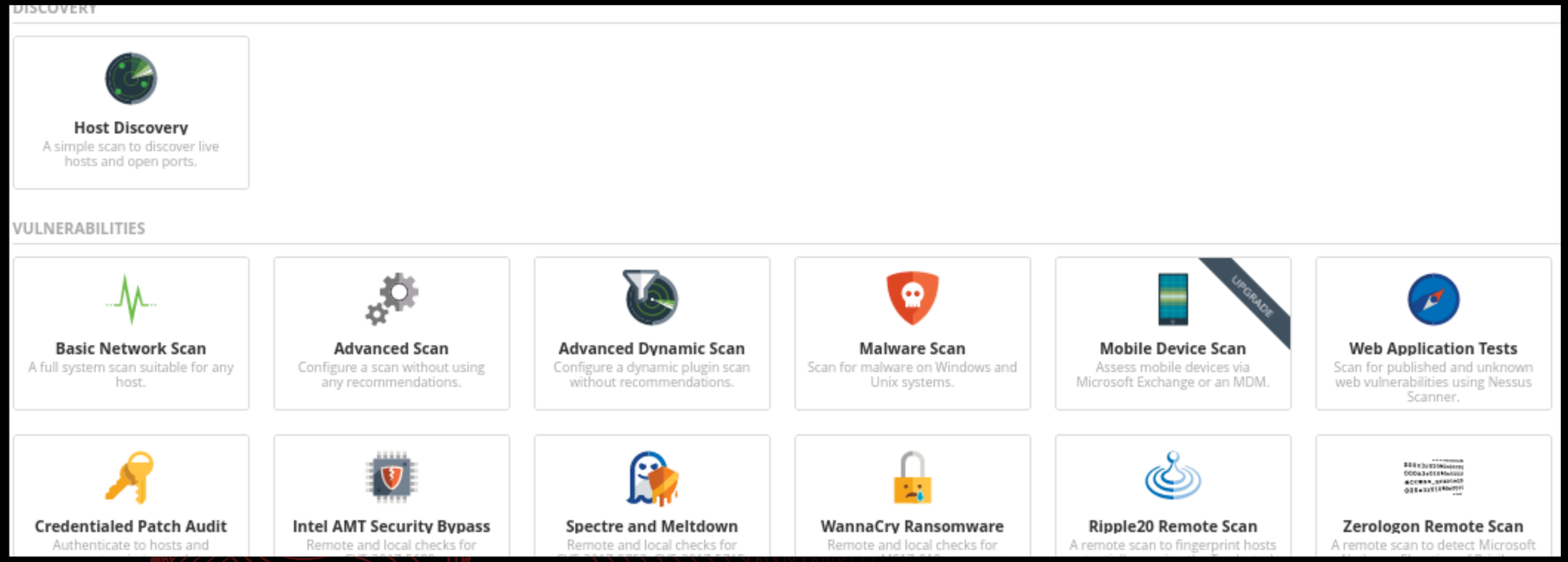
- FARE PRATICA CON LO STRUMENTO, CON LA CONFIGURAZIONE E L'AVVIO DELLE SCANSIONI.
- FAMILIARIZZARE CON ALCUNE DELLE VULNERABILITÀ NOTE CHE TROVERETE SPESSO SUL VOSTRO PERCORSO DA PENETRATION TESTER

COSA È NESSUS?

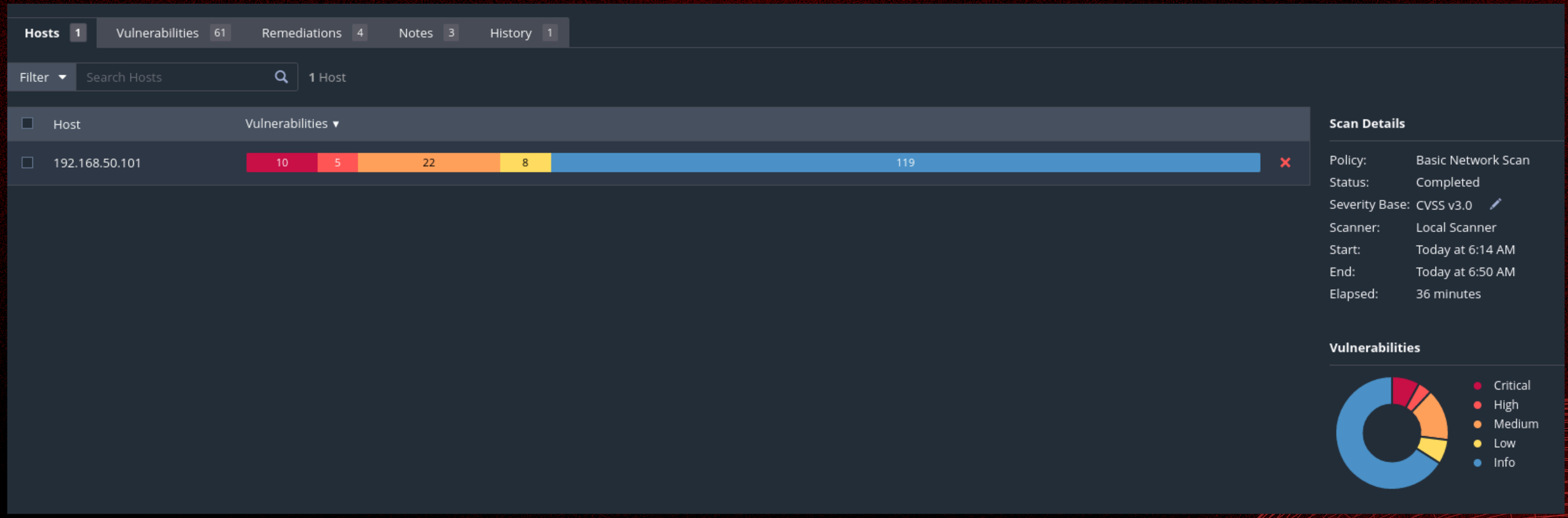
NESSUS È UNO DEI SOFTWARE PIÙ UTILIZZATI PER LA SCANSIONE E L'ANALISI DELLE VULNERABILITÀ DI SICUREZZA NEI SISTEMI INFORMATICI.

NESSUS È IN GRADO DI INDIVIDUARE UNA VASTA GAMMA DI VULNERABILITÀ, COME FALLE DI SICUREZZA SOFTWARE, CONFIGURAZIONI NON SICURE E POTENZIALI MINACCE ALLA SICUREZZA. IL SOFTWARE ESEGUE SCANSIONI AUTOMATIZZATE DEI SISTEMI, IDENTIFICA LE VULNERABILITÀ E FORNISCE REPORT DETTAGLIATI SULLE MISURE CORRETTIVE DA PRENDERE.

NELLA FIGURA IN BASSO, POSSIAMO NOTARE ALCUNE DELLE FUNZIONI PRINCIPALI DEL SOFTWARE



Possiamo notare che a seguito di una scansione Basic sulla macchina Metasploitable nel nostro laboratorio virtuale, sono state trovate più di 60 vulnerabilità di cui alcune critiche, che rappresentano una reale minaccia per eventuali attacchi esterni

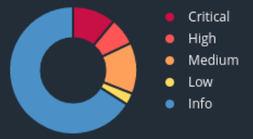


Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	Samba Badlock Vulnerability	General	1
HIGH	7.5		NFS Shares World Readable	RPC	1
MIXED	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9	4.4	SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9	4.4	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

Host Details

IP:	192.168.50.101
MAC:	08:00:27:EC:B7:92
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	Today at 6:14 AM
End:	Today at 6:50 AM
Elapsed:	36 minutes
KB:	Download

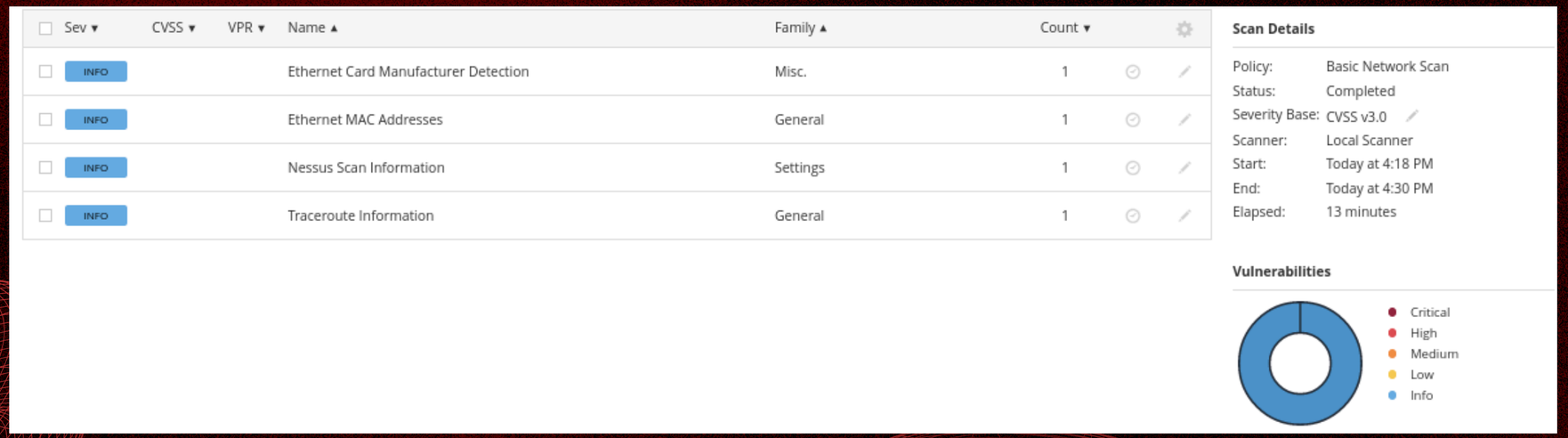
Vulnerabilities



Il risultato della scansione è molto dettagliato e ci permette di analizzare ogni vulnerabilità dandoci consigli per rimediare alle vulnerabilità.

MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2
LOW	2.6 *		X Server Detection	Service detection	1
LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	TLS (Multiple Issues)	General	4
INFO	...	...	VNC (Multiple Issues)	Service detection	3

Scansione su Windows 7 con il Firewall attivo, e come si può vedere la scansione non produce molti risultati, sono state trovate solo 4 vulnerabilità e nessuna particolarmente rilevante.



Sev	CVSS	VPR	Name	Family	Count
INFO			Ethernet Card Manufacturer Detection	Misc.	1
INFO			Ethernet MAC Addresses	General	1
INFO			Nessus Scan Information	Settings	1
INFO			Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:18 PM
End:	Today at 4:30 PM
Elapsed:	13 minutes

Vulnerabilities

Hosts 1 | Vulnerabilities 18 | Notes 1 | History 4

Filter | Search Vulnerabilities | 18 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	--	--	Microsoft Windows (Multiple Issues)	Windows	5
MIXED	--	--	SMB (Multiple Issues)	Misc.	2
LOW	2.1 *		ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	--	--	SMB (Multiple Issues)	Windows	7
INFO			DCE Services Enumeration	Windows	8
INFO			Nessus SYN scanner	Port scanners	3
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Ethernet Card Manufacturer Detection	Misc.	1
INFO			Ethernet MAC Addresses	General	1
INFO			Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
INFO			Nessus Scan Information	Settings	1
INFO			Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO			OS Identification	General	1
INFO			OS Security Patch Assessment Not Available	Settings	1
INFO			Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 3:26 PM
End:	Today at 3:29 PM
Elapsed:	3 minutes

Vulnerabilities

Scansione su Windows 7 con il Firewall disattivato, rilevate 18 vulnerabilità di medio e basso livello

REALIZZATO DA

MICHAEL ANDREOLI

OTMAN HMICH

STEFANO CESARONI