S5 L4

Svolgimento Progetto

Giulia Salani

Consegna

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).

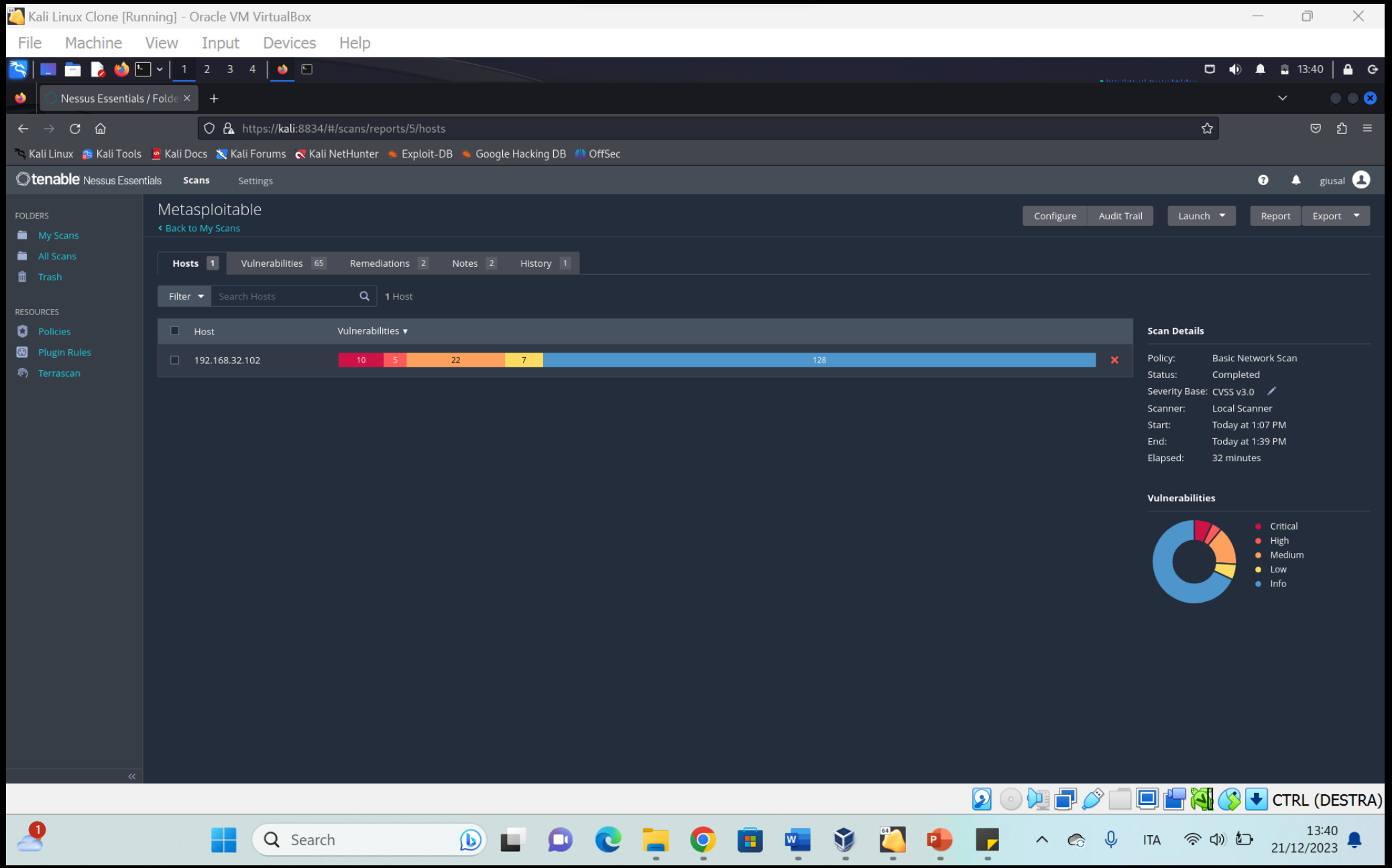
A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

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.

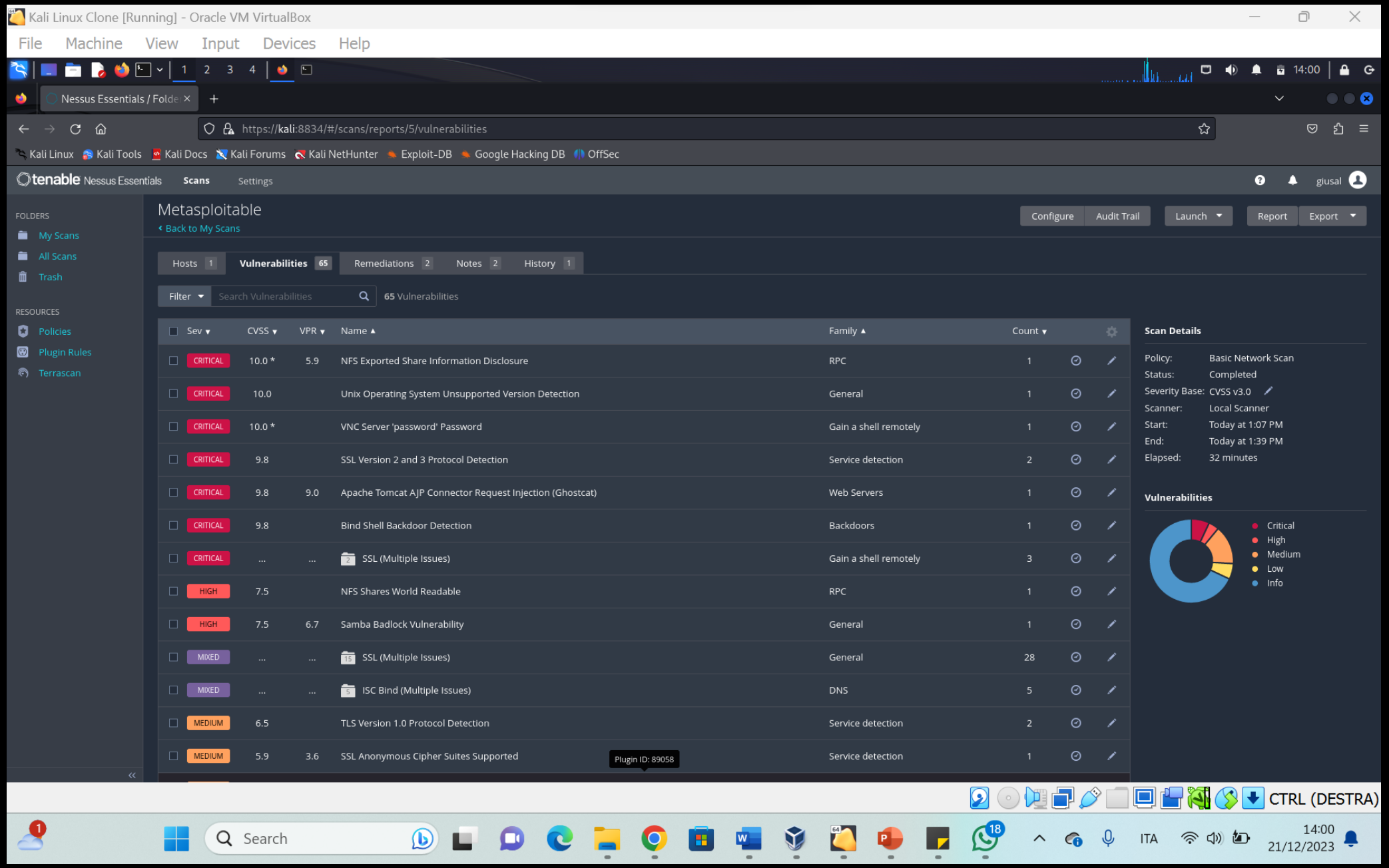
Svolgimento

1. Ho installato Nessus su Kali, con scheda di rete in bridged.
2. Ho impostato la NIC in internal e modificato l’IP di Kali in modo che fosse sulla stessa rete di Meta.
3. A questo punto ho fatto partire la scansione su Meta.

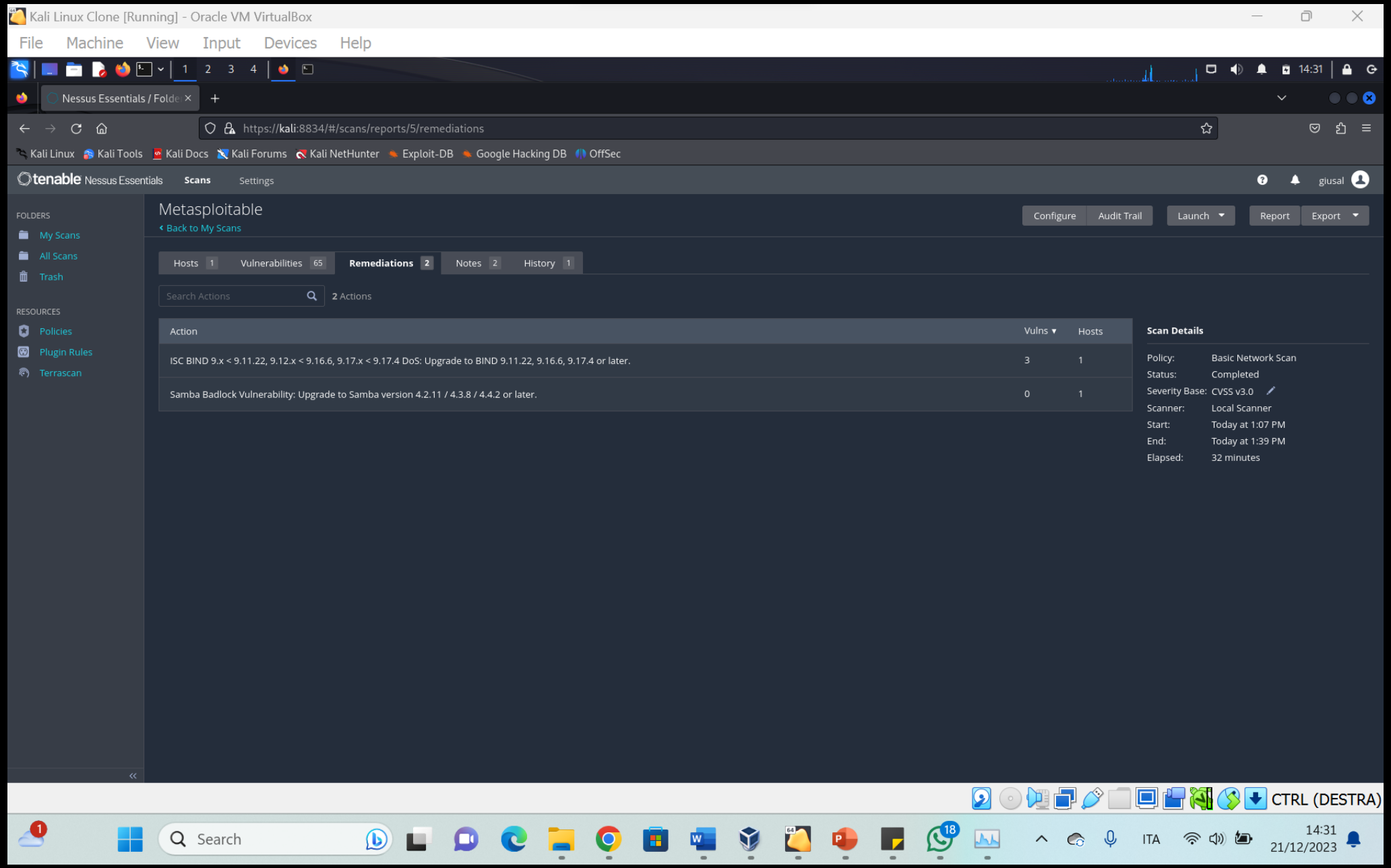
Questo il riepilogo della scansione, con la distribuzione delle vulnerabilità per gravità:



Nella tab «Vulnerabilities» è possibile approfondirle una per una:



Nella tab «Remediations», invece, è indicato come porvi rimedio:



Metasploitable / Plugin #11356

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 65** | Remediations 2 | Notes 2 | History 1

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.32.102

La vulnerabilità indica che almeno una delle condivisioni NFS (Network File System) sul server remoto può essere montata dall'host di scansione. Questo potrebbe consentire a un attaccante di accedere e potenzialmente modificare file sul server attraverso NFS. Per mitigare, occorre limitare l'accesso NFS solo agli host autorizzati e configurare correttamente le autorizzazioni e le regole di firewall.

Plugin Details

Severity:	Critical
ID:	11356
Version:	1.21
Type:	remote
Family:	RPC
Published:	March 12, 2003
Modified:	August 30, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Collapse Menu (/)

Metasploitable / Plugin #33850

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 65** | Remediations 2 | Notes 2 | History 1

CRITICAL **Unix Operating System Unsupported Version Detection**

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Output

```
Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09
Upgrade to Ubuntu 23.04 / LTS 22.04 / LTS 20.04 .

For more information, see : https://wiki.ubuntu.com/Releases
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.32.102

La vulnerabilità indica che il sistema Unix sul host remoto utilizza una versione non più supportata, rendendolo vulnerabile a potenziali minacce poiché non riceverà ulteriori patch di sicurezza dal produttore. Per mitigare, occorre aggiornare a una versione supportata o implementare misure di sicurezza aggiuntive per proteggere il sistema.

Plugin Details

Severity:	Critical
ID:	33850
Version:	1.289
Type:	combined
Family:	General
Published:	August 8, 2008
Modified:	October 18, 2023

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

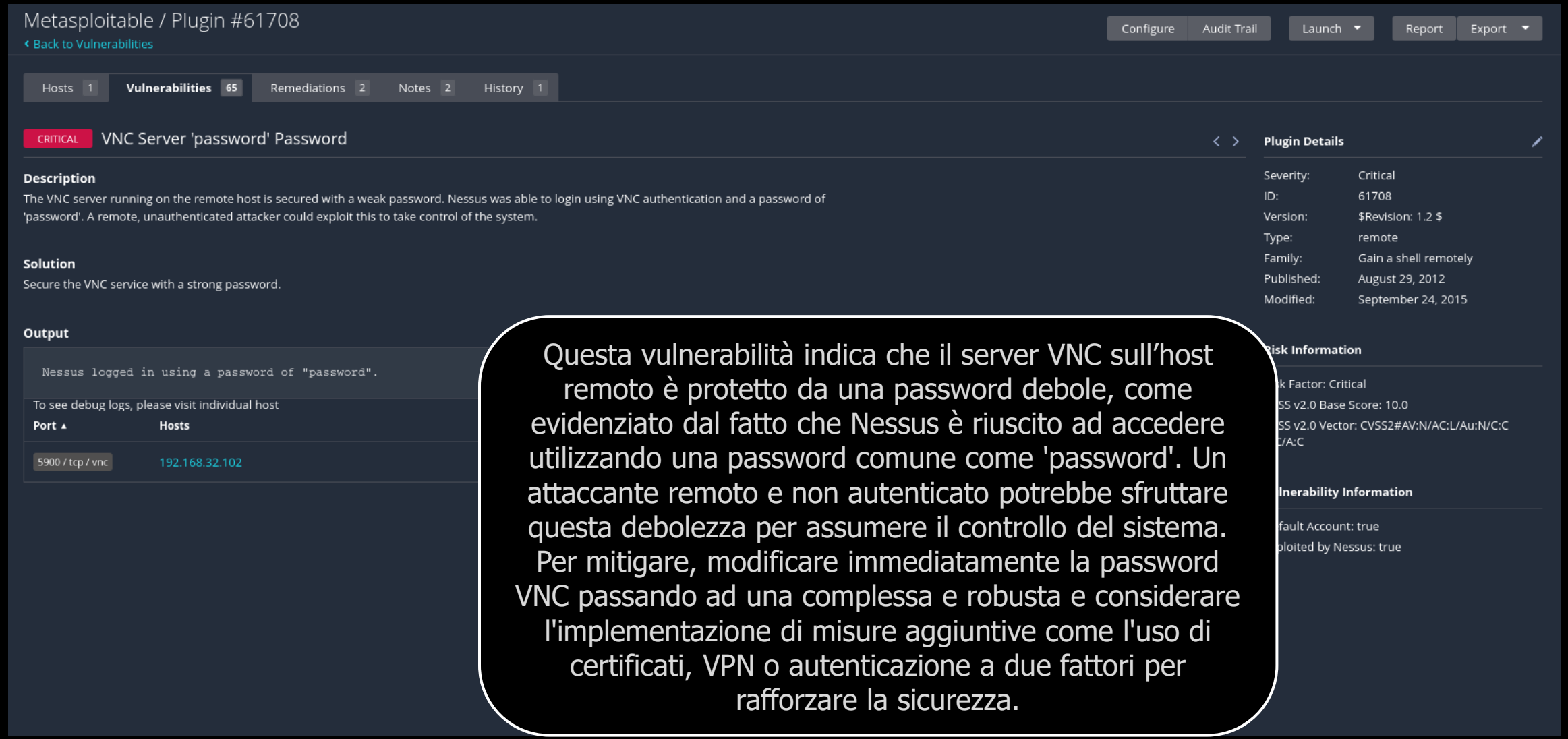
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Unsupported by vendor: true

Reference Information

IAVA: 0001-A-0502, 0001-A-0648



Questa vulnerabilità indica che il server VNC sull'host remoto è protetto da una password debole, come evidenziato dal fatto che Nessus è riuscito ad accedere utilizzando una password comune come 'password'. Un attaccante remoto e non autenticato potrebbe sfruttare questa debolezza per assumere il controllo del sistema. Per mitigare, modificare immediatamente la password VNC passando ad una complessa e robusta e considerare l'implementazione di misure aggiuntive come l'uso di certificati, VPN o autenticazione a due fattori per rafforzare la sicurezza.

Metasploitable / Plugin #20007

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 65** | Remediations 2 | Notes 2 | History 1

CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt co

Although SSL/TLS has a secure means for choosing the highest supported version of or server support nothing better), many web browsers implement this in an unsafe in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communication version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Plugin Details

Severity:	Critical
ID:	20007
Version:	1.34
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	April 4, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

La vulnerabilità indica che il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0, versioni vulnerabili a diversi difetti crittografici come schemi di padding insicuri e rinegoziazione non sicura. Questi difetti possono consentire a un attaccante di condurre attacchi di tipo "man-in-the-middle" o decifrare comunicazioni. È consigliato disabilitare completamente questi protocolli e utilizzare invece TLS 1.2 o versioni successive con suite crittografiche approvate.

Metasploitable / Plugin #134862

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities 65** | Remediations 2 | Notes 2 | History 1

CRITICAL **Apache Tomcat AJP Connector Request Injection (Ghostcat)**

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

See Also

http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
https://access.redhat.com/security/cve/CVE-2020-1745
https://access.redhat.com/solutions/4851251
http://www.nessus.org/u?dd218234
http://www.nessus.org/u?dd772531
http://www.nessus.org/u?2a01d6bf
http://www.nessus.org/u?3b5af27e
http://www.nessus.org/u?9dab109f
http://www.nessus.org/u?5eafcf70

Output

```
Nessus was able to exploit the issue using the following reque

0x0000:  02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ..
0x0010:  61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    as
0x0020:  09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .lo
0x0030:  6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocal
         00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep
```

Collapse Menu (/)

Plugin Details

Severity:	Critical
ID:	134862
Version:	1.42
Type:	remote
Family:	Web Servers
Published:	March 24, 2020
Modified:	September 25, 2023

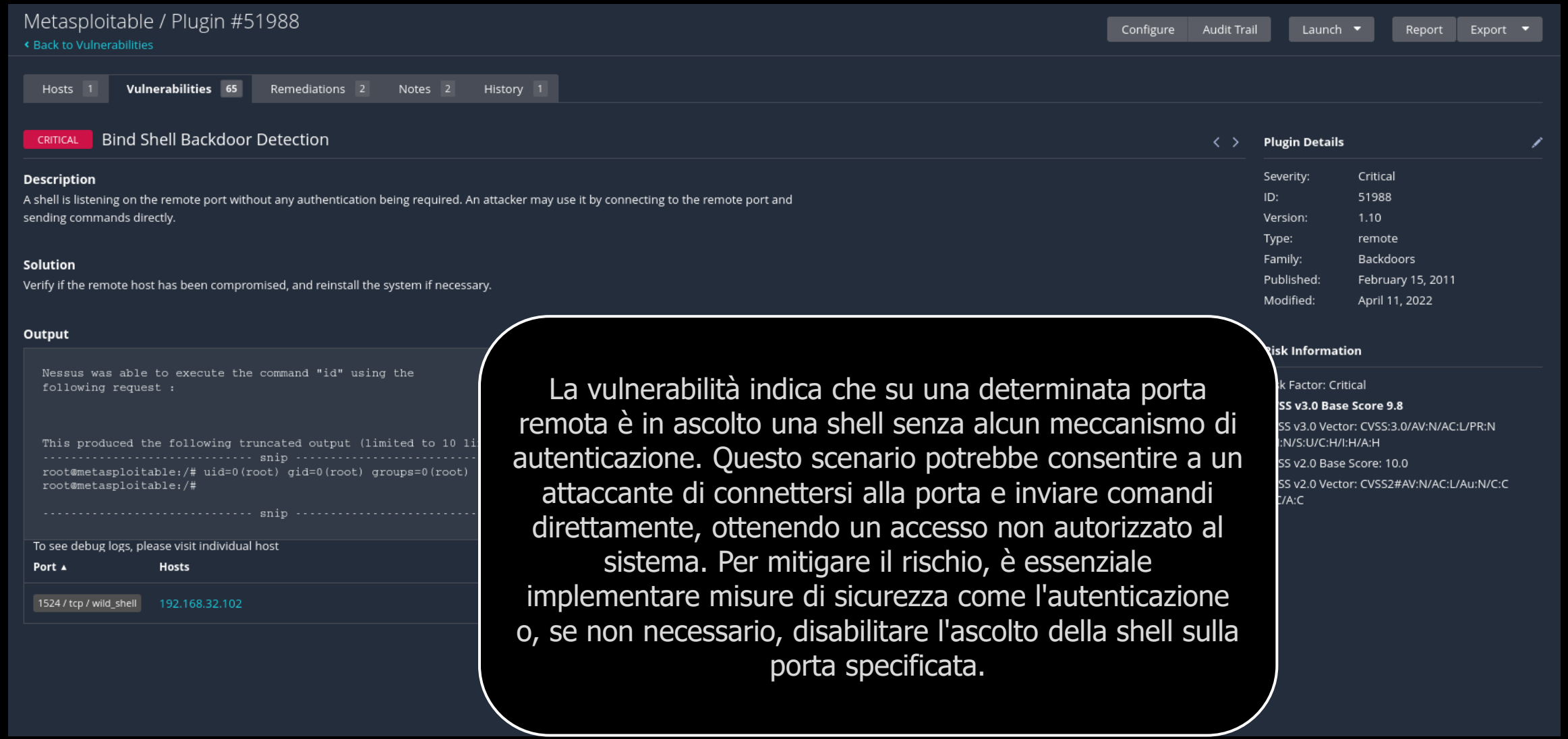
VPR Key Drivers

reat Recency: No recorded events
reat Intensity: Very Low
oloit Code Maturity: High
e of Vuln: 730 days +
oduct Coverage: Very High
SSV3 Impact Score: 5.9
reat Sources: No recorded events

sk Information

lnerability Priority Rating (VPR): 9.0
sk Factor: High
VSS v3.0 Base Score 9.8
SS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N
I:N/S:U/C:H/I:H/A:H
VSS v3.0 Temporal Vector: CVSS:3.0/E:H
/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4

La vulnerabilità riguarda una vulnerabilità di lettura/inclusione file nel connettore AJP. Un attaccante remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere file dell'applicazione web o, se consentito, caricare codice maligno JSP per eseguire codice a distanza (RCE). Per mitigare, aggiorna la configurazione AJP per richiedere autorizzazione e/o esegui un aggiornamento del server Tomcat alla versione 7.0.100, 8.5.51, 9.0.31 o successive.



La vulnerabilità indica che su una determinata porta remota è in ascolto una shell senza alcun meccanismo di autenticazione. Questo scenario potrebbe consentire a un attaccante di connettersi alla porta e inviare comandi direttamente, ottenendo un accesso non autorizzato al sistema. Per mitigare il rischio, è essenziale implementare misure di sicurezza come l'autenticazione o, se non necessario, disabilitare l'ascolto della shell sulla porta specificata.

La vulnerabilità indica che il certificato x509 sul server SSL remoto è stato generato su un sistema Debian o Ubuntu affetto da un difetto nel generatore di numeri casuali della sua libreria OpenSSL. A causa di questa mancanza di entropia, un attaccante potrebbe facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare le sessioni o eseguire un attacco "man-in-the-middle". Per risolvere, è necessario rigenerare il certificato con una versione corretta di OpenSSL e sostituire i certificati compromessi.