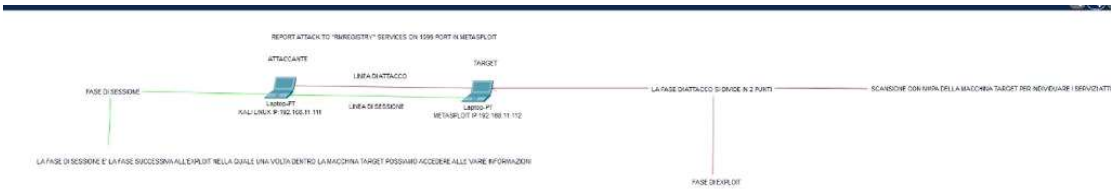
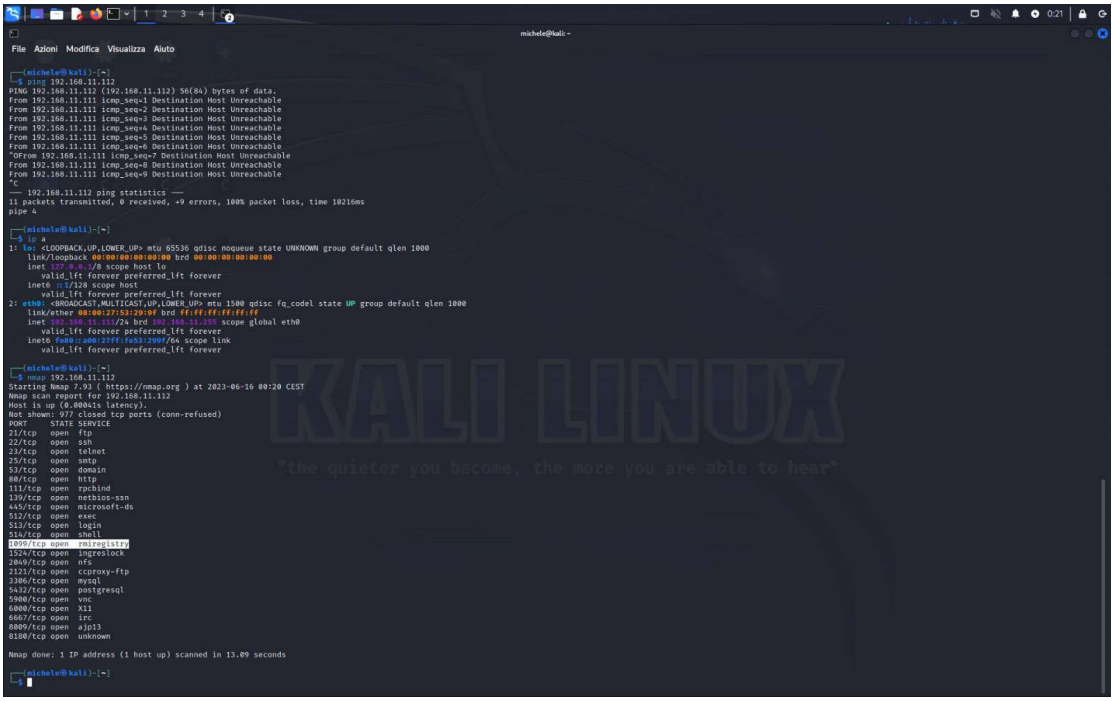
REPORT VULNERABILITA' JAVA RMI



FASE DI ATTACCO

LA FASE DI ATTACCO SI DIVIDE IN 2 PASSAGGI, LA PRIMA E' LA FASE DI SCANSIONE DELLE PORTE APERTE CON RELATIVI SERVIZI ATTIVI TRAMITE IL COMANDO "NMPA" SUL NOSTRO TERMINALE DELLA MACCHINA ATTACCANTE, VERSO LA MACCHINA TARGET.

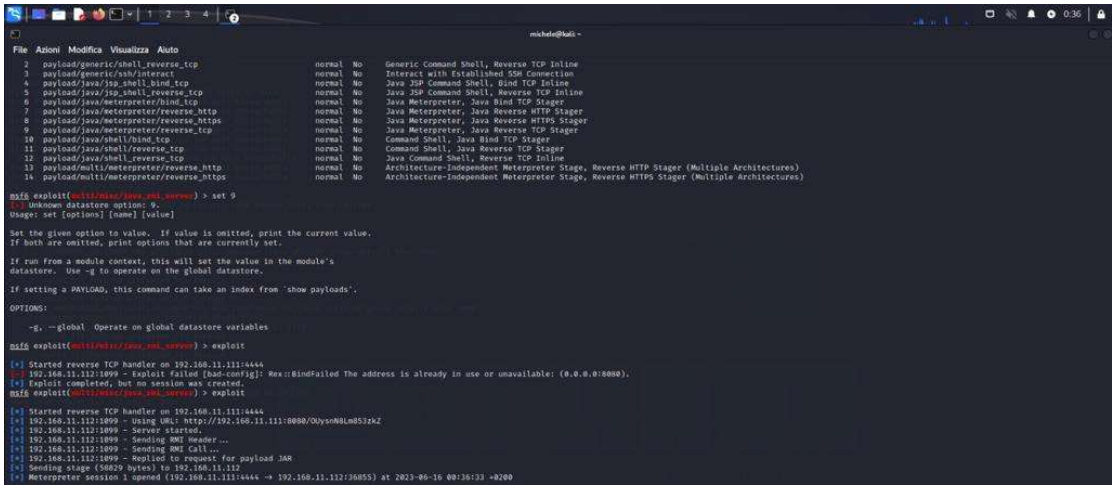


CON QUESTA SCANSIONE CI VENGONO RIPORTATI I SERVIZI ATTIVI CON LE PORTE ANNESSE, NEL NOSTRO CASO IL SERVIZIO CHE CI INTERESSA E' QUELLO SULLA PORTA "1099" OVVERO "RMIREGISTRY".

DOPO AVER CAPITO CHE SERVIZIO COLPIRE APRIAMO SEMPRE DA TERMINALE "MFSCOSNOLE" PER ANDARE A PREPARARCI PER LA FASE DI EXPLOIT.

UNA VOLTA APERTO MFSCONSOLE ANDIAMO A CONFIGURARE IL NOSTRO EXPLOIT COME SEGUE:

PER PRIMA COSA CON IL COMANDO "SEARCH" ANDIAMO A CERCARE IL SERVIZIO CHE CI INTERESSA (SEARCH RMIREGISTRY) UNA VOLTA ANDATO A SCEGLIERE L'EXPLOIT DA USARE ANDIAMO A CONFIGURARE I NOSTRI RHOST E RPORT (ENTRAMBI FANNO RIFERIMENTO ALLA MACCHINA TARGET), UNA VOLTA SETTATI L'IP DELLA MACCHINA TARGET E LA PORTA DEL SERVIZIO, ANDIAMO A SCEGLIERE IL PAYLOAD DA UTILIZZARE (POICHE' SENZA PAYLOAD L'EXPLOIT NON ANDREBBE A BUON FINE A DIFFERENZA DELL'AUXILIARY MOD)

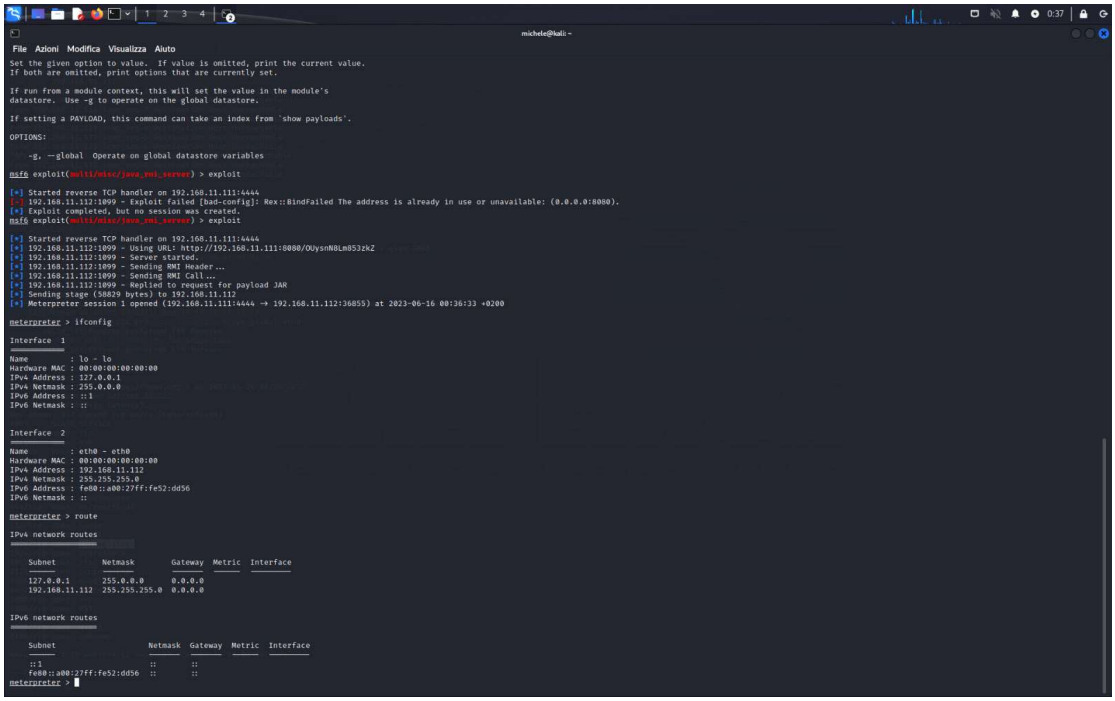


DOPO AVER SCELTO IL PAYLOAD LANCIAMO L'EXPLOIT CON IL COMANDO "EXPLOIT". SE L'EXPLOIT HA ESITO POSITIVO CI VERRA' RESTITUITA UNA SESSIONE NELLA MACCHINA TARGET.

FASE DI SESSIONE

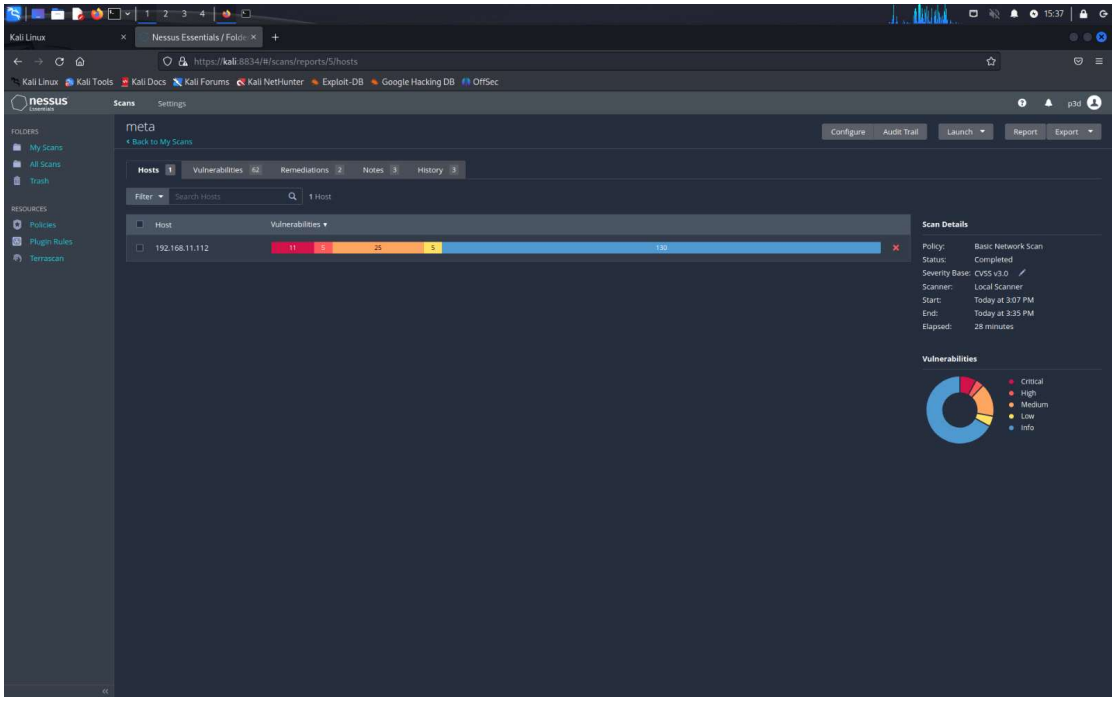
PER LA FASE DI SESSIONE INVECE, UNA VOLTA AVER COMPLETATO LA FASE DI EXPLOIT E

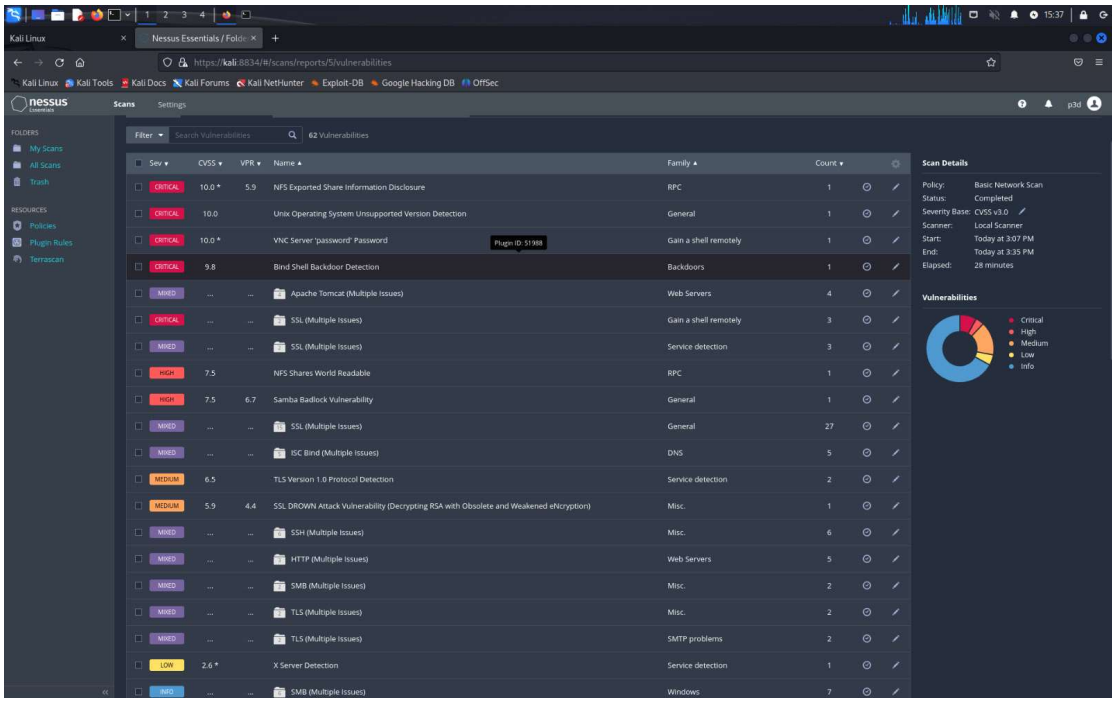
QUINDI AVENDO ACQUISITO UNA SESSIONE NEL SISTEMA TARGET ANDIAMO A REPERIRE LE INFORMAZIONI DI RETE E LA TABELLA DI ROUTING. PER LA RETE UTILIZZIAMO IL COMANDO "IFCONFIG" MENTRE PER LA TABELLA DI ROUTING IL COMANDO "ROUTE".

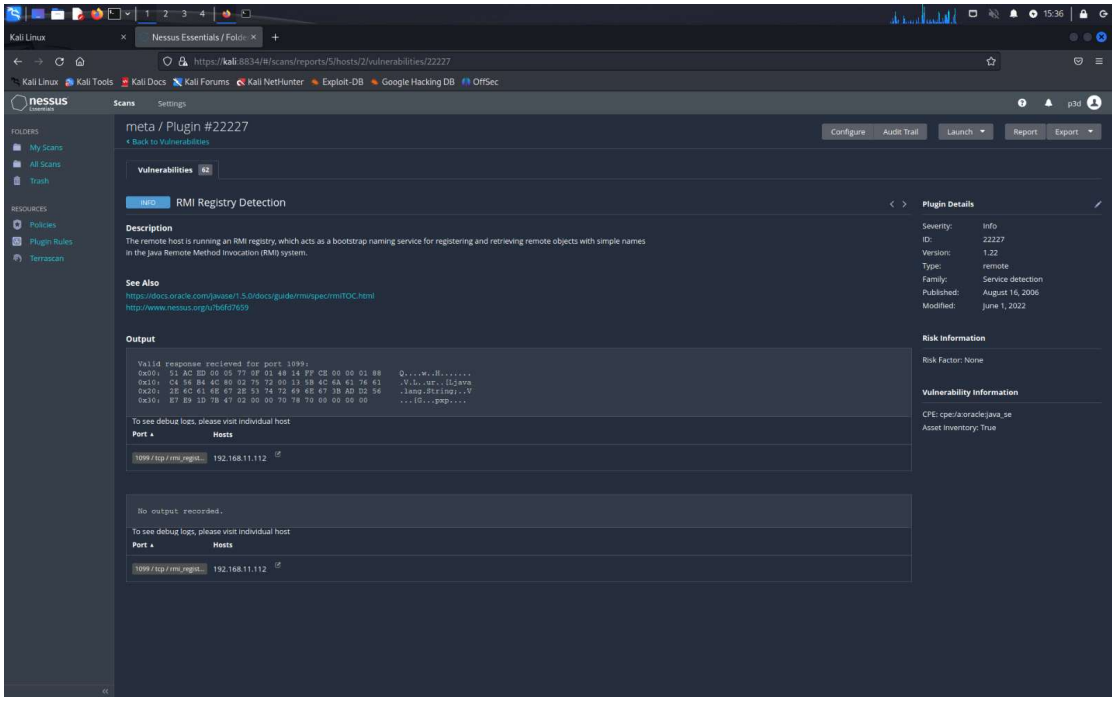


MENTRE CON IL COMANDO "CHECKVM" CAPIAMO SE CI TROVIAMO DAVANTI UNA MACCHINA VIRTUALE O UN COMPUTER REALE.

ANALISI CON NESSUS


Kali Linux
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/hosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus Essentials
Scans Settings
p3d
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
meta
Back to My Scans
Configure Audit Trail Launch Report Export
Hosts 1 Vulnerabilities 62 Remediations 2 Notes 3 History 3
Filter Search Hosts 1 Host
Host Vulnerabilities
192.168.11.112 11 5 25 5 130
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:07 PM
End: Today at 3:35 PM
Elapsed: 28 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


Kali Linux
Nessus Essentials / Folde
https://kali:8834/#/scans/reports/5/vulnerabilities
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
nessus Essentials
Scans Settings
p3d
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Filter Search Vulnerabilities 62 Vulnerabilities
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 Plugin ID: 51988 Gain a shell remotely 1
CRITICAL 9.8 Bind Shell Backdoor Detection Backdoors 1
MIXED ... ... Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL ... ... SSL (Multiple Issues) Gain a shell remotely 3
MIXED ... ... SSL (Multiple Issues) Service detection 3
HIGH 7.5 NFS Shares World Readable RPC 1
HIGH 7.5 6.7 Samba Badlock Vulnerability General 1
MIXED ... ... SSL (Multiple Issues) General 27
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 DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) Misc. 1
MIXED ... ... SSH (Multiple Issues) Misc. 6
MIXED ... ... HTTP (Multiple Issues) Web Servers 5
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
INFO ... ... SMB (Multiple Issues) Windows 7
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:07 PM
End: Today at 3:35 PM
Elapsed: 28 minutes
Vulnerabilities
Critical
High
Medium
Low
Info



PER ESSERE SICURI SUL LAVORO SVOLTO OLTRE AD NMAP USATO INIZIALMENTE ABBIAMO FATTO UNA BASIC SCANSIONE E SIAMO ANDATI A CERCARE LA VULNERABILITA' DEL SERVIZIO "RMIREGISTRY".