



NESSUS SCAN REPORT

Presented by Conti Samuele

Task

Obiettivi

Il progetto di questa settimana richiedeva lo scan e la risoluzione di almeno 2 vulnerabilità critiche identificate sulla piattaforma

Metasploit:

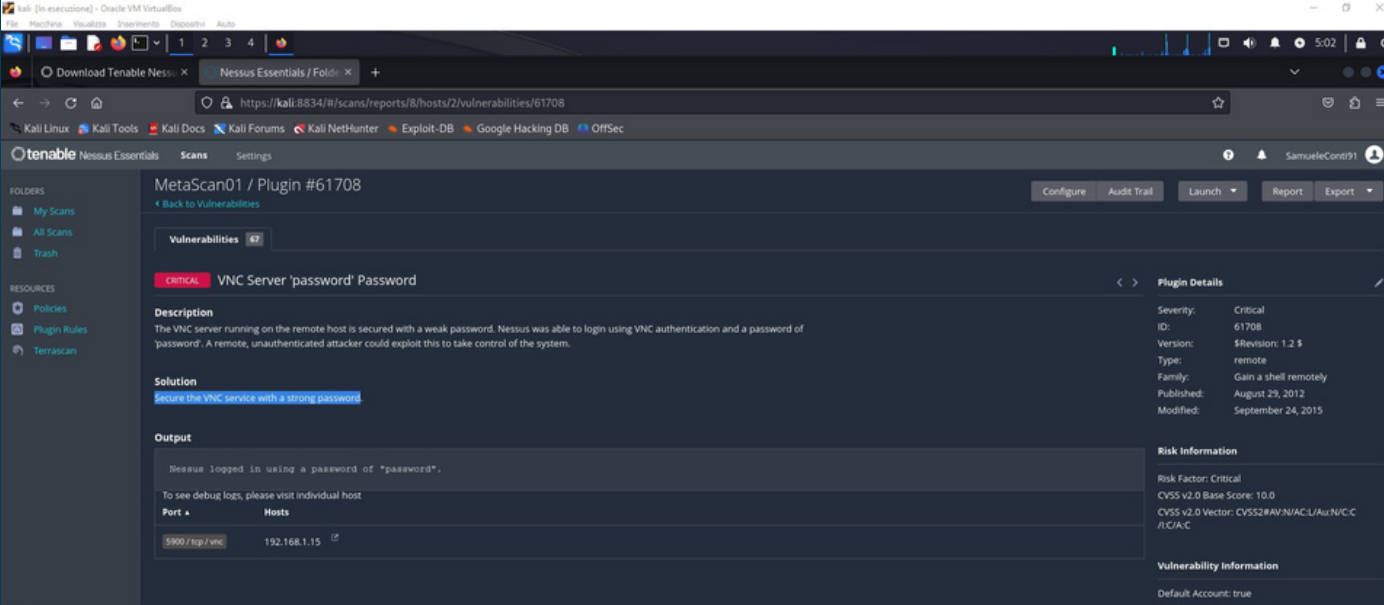
- VNC server 'password' Password
- NFS Exported Share Info Disclosure
- Bind Shell Backdoor detection

VNC SERVER 'PASSWORD'

VNC SERVER sta operando con una password debole

SOLUTION

Nessus ci consiglia di cambiarla e renderla piu forte



The screenshot displays the Nessus Essentials web interface within a Kali Linux virtual machine. The browser address bar shows the URL `https://kali:8834/#/scans/reports/8/hosts/2/vulnerabilities/61708`. The interface is in dark mode and shows a detailed view of a vulnerability identified by MetaScan01 / Plugin #61708.

Vulnerabilities 67

CRITICAL VNC Server 'password' Password

Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution
[Secure the VNC service with a strong password](#)

Output
Nessus logged in using a password of "password".
To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.1.15

Plugin Details

Severity:	Critical
ID:	61708
Version:	\$Revision: 1.2 \$
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

Risk Information

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

Default Account:	true
------------------	------

SOLUTION

Grazie al comando
'vncpasswd' è stato possibile
cambiare password, dopo di
che abbiamo fatto uno scan
di verifica e la vulnerabilità è
stata risolta

The screenshot displays the Tenable Nessus Essentials web interface. The main content area shows the results of a scan for 'Meta02 / 192.168.1.15 / VNC (Multiple Issues)'. A table lists the detected vulnerabilities, all of which are categorized as 'INFO' (Informational).

Sev	CVSS	VPR	Name	Family	Count
INFO			VNC Server Security Type Detection	Service detection	1
INFO			VNC Server Unencrypted Communication Detection	Service detection	1
INFO			VNC Software Detection	Service detection	1

On the right side of the interface, the 'Scan Details' section provides additional context: the policy used is 'Basic Network Scan', the status is 'Running', the severity base is 'CVSS v3.0', the scanner is 'Local Scanner', and the scan started 'Today at 5:58 AM'. Below this, a 'Vulnerabilities' donut chart shows the distribution of findings, with all three being 'Info' level.

NFS EXPOSED SHARE INFO DISCLOSURE

Almeno un NFS esportato su un host remoto puo essere montato da un port scanner. Un attaccante potrebbe far leva su questa vulnerabilità e leggere/scrivere su file da remoto

SOLUTION

Nessus ci consiglia di configurare NFS sul host remoto in modo da autorizzare solo specifici hosts

The screenshot displays the Nessus Essentials web interface in a browser. The URL bar shows a report for a vulnerability on host 192.168.1.15. The interface is divided into several sections:

- Left Sidebar:** Contains navigation links for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan).
- Header:** Shows the user 'SamueleConti' and navigation buttons like 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'.
- Main Content Area:**
 - Vulnerabilities:** A tab showing a list of vulnerabilities, with one highlighted as 'CRITICAL'.
 - Description:** Explains that at least one of the NFS shares exported by the remote server could be mounted by the scanning host, allowing an attacker to read or write files remotely.
 - Solution:** Advises configuring NFS on the remote host to authorize only specific hosts.
 - Output:** Displays a list of NFS shares that could be mounted, including '/usr/bin' and '/usr/sbin'.
 - Plugin Details:** Provides metadata for the vulnerability, including Severity (Critical), ID (11356), Version (1.21), Type (remote), Family (RPC), Published date (March 12, 2003), and Modified date (August 30, 2023).
 - VPR Key Drivers:** Lists factors contributing to the vulnerability's severity, such as Threat Recency, Threat Intensity, and CVSSV3 Impact Score (5.9).
 - Risk Information:** Shows the Vulnerability Priority Rating (VPR) as 5.9.
- Bottom Section:** A table titled 'Hosts' showing the host IP (192.168.1.15) and the port (2049) used for the NFS service.

Solution

Con il comando `nano /etc/exports` andiamo a modificare i permessi in modo che NFS non sara piu possibile essere montata da chiunque

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL `https://kali:8834/#/scans/reports/26/hosts/2/vulnerabilities/42255`. The interface is divided into a left sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash', and a main content area. The main area is titled 'meta03 / Plugin #42255' and shows details for the 'NFS Server Superfluous' vulnerability. The 'Description' states: 'The remote NFS server is not exporting any shares. Running an unused service unnecessarily increases the attack surface of the remote host.' The 'Solution' is 'Disable this service.' The 'Output' section shows 'No output recorded.' and a table with one entry: '2049 /tcp /rpcbind' on host '192.168.1.15'. The 'Plugin Details' section lists: Severity: Info, ID: 42255, Version: 1.4, Type: remote, Family: RPC, Published: October 26, 2009, Modified: October 4, 2019. The 'Risk Information' section shows: Risk Factor: None, CVSS v3.0 Base Score: 0.0, and CVSS v2.0 Base Score: 0.0.

meta03 / Plugin #42255

Back to Vulnerabilities

Vulnerabilities 15

INFO NFS Server Superfluous

Description
The remote NFS server is not exporting any shares. Running an unused service unnecessarily increases the attack surface of the remote host.

Solution
Disable this service.

Output
No output recorded.
To see debug logs, please visit individual host

Port	Hosts
2049 /tcp /rpcbind	192.168.1.15

Plugin Details

Severity: Info
ID: 42255
Version: 1.4
Type: remote
Family: RPC
Published: October 26, 2009
Modified: October 4, 2019

Risk Information

Risk Factor: None
CVSS v3.0 Base Score: 0.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
CVSS v2.0 Base Score: 0.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:N

Bind Shell Backdoor Detection

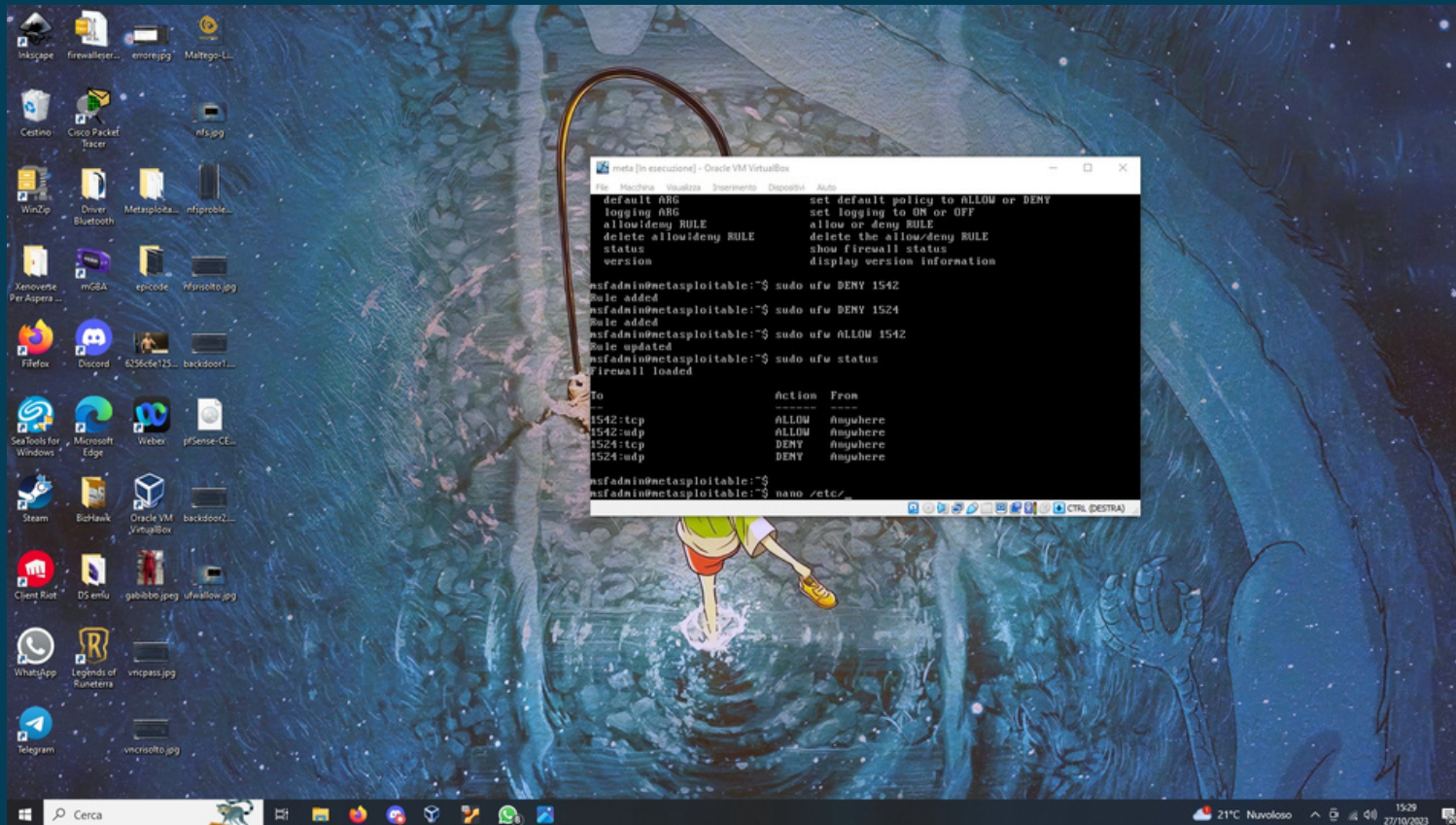
Questa vulnerabilità si tratta di una shell in ascolto sulla porta 1524 senza nessuna autenticazione richiesta

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL: `https://kali:8834/#/scans/reports/26/hosts/2/vulnerabilities/51988`. The interface is in dark mode. On the left sidebar, under 'FOLDERS', 'My Scans' is selected. Under 'RESOURCES', 'Policies', 'Plugin Rules', and 'TerraScan' are listed. The main content area is titled 'meta03 / Plugin #51988'. Below this, there's a 'Vulnerabilities' section with a 'CRITICAL' badge and the title 'Bind Shell Backdoor Detection'. The 'Description' states: 'A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.' The 'Solution' suggests: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The 'Output' section shows a command prompt where 'id' was executed, resulting in root access. On the right, the 'Plugin Details' section lists: Severity: Critical, ID: 51988, Version: 1.10, Type: remote, Family: Backdoors, Published: February 15, 2011, Modified: April 11, 2022. Below this, the 'Risk Information' section shows a 'Risk Factor: Critical' and a 'CVSS v3.0 Base Score 9.8'. At the bottom, a table lists the port and host for the vulnerability.

Port	Hosts
1524 / tcp / wild_shell	192.168.1.15

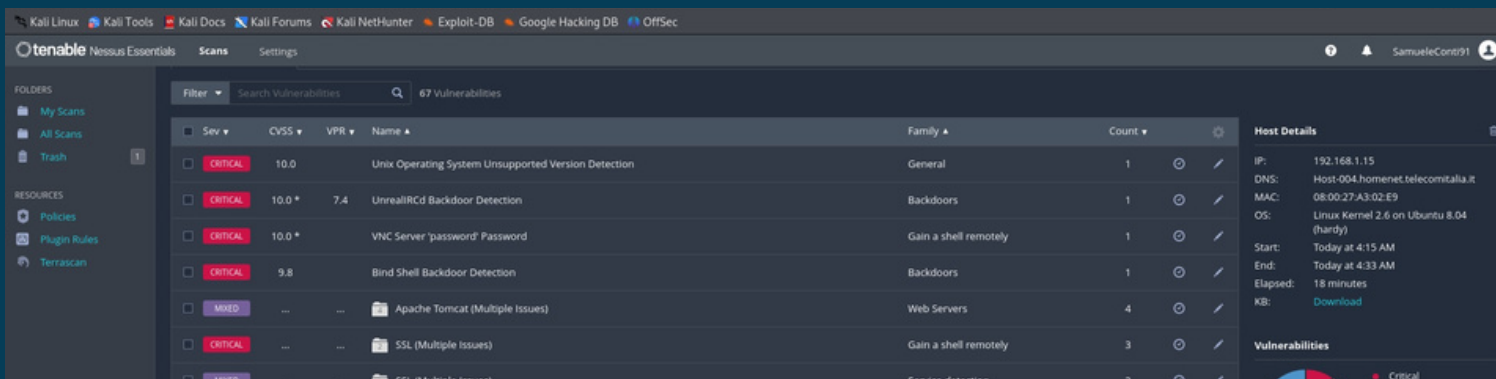
Solution

Con il comando `sudo ufw DENY 1524` andremo a bloccare il traffico su quella porta in modo che la Backdoor non possa rimanere in ascolto



Confronti

Primo Scan num Vulnerabilità: 67



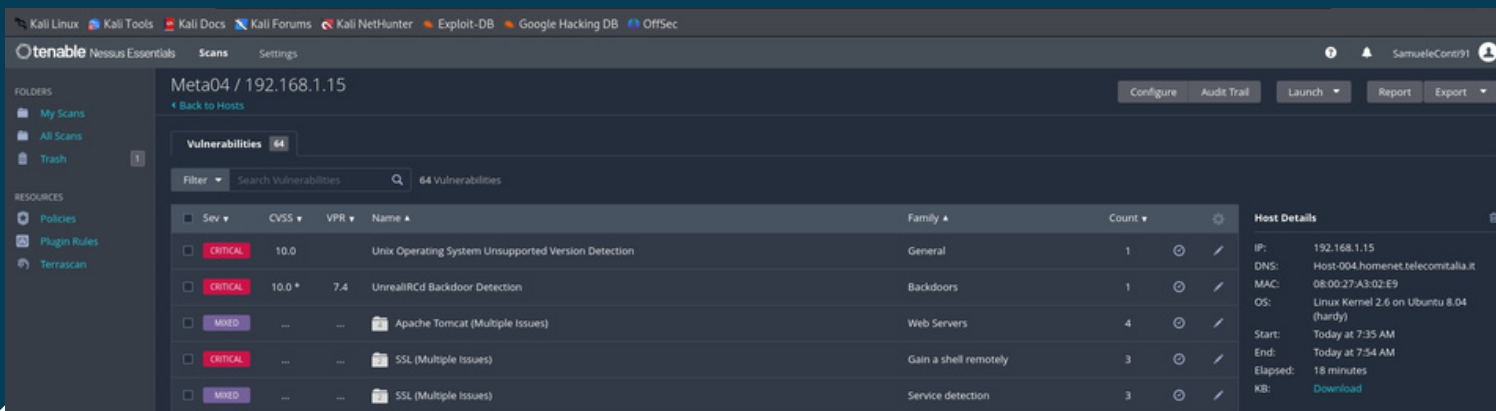
The screenshot shows the Tenable Nessus interface. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main header displays the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. The user 'SamueleConti91' is logged in. On the left, a sidebar lists 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area shows a table of vulnerabilities for a specific scan. The table has columns for Severity, CVSS, VPR, Name, Family, and Count. The first five vulnerabilities are listed: 'Unix Operating System Unsupported Version Detection' (Critical, 10.0), 'UnrealIRCd Backdoor Detection' (Critical, 10.0), 'VNC Server 'password' Password' (Critical, 10.0), 'Bind Shell Backdoor Detection' (Critical, 9.8), and 'Apache Tomcat (Multiple Issues)' (Mixed). To the right, the 'Host Details' panel shows information for IP 192.168.1.15, including DNS, MAC, OS, and scan timing.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *		VNC Server 'password' Password	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

Host Details

IP: 192.168.1.15
DNS: Host-004.homenet.telecomitalia.it
MAC: 08:00:27:A3:02:E9
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 4:15 AM
End: Today at 4:33 AM
Elapsed: 18 minutes
KB: [Download](#)

Ultimo Scan num Vulnerabilità: 64



The screenshot shows the Tenable Nessus interface for the latest scan. The top navigation bar is the same. The main header shows 'Meta04 / 192.168.1.15' with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. The left sidebar is identical. The main content area shows a table of vulnerabilities. The first five vulnerabilities are: 'Unix Operating System Unsupported Version Detection' (Critical, 10.0), 'UnrealIRCd Backdoor Detection' (Critical, 10.0), 'Apache Tomcat (Multiple Issues)' (Mixed), 'SSL (Multiple Issues)' (Critical), and 'SSL (Multiple Issues)' (Mixed). The 'Host Details' panel on the right shows the same IP and some updated scan timing information.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	7.4	UnrealIRCd 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

Host Details

IP: 192.168.1.15
DNS: Host-004.homenet.telecomitalia.it
MAC: 08:00:27:A3:02:E9
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 7:35 AM
End: Today at 7:54 AM
Elapsed: 18 minutes
KB: [Download](#)