

NETWORK SECURITY

P1705837 – John-Paul Milne

M7X01701

Dr Carlene Campbell

Abstract

Penetration testing is the analysis and testing of a computer system using tools that are available to attackers. Common attack methods were researched, with the OWASP Top10 used as a reference guide. Penetration testing was carried out on the website of Citizens United for Peace and Stability (CUPS) – cupstv.com

Tools used were Kali Linux, Nmap and Zenmap, Nikto, OWASP ZAP, DirBuster, WPScan, Discover, Metasploit Framework and Nessus. Testing methodology was documented with results and findings recorded.

Keywords - Penetration Testing, Vulnerabilities, Cyber-attack, OWASP Top10, CUPS, CUPSTV.COM, OWASP, Kali Linux, Nmap, Zenmap, Nikto, OWASP ZAP, DirBuster, WPScan, Discover, Metasploit Framework, Nessus, VPN, GoDaddy, WordPress

Table of Contents

1.	Table of Figures	4
2.	Introduction.....	6
3.	Related Work and Research.....	6
3.1	OWASP Top 10	6
3.2	Penetration Testing Methodology	9
3.3	Tools available for penetration testing.....	10
4.	Design and Implementation	12
4.1	Use of Kali	14
4.2	Use of Nmap to scan host	14
4.3	Use of Nikto to scan host	18
4.4	Use of OWASP ZAP to scan host.....	20
4.5	Use of DirBuster to scan host	21
4.6	Use of WPScan to scan host	25
4.7	Use of Discover to scan host.....	29
4.8	Use of Metasploit to scan host	31
4.9	Use of Nessus to scan host.....	31
5.	Analysis of Results and Findings.....	32
6.	Conclusion	36
7.	References and Bibliography	37
8.	Appendices.....	40

1. Table of Figures

Figure 1 Evolution of OWASP Top 10 from 2013- 2017[4]	9
Figure 2 Testing Approach[14].....	9
Figure 3 Identification of Target and Analysis of Scan Results	10
Figure 4 Attack/Test of Identified Vulnerabilities	10
Figure 5 Letter of Authority to perform penetration testing	13
Figure 6 Tests carried out directly from attacker's/penetration tester's network	13
Figure 7 Tests carried out using a VPN provider to hide identity of attacker/penetration tester	13
Figure 8 Comparison of IP address visibility without a VPN (left) and with a VPN (right)	14
Figure 9 Using Kali Terminal commands to update from Kali online repositories	14
Figure 10 Zenmap GUI for initiating an Nmap scan on a host	15
Figure 11 Host and port scan information results from Nmap	15
Figure 12 Host status and information results from Nmap	17
Figure 13 Host topology map from Nmap	17
Figure 14 Holding page at http://160.153.128.24	18
Figure 15 cPanel login page.....	18
Figure 16 Nikto HTML report showing failed test	19
Figure 17 Nikto CLI output showing failed test	19
Figure 18 Nikto CLI output showing successful scan of host	20
Figure 19 OWASP ZAP GUI for initiating a scan on a host	20
Figure 20 OWASP ZAP results summary	21
Figure 21 Use of DirBuster to scan host	21
Figure 22 Wordlist dictionaries provided by DirBuster.....	22
Figure 23 DirBuster GUI	22
Figure 24 DirBuster scan in progress.....	22
Figure 25 Login page at http://cupstv.com/login-page/	23
Figure 26 Login page at http://cupstv.com/kilishi-maidadi/	23
Figure 27 Lost your password page at http://cupstv.com/kilishi-maidadi/?action=lostpassword	24
Figure 28 Error when attempting recovery of password.....	24
Figure 29 Updating WPScan database.....	25
Figure 30 Initiating a WPScan on the target website.....	25
Figure 31 WPScan results showing contents of robots.txt.....	26
Figure 32 WPScan was not able to detect the version number of WordPress	26
Figure 33 Error Log with references to local path on web application server	27
Figure 34 Message that seems to confirm the existence of cupstvmanager769 username	27

Figure 35 Example CSRF attack code	28
Figure 36 WPScan results showing plugin details and failure to enumerate usernames	28
Figure 37 Changelog of wunderground readme file shows 2.1.3	29
Figure 38 Example code to be inserted into functions.php file to prevent user enumeration	29
Figure 39 DNS Map output from Discover	30
Figure 40 Nessus Summary of vulnerabilities – note 0 Critical/High found	31
Figure 41 GoDaddy Managed WordPress Plans.....	34
Figure 42 Features included in all GoDaddy WordPress hosting plans.....	34
Figure 43 Key features of GoDaddy WordPress hosting.....	35
Figure 44 GoDaddy security features	35

2. Introduction

Tecomex Forensics is a Digital Forensics and Network Security company based in Swansea, UK who have been approached by Citizens United for Peace and Stability (CUPS) to assist in ensuring that the CUPS website (<http://cupstv.com>) is secure against external threats.

CUPS is a not-for profit, non-governmental organisation (Company Registration Number 9857221) based in the UK. CUPS is an organisation that is highly involved in the protection and promotion of human rights in Nigeria and has about 100,000 followers around the globe[1]. Boko Haram is a Nigerian based Islamist militant sect that has links to terrorist activities in the region. Muhammadu Buhari, Nigeria's president and former army general, has publicly declared his government's intention to eradicate Boko Haram and other Islamist insurgent groups. The conflict between Boko Haram and the Nigerian military forces have resulted in many human rights violations on both sides. CUPS consider themselves an organisation that promotes the unity, peace, and security of all Nigerians at home and around the globe[1].

3. Related Work and Research

Farmer and Venema introduced the concept of penetration testing in 1995 when they developed Security Administrator Tool for Analyzing Networks (SATAN)[2]. Their suggestion was to analyse computer systems from the perspective of a potential attacker. This was a highly controversial proposal in the beginning, but penetration testing has now become an established procedure in information security. A penetration tester's primary goal is to imitate the attackers that might be targeting a service that a company is using or providing[3].

3.1 OWASP Top 10

The Open Web Application Security Project (OWASP) is an open source community aimed at helping companies develop, purchase and maintain applications that can be trusted. There is an OWASP project called the OWASP Top 10. The initial aim of this project was to simply raise awareness amongst developers, but it has now become the de facto application security standard[4]. The OWASP Top 10 2017 is the latest release in an ongoing project that has been regularly updated since it was first published in 2003.

The OWASP Top 10 2017 comprises of the following methods of attack/vulnerabilities:

A1:2017-Injection

An injection attack is a group of attacks that consist of injecting code to be executed by an application. The application can be tricked into executing unintended commands or accessing unauthorised data. A famous example of this was when Sony Pictures was attacked in 2011. A hacktivist group called 'LulzSec' claimed they used a simple SQL injection attack to access customer data including names, addresses, passwords and financial information[5].

A2:2017-Broken Authentication

Incorrect implementation of control measures for application authentication can be exploited to compromise the application and access unauthorised data. A simple example is user access to a website or service. Mechanisms should be implemented to ensure session timeouts. After a certain period of inactivity, the user should be automatically logged out and prompted to login again if they wish to continue[6].

A3:2017-Sensitive Data Exposure

Sensitive data should not be accessible to external sources. This can include passwords, credit card numbers, personal information etc. Data should be stored in an encrypted format using up-to-date and strong algorithms. The previously mentioned Sony Pictures attack in 2011 was another good example of this. The customer information was stored in plain text, so once the attackers had access, it was a simple process to access the password information for those customers. Because people are prone to password re-use, these stolen credentials could then be used for attacks on other companies/services[5].

A4:2017-XML External Entities

When an application parses XML input, it can be attacked by providing an input that references an external entity. This exploit can be used to access unauthorised data or access devices that the attacker would otherwise not have access to. It can also be used as a Denial of Service (DoS) attack. A famous example is the ‘Billion Laughs’ or ‘XML Bomb’ attack. The most basic example is where an XML file is created with ten entities. The first entry can be defined as the string ‘lol’. Each subsequent entity is defined to be 10 of the previous entity. The target application is passed a reference to only the last entity, however, upon parsing the identity, it expands each individual identity and this results in a massive flood of data to the application which can cause exponential use of resources and system crash[7].

A5:2017-Broken Access Control

Access Control is the enforcement of policy to grant/deny access to resources for users. Incorrect implementation can lead to an imposter accessing unauthorised resources. An example of this is a known attack on Twitter accounts. A company can use Twitter and pay for advertising services. A user can intercept a request to delete his own credit card details. By changing the ID of the credit card – a competitor’s card can be deleted. This would then give the attacker a competitive advantage by preventing the competitor from paying for advertising services using Twitter[8].

A6:2017-Security Misconfiguration

An application can be vulnerable to attack if not configured correctly. This can occur at multiple levels within the application. Examples include using default accounts/passwords and installation of unnecessary features. The Mirai Botnet attack in 2016 is an example of this. Factory default credentials are used to gain access to misconfigured consumer IoT devices. These devices can be used to co-ordinate large scale Distributed Denial of Services (DDoS) attacks[9].

A7:2017-Cross-Site Scripting (XSS)

An attacker can exploit a vulnerability in a website and use that website to deliver malicious code to the web browser of the user that visits the attacked website. It is the user of the website that is the actual target of the attacker. A famous example is the Samy XSS worm that affected one million MySpace users in just twenty hours back in 2005[10]. Another example is the UK Parliament website. In 2014 they had to address a XSS flaw that allowed for an attacker to add or amend content on the site[11]. Because it is an official government resource, users assume a significant level of trust and any breach of security can have huge implications.

A8:2017-Insecure Deserialization

Serialization is the process of converting data into a storable format for restoration at a later point in time. An application could be attacked by accessing and amending this stored data to grant unauthorised application privileges to the attacker.

A9:2017-Using Components with Known Vulnerabilities

Software providers should constantly develop and update their applications. These updates can provide additional features, but should also address any security flaws. Application administrators should ensure that policies are in place to keep applications patched and updated at regular intervals. There are any number of reasons why applications and devices are not kept up to date. Increased workload, legacy application compatibility issues, lack of financial resources can all lead to the absence of appropriate patching and system updates. This inevitably results in increased risk due to the existence of vulnerabilities that should be removed.

A10:2017-Insufficient Logging & Monitoring

Logging and monitoring systems should be in place. Historical records of logins, failed logins, errors etc. should be stored and easily accessible to application administrators to alert them about any unexpected events. Advanced Persistent Threats (APT) describes the skilled, targeted and orchestrated attack methods that modern cyber criminals can use to attack a target. They can involve multi-stage attacks that take place over a long period of time[12][13]. Threat protection measures should be in place that not only aim to protect a network, but also log network activity so repeated attack attempts can be flagged and if necessary, information regarding a security breach can be escalated to the relevant authorities.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	→	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	→	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	→	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Figure 1 Evolution of OWASP Top 10 from 2013- 2017[4]

As illustrated in Fig. 1, there have been changes to the list of vulnerabilities but six of the ten issues have remained the same in 2017.

3.2 Penetration Testing Methodology

There is an industry wide accepted methodology when it comes to performing a penetration test. The process can be broken down into four high-level steps[14].

- **Identify:** Identification of the target using scanning tools to determine application platform and any potential vulnerabilities.
- **Analyse:** Cross-reference findings against known vulnerability lists and ascertain relevant Vulnerability Assessment Tools (VAT)
- **Test:** Use selected VAT to perform tests against the target
- **Report:** Document findings and results.

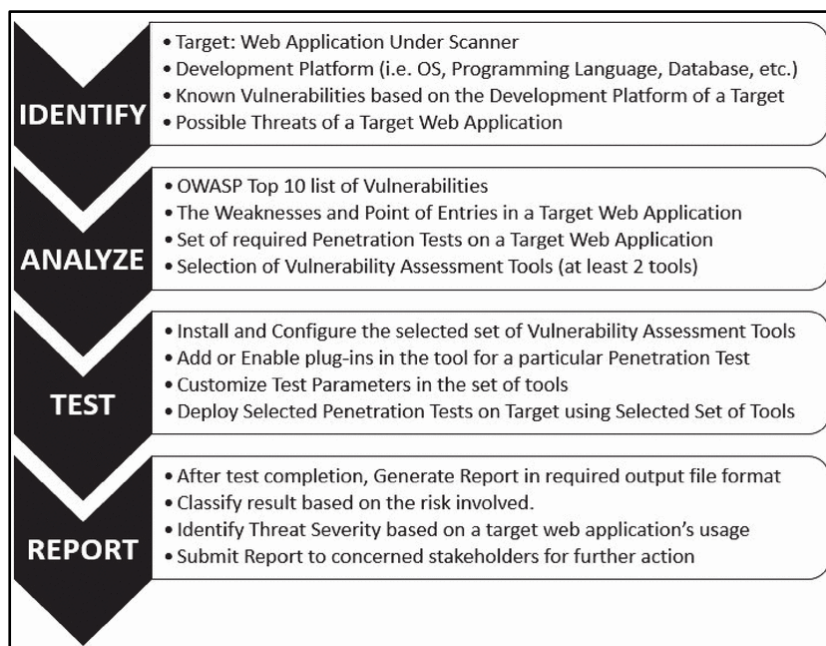


Figure 2 Testing Approach[14]

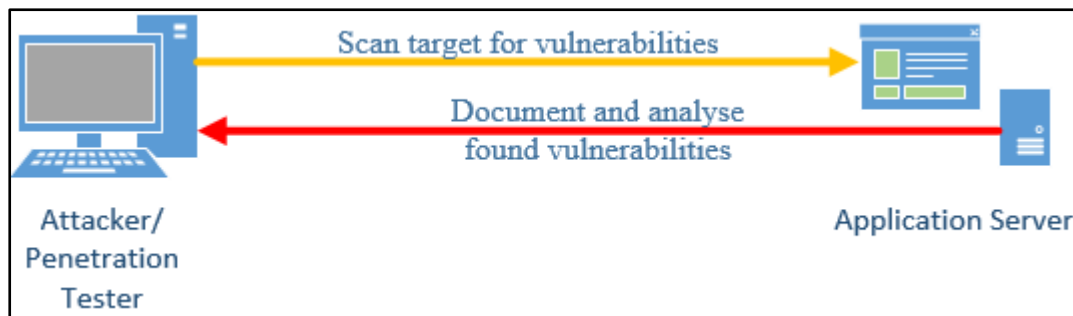


Figure 3 Identification of Target and Analysis of Scan Results

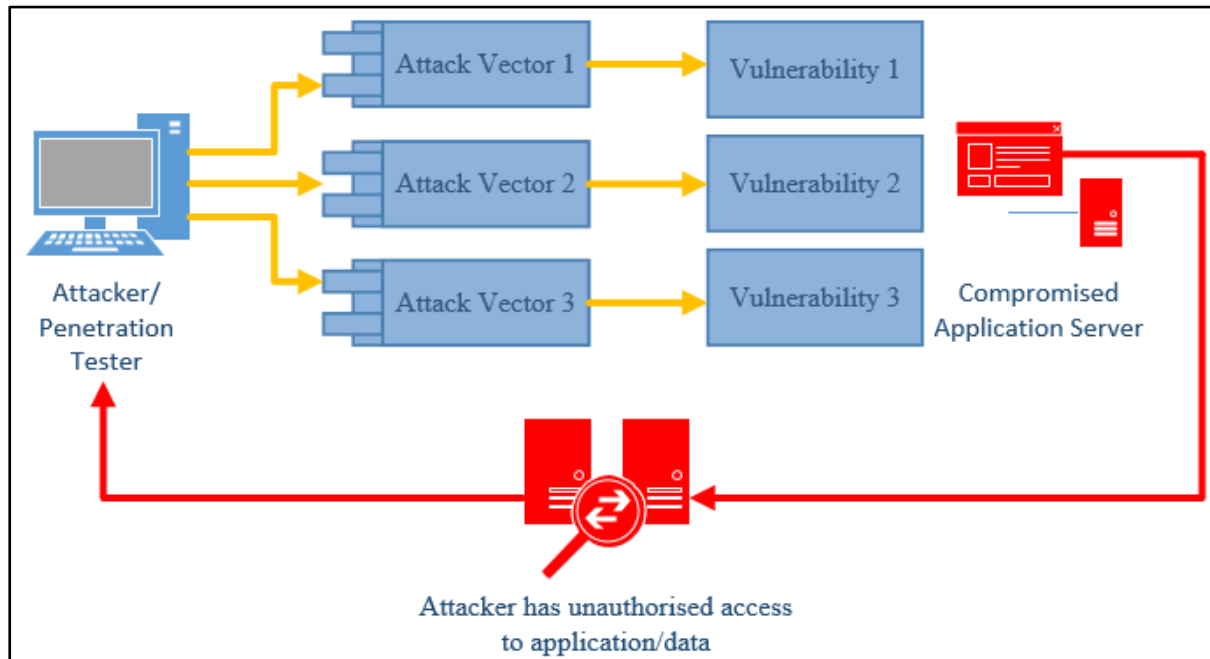


Figure 4 Attack/Test of Identified Vulnerabilities

3.3 Tools available for penetration testing

There are a wide and varied array of testing tools available to the penetration testing community. The following tools have been selected for scanning and testing the CUPS website.

Kali

Kali Linux is an Open Source project that is maintained and funded by Offensive Security. It is a Linux based operating system that gathers more than 300 penetration test tools[15][16].

Nmap/Zenmap

Nmap is an Open Source utility for network mapping and security auditing. It can be used for service discovery when scanning a target host[17][16]. Zenmap is the official GUI interface to the CLI based Nmap application. The latest version is 7.60.

Nikto

Nikto is Open Source software that can be used to scan web servers. It checks for multiple potentially high-risk files/programs and can cross-reference application version numbers with lists of known vulnerabilities[18][14]. The latest version for Kali is 2.1.6. The latest version for Windows10 is 2.1.5.

OWASP ZAP

The OWASP Zed Attack Proxy (ZAP) is another popular security tools that is free. It can automatically find application vulnerabilities. It is a project that is actively maintained by hundreds of volunteers from around the world[19][3]. The latest version is 2.7.0

DirBuster

DirBuster is a utility that can be used to crawl directories and file names on a web server. Hidden folders and pages that are not visible through the HTML web interface can be found. These folders can potentially contain data that can be useful to attackers. A dictionary file is used along with a brute force method of checking for the existence of files/folders. The latest version is 1.0-RC1.

WPScan

WPScan is a Kali Linux scanner that is specifically designed to target vulnerabilities in the WordPress content management system[20]. WordPress is an extremely common Content Management System (CMS) that some resources claim is used on more than 50% of websites that use a CMS[21]. It can find vulnerable themes and plugins that could potentially leave a WordPress site vulnerable to attack. The latest version is 2.9.3.

Discover

Discover is a collection of scripts for Kali applications that was written by Lee Baird[22]. It can automate many tasks to speed up passive reconnaissance on a target and output the information gathered into a complete HTML report.

Metasploit Framework

Metasploit is a collaboration between the open-source community and Rapid7 – a commercial IT security services company. They have joined forces to provide a collection of security testing tools with various plugins, modules and libraries[23]. The latest version is 4.16.21-0kali1.

Nessus

Nessus is a commercial vulnerability scanning platform by Tenable. Tenable allow personal users in a non-enterprise environment to use the software for free. It has a number of pre-configured policies and over 80,000 user configurable plugins that can cross-reference against a huge list of known vulnerabilities. Nessus uses the Common Vulnerability Scoring System (CVSS) to group each of these vulnerabilities into different risk categories ('Critical', 'High', 'Medium', 'Low', 'None')[24]. The latest version is 6.11.3.

4. Design and Implementation

Tecomex-Forensics provided a full scope of works for the web application penetration test. See **Appendix A – Scope of Work**

The following work is included within this project:

- Application scan of <http://cupstv.com> and any associated IP addresses.
- Cross-reference against lists of known applications and known vulnerabilities.
- Attempt brute-force password attacks against any externally exposed applications.
- Provide written documentation to include outcomes of above tests.
- Provide description of recommended measures that could be implemented to reduce risk exposure.

The following tests are NOT included in the scope of this project but can be included in follow-up tests at a later stage.

- Onsite data centre network penetration tests
- Onsite data centre physical penetration tests
- Employee Social Engineering penetration tests
- Cross Site Scripting penetration test
- Code Injection penetration test
- Stress testing/availability test

Tecomex-Forensics policy dictates that when conducting penetration testing on behalf of a customer the relevant documentation needs to be in place granting permission to perform said penetration testing. See **Appendix B – SLA[25]**

During the test period it was understood:

- If the customer discovers any service disruption they should contact Tecomex-Forensics immediately. Tecomex-Forensics will then confirm if the outage was brought about by testing activity. If testing is currently underway, testing will immediately cease and Tecomex-Forensics will begin work to rectify the problem and resume normal service.
- If Tecomex-Forensics perform any actions that result in service disruption to the customer applications, they will immediately cease testing, notify the customer and begin working to rectify the problem and resume normal service.

In addition to the signed Service Level Agreement, Tecomex-Forensics ensured that a full letter of authority was in place before testing commenced.

Letter of Authority to perform penetration testing on a live website

I am writing you regarding the above subject matter. As part of our commitment to support both the lecturers and students of University of Wales Trinity St David, I hereby give your students the express permission to perform penetration testing on a live website, which is owned and created by Tecomex Forensics Ltd.

It is our wish that your students who are taught information security courses are able to peacefully and lawfully practice what they learned in lectures and tutorials without the fear of being prosecuted for breaking the law on hacking, which carries mandatory jail sentence without the option of fine.

The website your students are allowed to conduct penetration testing on is: <http://tecomex-forensics.com> and/or <http://cupstv.com> websites. It is our hope that you will share the outcome of your student's finding with us in electronic format.

Best regards,

Dr. Idris Ahmed.

CEO Tecomex Forensics Ltd.

Figure 5 Letter of Authority to perform penetration testing

Tecomex-Forensics policy dictates that when conducting penetration testing, equipment used to carry out the tests will be behind an internet connection that anonymises traffic. The IP address of the Attacker/Penetration Tester will not be visible to the Internet Service Provider (ISP) or the target. See **Appendix C – VPN Policy**

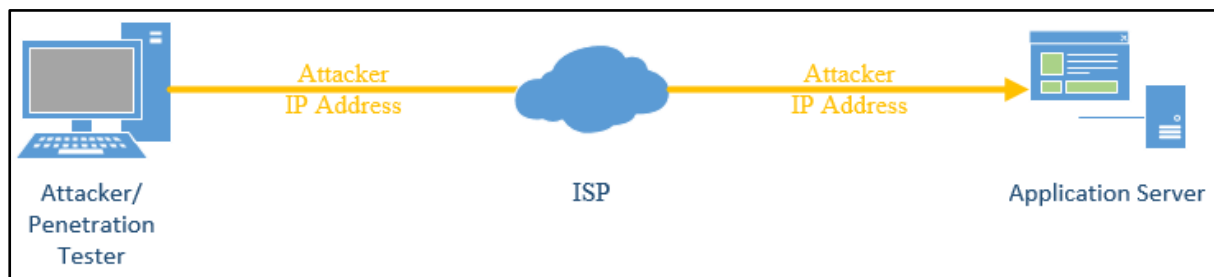


Figure 6 Tests carried out directly from attacker's/penetration tester's network

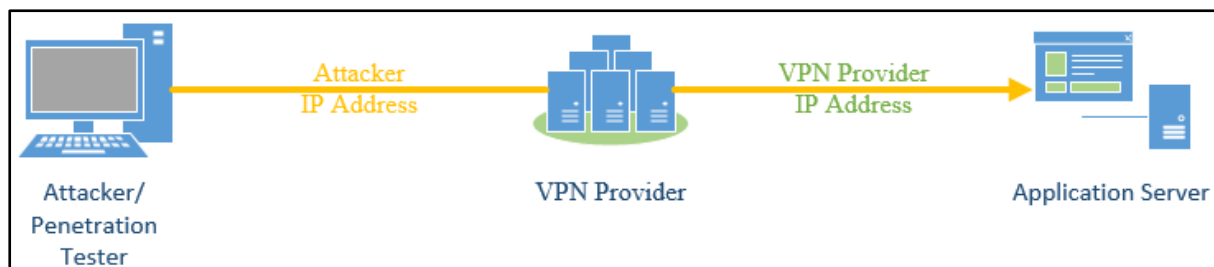


Figure 7 Tests carried out using a VPN provider to hide identity of attacker/penetration tester

For this test, it was decided to use NordVPN as the VPN provider. NordVPN have more than 2000 servers worldwide, promise fast and reliable service and have a strict no-logs policy[26].

Your Information		Your Information	
IP Address:	86.175.101.160 IPv4 ← Blacklisted ?	IP Address:	109.169.94.21 IPv4 ← Blacklisted ?
Hostname:	host86-175-101-160.range86-175.btcentralplus.c...	Hostname:	109.169.94.21
ISP:	BT Public Internet Service	ISP:	Iomart Hosting Ltd
Location:	Birmingham, England GB	Location:	Maidenhead, England GB
Coords:	Lat 52.4862 , Lon -1.8904	Coords:	Lat 51.5288 , Lon -0.725042
Local:	07:21 pm - Europe/London	Local:	07:29 pm - Europe/London
Browser:	Firefox on Linux ← Browser Info	Browser:	Firefox on Linux ← Browser Info
Language:	English (United States)	Language:	English (United States)
Referred:	https://www.google.co.uk/	Referred:	https://www.google.co.uk/

Figure 8 Comparison of IP address visibility without a VPN (left) and with a VPN (right)

4.1 Use of Kali

Kali Linux 2017.2 was already installed on a testing laptop. To ensure that Kali uses the latest packages and applications, the following commands can be run from a terminal session:

```
apt-get update
```

```
apt-get upgrade
```

This will communicate with the predetermined Kali web servers for updates. If there are any available updates, it will prompt to install them.

```
root@mil23-lt-k:~# apt-get update
Hit:1 http://ftp.hands.com/kali kali-rolling InRelease
Hit:2 https://packages.microsoft.com/ubuntu/14.04/prod trusty InRelease
Reading package lists... Done
root@mil23-lt-k:~# apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@mil23-lt-k:~#
```

Figure 9 Using Kali Terminal commands to update from Kali online repositories

4.2 Use of Nmap to scan host

The Zenmap GUI can be used to adjust the parameters for a scan. The following scan parameters were used:

```
nmap -T4 -A -v cupstv.com
```

nmap -h can be used to list the summary of options available.

- -T4 Timing Template 0-5 (higher is faster)
- -A Enable OS detection, version detection, script scanning and traceroute
- -v Increase verbosity level
- Intense Intense scan scans the 1000 most common TCP ports.
This is more in-depth than a quick scan that only scans the top 100 most common ports

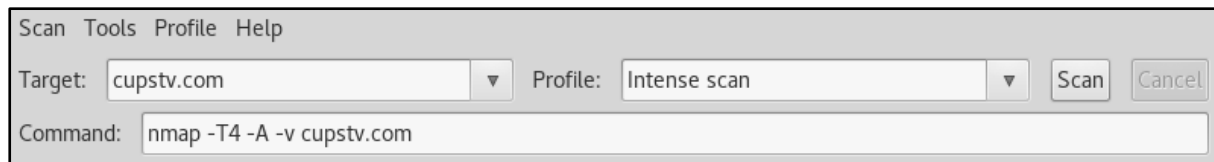


Figure 10 Zenmap GUI for initiating an Nmap scan on a host

The results of the completed Nmap scan show the following details:

- IP address associated with cupsttv.com
- Open ports on the host
- Host status and information
- Topology layout of the path network traffic must take to travel from tester to target

See **Appendix D – Nmap Report** for full Nmap scan report details

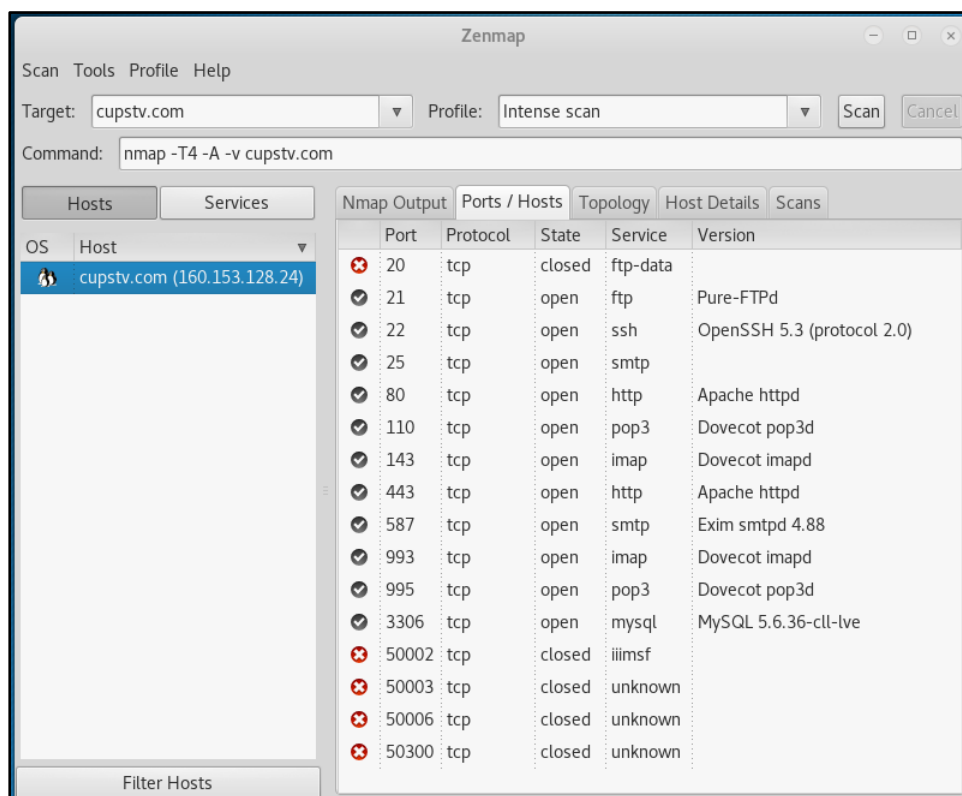


Figure 11 Host and port scan information results from Nmap

The following ports were identified as being open:

- Port 21 FTP
File Transfer Protocol (FTP) is a method of transferring files between computers. Usual implementation is using the server and client model.
- Port 22 SSH
Secure Shell (SSH) is a method of establishing remote login from one computer to another using encryption to protect communication security and integrity.
- Port 25 SMTP
Simple Mail Transfer Protocol (SMTP) is an internet standard for e-mail servers to communicate. Port 25 can also be used for remote clients to send messages to a server for message relaying.
- Port 80 HTTP
Hyper Text Transfer Protocol (HTTP) uses port 80 as the standard port for web servers. Web browsers attempt to connect to a web server using port 80 as the default.
- Port 110 POP3
Post Office Protocol (POP3) is a mail delivery protocol. It is used for clients to retrieve e-mail from an e-mail server. E-mails are retrieved from the server and stored on the client.
- Port 143 IMAP
Internet Messaging Access Protocol (IMAP) is an updated version of POP3. It is used for clients to retrieve e-mail from an e-mail server. E-mails are stored on the server and the client downloads copies of the e-mail.
- Port 443 HTTPS
HTTP over Transport Layer Security/Secure Socket Layer (TLS/SSL) is used for HTTP traffic but data is transmitted using a secured encrypted communications channel.
- Port 587 SMTP
Port 587 is used for SMTP, specifically for clients to send e-mail to servers (as opposed to port 25 which is for server to server communication or SMTP relay)
- Port 993 IMAPS
IMAP over TLS/SSL uses port 993. It is used for clients to retrieve email from servers via IMAP using a secure encrypted communications channel.
- Port 995 POP3S
POP3 over TLS/SSL uses port 995. It is used for clients to retrieve email from servers via POP3 using a secure encrypted communications channel.
- Port 3306 MySQL
MySQL is an open source database application. It uses port 3306 by default for remote access.

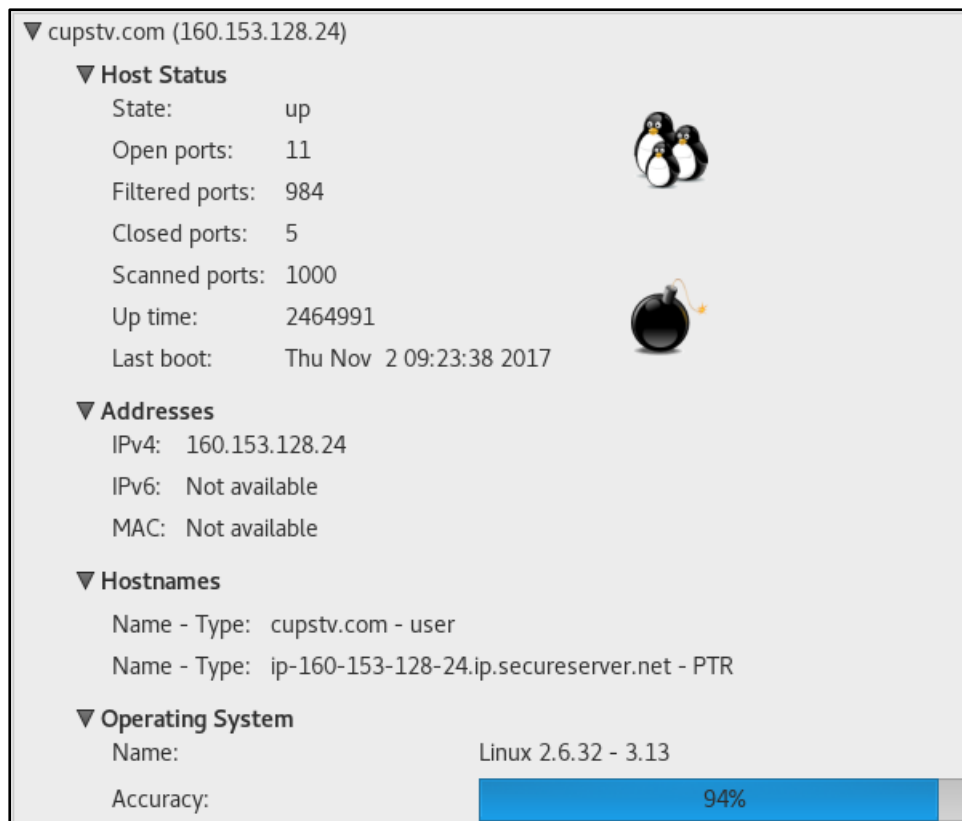


Figure 12 Host status and information results from Nmap

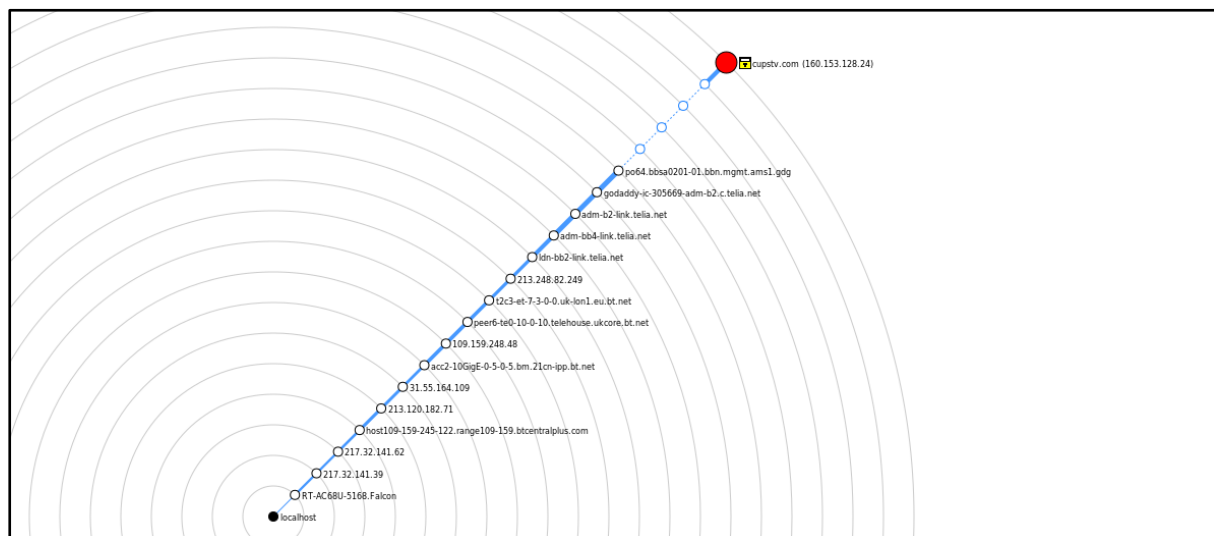


Figure 13 Host topology map from Nmap

The results of the Nmap scan show an IP address of 160.153.128.24. When that IP address is entered into a web browser a holding page is displayed.

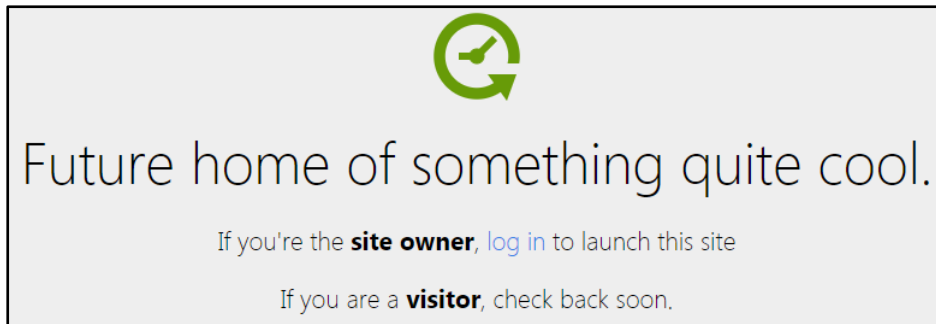


Figure 14 Holding page at <http://160.153.128.24>

There is a link on that holding page for the site owner. The link points to the following URL:

<http://160.153.128.24/cpanel>

This redirects to the following URL:

<https://n3plcpnl0001.prod.ams3.secureserver.net:2083/>

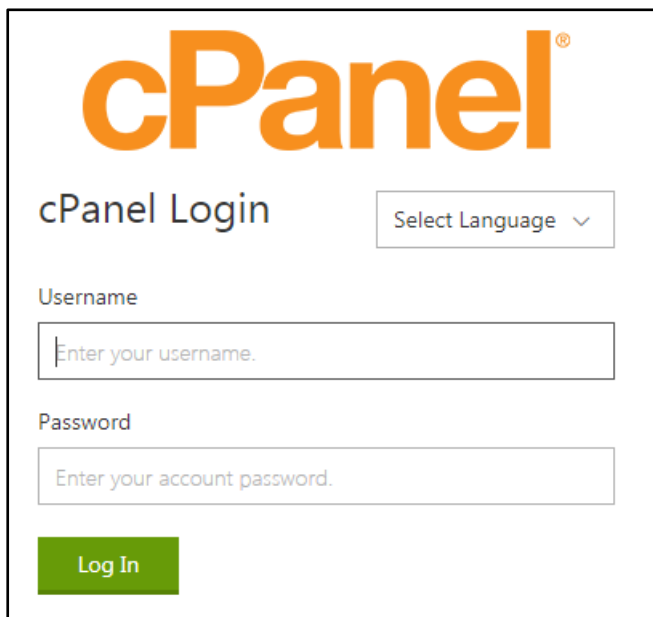


Figure 15 cPanel login page

cPanel is a commercial web-based control panel that allows site owners to use graphical tools to simplify the process of Linux-based site administration.

4.3 Use of Nikto to scan host

Nikto is a command line utility. The following scan parameters were used:

`nikto -host http://cupstv.com -Display V -Format htm -output NiktoReport.html`

nikto -H can be used to list the summary of options available.

- -host Target host
- -Display V Turn on verbose display output
- -Format htm Save output file in HTML format
- -output Write output to this file

This unexpectedly failed to return any results. Initially, it was suspected that a corrupted installation of Nikto on Kali was the source of the problem. Nikto was then installed on a Windows10 test machine. The output results from this test were the same.

Scan Summary	
Software Details	Nikto 2.1.5
CLI Options	-host cupstv.com -Display V -Format htm -output NiktoReport.html
Hosts Tested	0
Start Time	Thu Dec 7 15:48:37 2017
End Time	Thu Dec 7 15:51:21 2017
Elapsed Time	164 seconds
© 2008 CIRT, Inc.	

Figure 16 Nikto HTML report showing failed test

```
V:Thu Dec 7 15:48:37 2017 - Target:cupstv.com port:80
V:Thu Dec 7 15:48:37 2017 - Checking for HTTP on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:48:57 2017 - for HEAD: /
V:Thu Dec 7 15:48:57 2017 - Checking for HTTPS on port cupstv.com:80, using HEAD
V:Thu Dec 7 15:50:00 2017 - for HEAD: /
V:Thu Dec 7 15:50:00 2017 - Checking for HTTP on port cupstv.com:80, using GET
V:Thu Dec 7 15:50:20 2017 - for GET: /
V:Thu Dec 7 15:50:20 2017 - Checking for HTTPS on port cupstv.com:80, using GET
V:Thu Dec 7 15:51:21 2017 - for GET: /
+ No web server found on cupstv.com:80

-----
V:Thu Dec 7 15:51:21 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 15:51:21 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 15:51:21 2017 - 6544 server checks loaded
V:Thu Dec 7 15:51:21 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 15:51:21 2017 - Running start for "Content Search" plugin
+ 0 host(s) tested
V:Thu Dec 7 15:51:21 2017 + 8 requests made in 164 seconds
```

Figure 17 Nikto CLI output showing failed test

Nikto was then tested against an internal web server that belonged to the tester and Nikto worked as expected. A similar test was run against an external web server for test purposes only – <http://pentest-tools.com>. Again, this worked as expected. There seems to be measures in place that block Nikto from performing a scan. This is a well-known protection measure to prevent attackers from gathering information about a site.

```

V:Thu Dec 7 16:02:41 2017 - Checking for HTTP on port pentest-tools.com:80, using HEAD
V:Thu Dec 7 16:02:41 2017 - 302 for HEAD: /
V:Thu Dec 7 16:02:41 2017 - Opening reports (htm, NiktoReport.html)
V:Thu Dec 7 16:02:41 2017 - Opening report for "Report as HTML" plugin
V:Thu Dec 7 16:02:41 2017 - 6544 server checks loaded
V:Thu Dec 7 16:02:41 2017 - Running start for "Embedded Detection" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Favicon" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "HTTP Headers" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Guess authentication" plugin
V:Thu Dec 7 16:02:41 2017 - Running start for "Content Search" plugin
V:Thu Dec 7 16:02:41 2017 - 302 for GET: /
+ Target IP: 212.71.238.108
+ Target Hostname: pentest-tools.com
+ Target Port: 80
+ Start Time: 2017-12-07 16:02:41 (GMT0)
-----
+ Server: pentest-tools.com
V:Thu Dec 7 16:02:41 2017 - 302 for GET: /
+ Cookie PTSESSIONID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: https://pentest-tools.com/

```

Figure 18 Nikto CLI output showing successful scan of host

See **Appendix E – Nikto Report and Results** for full details

4.4 Use of OWASP ZAP to scan host

OWASP ZAP is a GUI based application that can scan a website for and cross-reference against lists of known vulnerabilities. Full output results can then be exported into a HTML report.



Figure 19 OWASP ZAP GUI for initiating a scan on a host

A scan was started on the cupstv website. This was left to run until completion, which took over 100 hours. Results showed a total of 11 alerts. Over 25% of these were identified as High Risk, under 10% were Medium Risk and over 60% were Low Risk.

See **Appendix F – OWASP ZAP REPORT** for full html report of results

Unfortunately, when initially opening the application, a prompt appears asking if the user session should be persisted or not. The default option is not to persist and in this test, the session was not saved. After a 100-hour scan, there was not enough time to repeat the scan and some additional useful information is now unavailable.

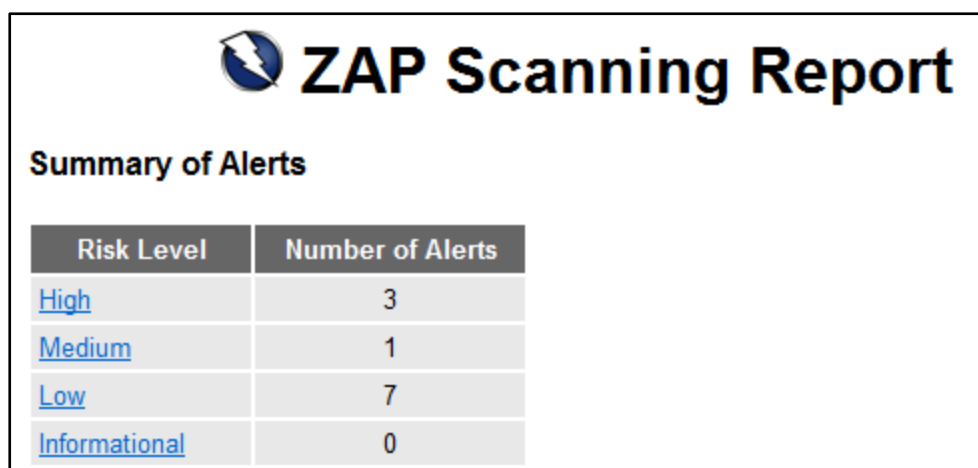


Figure 20 OWASP ZAP results summary

	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			0:42:08	2076		
Plugin						
Path Traversal	Medium	100	8:59:23	108474	0	Completed
Remote File Inclusion	Medium	100	7:50:59	72068	7	Completed
Server Side Include	Medium	100	4:34:45	28943	0	Completed
Cross Site Scripting (Reflected)	Medium	100	7:36:43	55891	0	Completed
Cross Site Scripting (Persistent) - Prime	Medium	100	0:43:42	7237	0	Completed
Cross Site Scripting (Persistent) - Spider	Medium	100	0:46:00	7216	0	Completed
Cross Site Scripting (Persistent)	Medium	100	0:11:53	0	0	Completed
SQL Injection	Medium	100	13:27:50	174948	1	Completed
Server Side Code Injection	Medium	100	4:46:37	57866	0	Completed
Remote OS Command Injection	Medium	100	17:20:06	231426	6	Completed
Directory Browsing	Medium	100	0:52:08	7220	0	Completed
External Redirect	Medium	100	5:16:06	65079	0	Completed
Buffer Overflow	Medium	100	14:40:24	3493	0	Completed
Format String Error	Medium	100	2:30:02	21711	1	Completed
CRLF Injection	Medium	100	3:42:16	50629	0	Completed
Parameter Tampering	Medium	100	6:19:15	49192	0	Completed
Script Active Scan Rules	Medium	100	0:00:00	0	0	Skipped, no scripts enabled.
Totals			100:20:18	965472	15	

Figure 21 Use of DirBuster to scan host

4.5 Use of DirBuster to scan host

The DirBuster GUI can be used to adjust the parameters for a scan. DirBuster requires use of a dictionary list. It comes with numerous, but final choice of dictionary is a user preference. The recommended list to use is directory-list-2.3-medium.txt[27]. The wordlists that are provided by DirBuster were generated by crawling web servers across the internet and collating real life directories and filenames that were found.

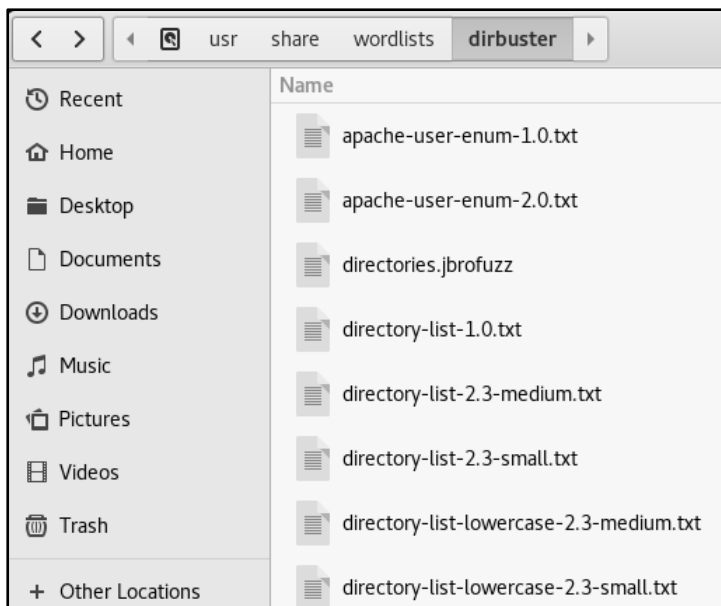


Figure 22 Wordlist dictionaries provided by DirBuster

The following scan parameters were used:

- Target URL: <http://cupstv.com:80/>
- Dictionary: directory-list-2.3-medium.txt
- All other settings were left as default.

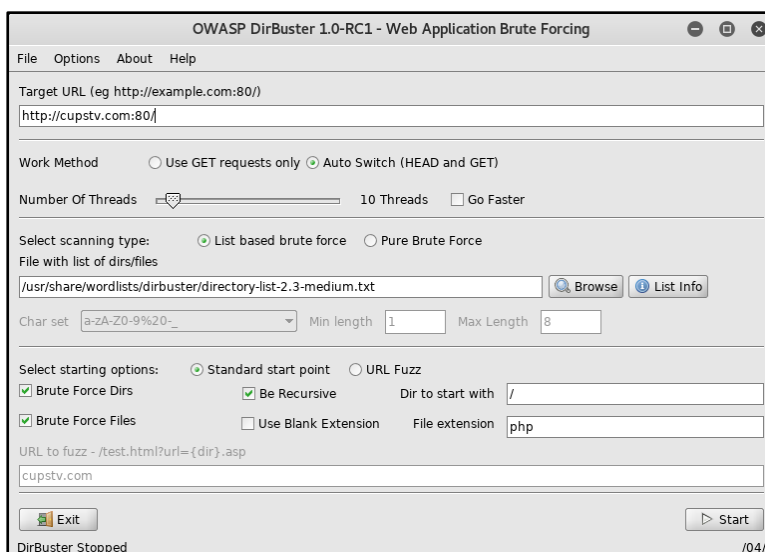


Figure 23 DirBuster GUI

Scan Information \ Results - List View: Dirs: 54 Files: 20 \ Results - Tree View \ Errors: 0 \			
Directory Structure	Response Code	Response Size	
about	200	148951	
crack	301	453	
12	301	519	
contact	301	522	
10	301	455	
new	301	509	
blog	301	501	
logo	301	459	
rss	200	476	
home	301	452	
login	301	463	
sitemap	301	453	
index.php	301	455	
content	301	349	
feed	200	460	
press	301	489	
media	301	536	
	301	453	

Figure 24 DirBuster scan in progress

The results of the DirBuster scan show a sitemap/directory tree of the site.

See **Appendix G – DirBuster Report** for full DirBuster scan report details

After browsing some of the URL's that were returned by the scan, one URL in particular was noteworthy:

<http://cupstv.com/login/>

When visiting that URL, the user is re-directed to the following URL:

<http://cupstv.com/login-page/>

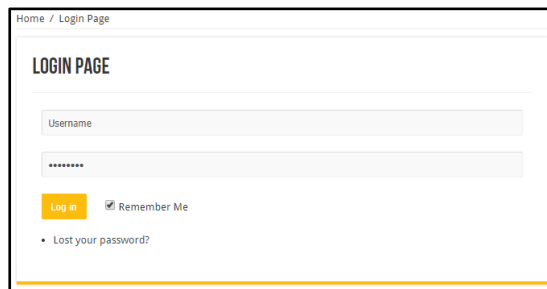
A screenshot of a web browser showing a login page. The page has a header with "Home / Login Page". Below the header, the title "LOGIN PAGE" is displayed. There are two input fields: "Username" and a password field with masked characters. Below the password field is an orange "Log in" button and a checkbox labeled "Remember Me". At the bottom, there is a link "Lost your password?".

Figure 25 Login page at <http://cupstv.com/login-page/>

After entering a random username and password combination the user is re-directed to the following URL:

<http://cupstv.com/kilishi-maidadi/>

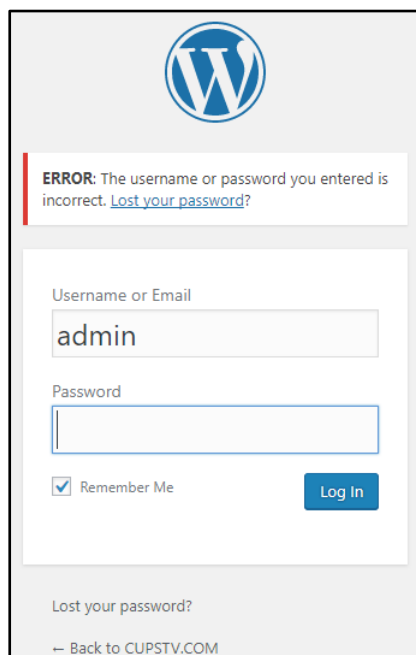
A screenshot of a web browser showing a login page. At the top is a WordPress logo. Below it is a red error message: "ERROR: The username or password you entered is incorrect. [Lost your password?](#)". Below the error message are two input fields: "Username or Email" with the text "admin" and a "Password" field. Below the password field is a checkbox labeled "Remember Me" and a blue "Log In" button. At the bottom, there is a link "Lost your password?" and a link "Back to CUPSTV.COM".

Figure 26 Login page at <http://cupstv.com/kilishi-maidadi/>

After clicking on the 'Lost your password' link, the user is re-directed to the following URL:

<http://cupstv.com/kilishi-maidadi/?action=lostpassword>

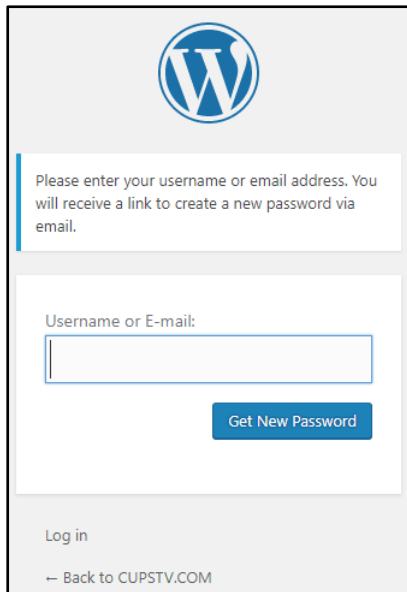


Figure 27 Lost your password page at <http://cupstv.com/kilishi-maidadi/?action=lostpassword>

After entering a guessed username of 'admin', the user is given an error message saying:

Error: Invalid username or e-mail

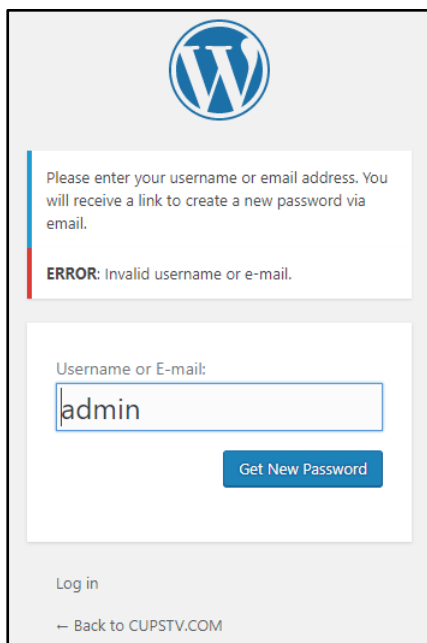


Figure 28 Error when attempting recovery of password

After a handful of attempts at guessing a username and password combination, the user is given an error message saying:

Error: Access from your IP address has been blocked for security reasons. Please contact the administrator.

There seems to be measures in place that block an IP address when multiple incorrect entries are detected. This is a well-known protection measure to prevent attempted brute force attack on a user account. For the tester, it was not a concern as testing was carried out on a computer that was accessing the target website from behind a VPN. It was simply a case of disconnecting

from the current VPN server and selecting a different VPN server. Any subsequent tests would then appear to the target to be coming from a new IP address. This was tested and the error about using a blocked IP address disappeared.

4.6 Use of WPScan to scan host

WPScan is a CLI tool that is included by default in the Kali Linux Operating System. It contains a built-in update method to update the database to the latest version.

`wpscan -h` can be used to list the summary of options available.

- `--update` Update database from online repository
- `--url` Target host
- `--enumerate u` Enumerate users

The following command was used to update the WPScan database:

`wpscan --update`

```
root@mil23-1t-k:~# wpscan --update

      W P S C A N
    _____

WordPress Security Scanner by the WPScan Team
Version 2.9.3
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[i] Updating the Database ...
[i] Update completed.
root@mil23-1t-k:~#
```

Figure 29 Updating WPScan database

The following command was used to initiate a scan against the CUPS website:

`wpscan --url cupstv.com --enumerate u`

See **Appendix H – WPScan Report** for complete results of the WPScan

```
root@mil23-1t-k:~# wpscan --url cupstv.com --enumerate u

      W P S C A N
    _____

WordPress Security Scanner by the WPScan Team
Version 2.9.3
Sponsored by Sucuri - https://sucuri.net
 @_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

[+] URL: http://cupstv.com/
[+] Started: Fri Dec 8 11:52:00 2017
[+] robots.txt available under: 'http://cupstv.com/robots.txt'
```

Figure 30 Initiating a WPScan on the target website

```
[+] robots.txt available under: 'http://cupstv.com/robots.txt'
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-admin/admin-ajax.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/js/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-includes/images/
[+] Interesting entry from robots.txt: http://cupstv.com/trackback/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-login.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-register.php
[+] Interesting entry from robots.txt: http://cupstv.com/temp/
[+] Interesting entry from robots.txt: http://cupstv.com/readme.html
[+] Interesting entry from robots.txt: http://cupstv.com/cgi-bin/
[+] Interesting entry from robots.txt: http://cupstv.com/recommended/
[+] Interesting entry from robots.txt: http://cupstv.com/comments/feed/
[+] Interesting entry from robots.txt: http://cupstv.com/index.php
[+] Interesting entry from robots.txt: http://cupstv.com/license.txt
[+] Interesting entry from robots.txt: http://cupstv.com/xmlrpc.php
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/plugins/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/themes/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/upload/
[+] Interesting entry from robots.txt: http://cupstv.com/
[+] Interesting entry from robots.txt: http://cupstv.com/wp-content/uploads/
```

Figure 31 WPScan results showing contents of robots.txt

Search engines use automated programs to scan websites across the internet to gather information for search engine users. These web robot automated programs are called web crawlers or search engine spiders. The Robots Exclusion Protocol (REP) has been adopted by the majority of commercial search engines to allow website owners to control what website data is made available to a web crawler. By placing a text file called *robots.txt* in the root of the website, specific instructions are given that request a web crawler to ignore certain files and folders within a site directory structure. By analysing the content of this file, an attacker can see if the developer has tried hiding any files or folders that might be of use to the attacker[28].

After browsing all the URL's in the robot.txt file, the only ones that didn't return an error were:

- <http://cupstv.com/comments/feed/>
This contained a list of user comments that had been written to the site and the relevant URLs
- <http://cupstv.com/license.txt>
This contained the default WordPress software license
- <http://cupstv.com/wp-content/upload/>
This page returned an error message 'Access Denied'
- <http://cupstv.com/wp-json/>
This page contained what seemed to be a list of JSON code commands for the WP REST API.

WPScan failed to identify the version of WordPress that is in use on the site. This is likely due to a configuration change that the site administrator has implemented. To hide the version number, the following line needs to be added to the *functions.php* file:

```
remove_action('wp_head', 'wp_generator');
```

```
[+] Interesting header: LINK: <http://cupstv.com/wp-json/>; rel="https://api.w.org/", <http://cupstv.com/>; rel=shortlink
[+] Interesting header: SERVER: Apache
[+] Interesting header: SET-COOKIE: wfvvt_3219804454=5a2a7ce8d122b; expires=Fri, 08-Dec-2017 12:22:08 GMT; path=/; httponly
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-POWERED-BY: PHP/5.4.45
[!] WordPress version can not be detected
```

Figure 32 WPScan was not able to detect the version number of WordPress

Additionally, WPScan reported that there were a number of known vulnerabilities found:

- An error log was found at the following location:

http://cupstvt.com/wp-content/themes/sahifa/error_log

Upon browsing the URL, an error log was displayed with numerous entries showing a folder structure path:

/home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php

```
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 01:57:45 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 06:08:12 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 14:34:00 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 14:45:01 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 15:02:00 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 15:12:25 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[06-Dec-2017 16:27:41 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 11:51:25 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 11:54:13 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 14:33:28 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
[08-Dec-2017 17:13:10 UTC] PHP Fatal error: Call to undefined function get_header() in /home/cupstvtmanager769/public_html/wp-content/themes/sahifa/index.php on line 1
```

Figure 33 Error Log with references to local path on web application server

This seems to expose the local folder structure of the web application server itself. From this path, it is possible to assume that *cupstvtmanager769* is a local user (and possibly an administrator user) on the server. This would be information that an attacker could possibly use in further attacks on this server.

Previously, as part of the testing done after using DirBuster, the tester attempted to use the ‘Lost your password page’ but could not progress past an error message saying ‘*Invalid username or e-mail*’. The same test was attempted using the *cupstvtmanager769* username and a message appeared saying ‘*Check your e-mail for the confirmation link*’. This seems to confirm that *cupstvtmanager769* is a valid username.

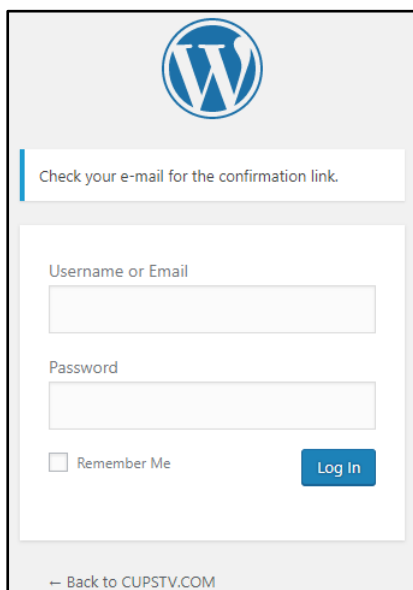
The image shows a WordPress login page. At the top is the WordPress logo. Below it is a blue banner with the text "Check your e-mail for the confirmation link." Underneath the banner is a login form with two input fields: "Username or Email" and "Password". Below the "Username or Email" field is a "Remember Me" checkbox. To the right of the "Password" field is a blue "Log In" button. At the bottom of the page is a link that says "← Back to CUPSTV.COM".

Figure 34 Message that seems to confirm the existence of *cupstvtmanager769* username

- Known Vulnerability found
Sahifa 2.4.0 - Multiple Script Path Disclosure Direct Request Path Disclosure
This known vulnerability allows an attacker to determine the full path of the web application server. This is the second vulnerability that exposes the local folder structure of the server.
- Known Vulnerability found
Sahifa 2.4.0 - Site Setting Reset CSRF
Cross-Site Scripting Request Forgery (CSRF) appeared at number 8 in the OWASP Top10 2013 but disappeared from the Top10 2017[29]. This does not mean that the vulnerability has disappeared, just that OWASP have rated other vulnerabilities with a higher significance. CSRF weaknesses can be exploited by an attacker to use the web browser of a victim to perform an undesirable action on a website without the users knowledge[30][31]. In conjunction with a social engineering attack, the attacker could trick the site administrator into running a script. This could be done by including a URL link in an email. The attacker would need to setup a web page containing malicious code. Using social engineering, they would need to trick the site administrator to visit that page. Upon doing so, the malicious code would run and exploiting the known vulnerable code in the WordPress Sahifa Theme, the site settings would be reset and a loss of data would result[32].

```
===== BEGIN CSRF EXPLOIT =====
<h1>Wordpress sahifa theme CSRF exploit By AkaStep<br></h1>

<body onload="javascript:document.forms[0].submit()">
<form method="post" action="http://hacker1.own/wp/wp-admin/admin.php?page=panel&reset=true">
<input type="hidden" name="action" value="reset" />
<!-- <input name="reset" type="submit" value="Reset Settings" />-->
</form>

===== END OF CSRF EXPLOIT =====
```

Figure 35 Example CSRF attack code

See **Appendix I - WPScan Sahifa Vulnerability** for full details of CSRF exploitation

- Known vulnerability found
Wunderground plugin version is out of date, the latest version is 2.1.3
Weather Underground is a commercial weather service. Using a plugin, a website can display real-time weather information.

```
[+] Enumerating plugins from passive detection ...
| 1 plugin found:

[+] Name: wunderground - v2.0.11
| Last updated: 2016-06-30T23:50:00.000Z
| Location: http://cupsttv.com/wp-content/plugins/wunderground/
| Readme: http://cupsttv.com/wp-content/plugins/wunderground/readme.txt
[!] The version is out of date, the latest version is 2.1.3

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Fri Dec 8 11:54:22 2017
[+] Requests Done: 369
[+] Memory used: 67.82 MB
[+] Elapsed time: 00:02:21
```

Figure 36 WPScan results showing plugin details and failure to enumerate usernames

WPScan detects the plugin as version 2.0.11. However, upon visiting the URL in the scan results a text file is displayed:

<http://cupstv.com/wp-content/plugins/wunderground/readme.txt>

```
== Changelog ==

= 2.1.2 and 2.1.3 on June 30, 2016 =
* Added: Ability to override API key using the `wunderground_api_key` filter or the `WUNDERGROUND_API_KEY`
* Fixed: Location autocomplete issue on HTTPS websites
* Fixed: Don't cache responses if they result in errors (good idea, eh?)
* Added: `wunderground_include_pws` filter to toggle whether to include Personal Weather Stations as data
* Updated: Twig template framework from 1.21.0 to 1.24.1

= 2.1.1 on August 25, 2015 =
* Fixed: WordPress 4.3 compatibility
* Added: Display any errors while fetching forecasts to administrators
* Updated: Polish translation (thanks Cezary!) and Brazilian Portuguese (thanks Filipe!)
* Removed unused `<thead>` code in `table-horizontal.html` template
* Updated: Twig template loader to version 1.21 from 1.18.1

= 2.1 on April 29, 2015 =
* Added: Now supports Weather Underground Severe Weather alerts & warnings
* Fixed: Issue using multi-word cities (thanks [@christianriley](https://github.com/christianriley)!)
* Fixed: Restored `alt` text for icon when using the Current template
* Fixed: Widget preview for "Old School" icon set
* Fixed: Fatal error if plugin or theme already used Twig template loader
* Fixed: Replace Icon Set FAQ code
* Updated: Translations - thanks to all the translators!
    - Slovenian: AleÅ; HoÄevlar
    - Bosnian: Marko Saraba
```

Figure 37 Changelog of wunderground readme file shows 2.1.3

Upon inspection, the changelog section of the Weather Underground readme file appears to contain details referring to plugin changes that were introduced in versions later than 2.0.11. The changelog entry for 2.1.3 is June 30, 2016. The WPScan scan says plugin last updated 2016-06-30T23:50:00. It is ambiguous if the plugin is reporting the date that the latest version was updated, or the date that the plugin was updated on the host server.

It appears that 2.1.3 is the likely version that is installed on this server and this is a false positive result from WPScan.

There seems to be measures in place that prevent username enumeration. This is a well-known protection measure to prevent attackers finding usernames and then attempting a brute force attack on that user account. This is likely due to a configuration change that the site administrator has implemented. To prevent username enumeration, code needs to be added to the 'functions.php' file[33].

```
// block WP enum scans
// https://m0n.co/enum
if (!is_admin()) {
    // default URL format
    if (preg_match('/author=([0-9]*)/i', $SERVER['QUERY_STRING'])) die();
    add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
}

function shapeSpace_check_enum($redirect, $request) {
    // permalink URL format
    if (preg_match('/\?author=([0-9]*) (\/*)/i', $request)) die();
    else return $redirect;
}
```

Figure 38 Example code to be inserted into functions.php file to prevent user enumeration

4.7 Use of Discover to scan host

Discover is a CLI tool that is included by default in Kali and can be launched from a terminal window. It contains a number of pre-configured scripts that can be run from a terminal GUI. It contains a built in feature to update to the latest versions from an online repository. A passive scan was initiated against the CUPS website. This then runs through a series of tools to perform passive reconnaissance on the target. The results from the scan can be exported to a comprehensive HTML report. See **Appendix J – Discover Report** for notable findings

Some of the most notable findings in the scan against the CUPS website were:

- A list of squatting domains that have been registered
These could potentially be used as part of a social engineering attack.
- Domain Registration details including name, address, phone number, email address
 Idris Ahmed
 Tecomex Forensics Ltd
 115 Lythalls Lane
 Holbrooks
 Coventry
 West Midlands
 CV6 6FN
 UK
 +44.7539288602
nubiantiger2000@gmail.com
 Again, these could be used as part of a targeted attack
- MX record found
 mail.cupstv.com
 This suggests that the domain has been configured for an e-mail server
- Site is hosted by GoDaddy
- DNS topology map creation

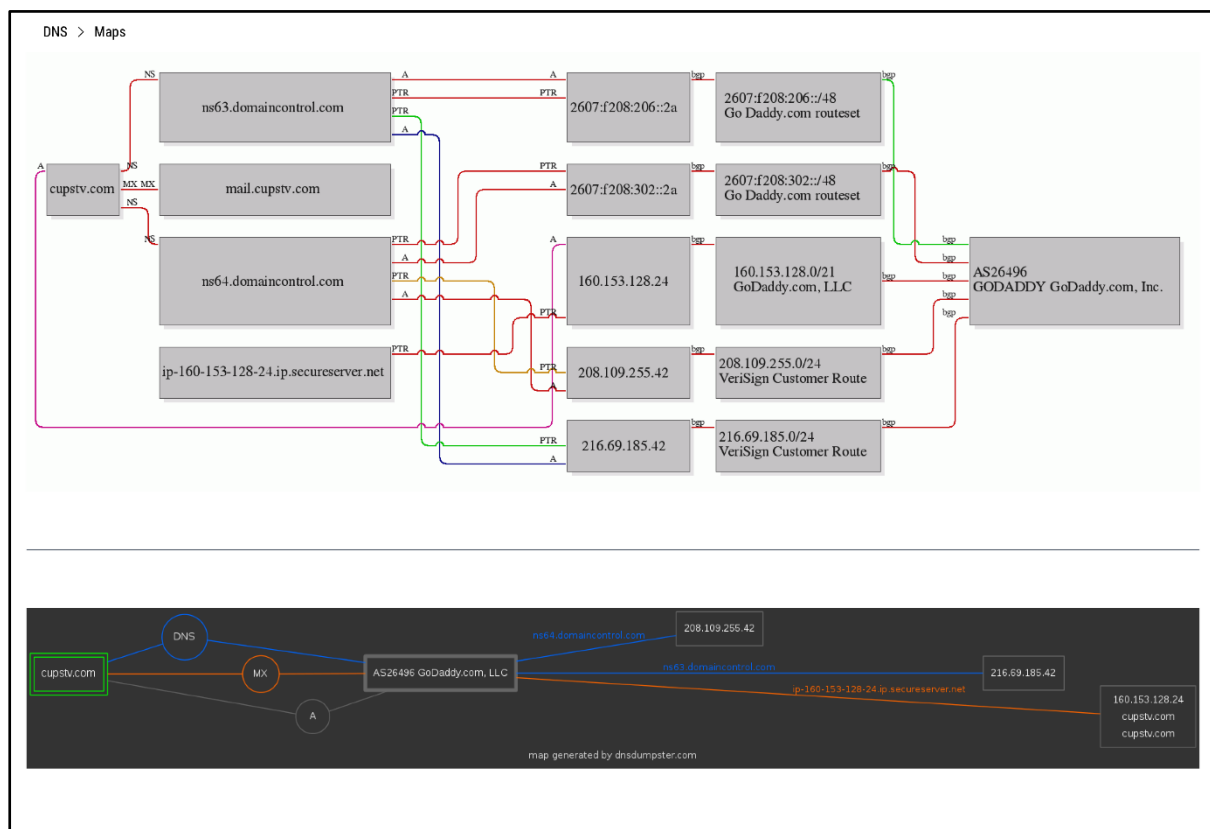


Figure 39 DNS Map output from Discover

4.8 Use of Metasploit to scan host

Metasploit can be used for many aspects of penetration testing. In this particular case, it was used for interrogation of the MySQL database that was previously found during the Nmap scan. See **Appendix K – Metasploit MySQL Results** for full details of the commands that were used and the results of the scans.

The most notable findings were:

- The version of MySQL that the server is running could initially be enumerated. Metasploit reported that it is running MySQL 5.6.36-cll-lve
- Metasploit has the ability to attempt brute force attacks on a MySQL database. However, after attempting to do so, it seems that intrusion detection measures blocked the IP address of the testers machine. After this was done, the target server would not respond and MySQL version could not be enumerated again. Once more, by changing VPN server, this could be temporarily circumvented but it meant that brute force password attacking prevention measures put a stop to further password testing.

4.9 Use of Nessus to scan host

Nessus is a web based tool that can be used to scan a host with a large number of configurable options. The following parameters were used:

- Discovery Scan Type Port scan (common ports)
- Assessment Scan Type Scan for all web vulnerabilities (complex)
- Advanced Scan Type Default

See **Appendix L – Nessus Scan Settings** for full details of the settings that were used.

Nessus can output results to a PDF document with full breakdown of results.

See **Appendix M – Nessus Scan Report** for full Nessus report

The most notable findings were:

- Total of 54 found vulnerabilities
- Zero Critical and High vulnerabilities
- Less than 15% Medium
- Less than 6% Low
- More than 79% Informational

160.153.128.24					
Summary					
Critical	High	Medium	Low	Info	Total
0	0	8	3	43	54
Details					

Figure 40 Nessus Summary of vulnerabilities – note 0 Critical/High found

5. Analysis of Results and Findings

After a comprehensive set of scans on the target website, there were lots of potential items for discussion. The recommended next step would be to provide all scan results to the CUPS System Administrator and arrange for a debrief meeting to discuss. The following questions regarding the most notable findings should be discussed:

- The list of ports that were found to be open after a Nmap scan
How many of these ports are actually currently in use?
Are the following services required? Recommend removal of any that are not.
 - FTP
 - SSH
 - e-mail ports – preferable to use secure ports rather than unencrypted ports
 - MySQL
- Operating System version
Nmap scan identified OS to be Linux 2.6.32 – 3.13
Is this correct?
Patch management should be carried out on a regular basis to ensure known vulnerabilities are addressed. What policies and procedures are in place to ensure this is occurring on a regular basis? Recommendation is to upgrade to the latest available version.
- Nikto scan was unsuccessful when scanning cupstv.com
Assumption is there are Intrusion Detection/Prevention Systems (IDS/IPS) in place.
What policies are in place to ensure these are kept up to date?
What reporting tools are available for the system administrator to be notified on any suspicious activity?
- OWASP ZAP detected the following alerts:

Number of alerts	Alert type
7	Remote File Inclusion
1	SQL Injection
6	Remote OS Command Injection
1	Format String Error
Total 15	

As previously mentioned, full report results for this scan were not saved.

Recommended action would be to initiate a new complete scan for further analysis of results.

- DirBuster was able to successfully crawl the directory structure of the CUPS website
Modern IDS/IPS systems can prevent this kind of attack. Implementation of additional authentication mechanisms can make it more difficult to successfully use automated tools – CAPTCHA forms etc.
- WPScan noted lots of entries in robots.txt file that didn't exist
Is a default robots.txt file being used with some additional custom entries?
When was this file last reviewed and how often do reviews occur?
Are all the current entries required?
Are there any additional entries required?
- WPScan was not able to identify the version of WordPress
What measures are in place to implement this?

What version is currently installed?

What policies are in place to ensure regular installation of updates/upgrades?

Recommendation is to upgrade to the latest available version.

- WPScan detected an error log with a reference to a user account (cupstvmanager769)
This error log should not be visible externally. Recommendation is to rectify this.
Are there any measures in place to ensure automated clean-up of old log files?
If possible – recommend changing username as a precaution.
- WPScan detected use of out of date software - Sahifa 2.4.0 theme and Weather Underground plugin
What version of the Sahifa theme is currently installed?
What version of the Weather Underground plugin is currently installed?
Was this a false positive result by WPScan?
What policies are in place to ensure regular installation of updates/upgrades?
Recommendation is to upgrade to the latest available version.
- Discover found a list of squatting domains.
Are any of these held by CUPS?
Is the System Administrator aware that these domain names have been registered?
This is something to be mindful of as they could potentially be used as part of a social engineering attack.
- Domain Registration details – are these still correct?
Recommend against use of a personal e-mail address for this.
nubiantiger2000@gmail.com
An MX record exists for mail.cupstv.com.
Use of a ***@cupstv.com e-mail address would be more suitable.
Is the mobile number still the best phone number to use?
Is there a fixed company office phone number that could be used instead?
- Metasploit detected that MySQL version 5.6.36-cll-lve was installed.
The latest version is 5.7.20
What policies are in place to ensure regular installation of updates/upgrades?
Recommendation is to upgrade to the latest available version.
- Metasploit was unsuccessful in any attempts at brute force attacks
Assumption is there are Intrusion Detection/Prevention Systems (IDS/IPS) in place.
What policies are in place to ensure these are kept up to date?
What reporting tools are available for the system administrator to be notified on any suspicious activity?
- Nessus detected 0 Critical/High vulnerabilities.
There were 8 Medium and 3 Low vulnerabilities detected and 43 informational alerts.
Recommendation is to carry out a further review of these results.
- All of the above are in addition to the standard recommended policies that should be in place regarding ensuring use of strong passwords, password change policies and password reuse policies etc. Tecomex-Forensics are available to assist if CUPS require any assistance with ensuring the relevant policies are in place.

GoDaddy are the existing site hosting providers – they have a number of different levels of service.

Basic	Deluxe	Ultimate	Developer
A great way to get started.	Get more visitors with an integrated SEO wizard.	More websites. More storage. More security.	Up to 5 sites and packed with pro features.
As low as \$3.99/mo On sale - Save 50% \$7.99/mo when you renew ⁴	As low as \$4.99/mo On sale - Save 50% \$9.99/mo when you renew ⁴	As low as \$7.99/mo On sale - Save 46% \$14.99/mo when you renew ⁴	As low as \$13.99/mo On sale - Save 44% \$24.99/mo when you renew ⁴
Configure	Configure	Configure	Configure
1 website	1 website	2 websites	5 websites
10 GB SSD storage ?	15 GB SSD storage ?	30 GB SSD storage ?	50 GB SSD storage ?
25,000 monthly visitors ?	100,000 monthly visitors ?	400,000 monthly visitors ?	800,000 monthly visitors ?
SFTP access	SSH/SFTP access	SSH/SFTP access	SSH/SFTP access
Free domain with annual plan ?	Free domain with annual plan ?	Search engine optimization for 2 sites ?	Free domain with annual plan ?
Pro Sites multi-site management tool ?	One-click staging site	Free domain with annual plan ?	One-click staging site
	Search engine optimization plugin ?	One-click staging site	1 SSL certificate – 1 year free (\$74.99 renewal annually) ?
	Pro Sites multi-site management tool ?	1 SSL certificate – 1 year free (\$74.99 renewal annually) ?	Need more sites? Call one of our experts at 020 7084 1810
		Ongoing malware scan & removal for 2 sites ?	Pro Sites multi-site management tool ?
		Need more sites? Call one of our experts at 020 7084 1810	
		Pro Sites multi-site management tool ?	

Figure 41 GoDaddy Managed WordPress Plans

GoDaddy are the world’s largest domain name registrar with over 17 million customers[34]. By using a large reputable company such as GoDaddy, there are a number of features available to customers that might not easily be implemented by a smaller company looking to host their own web site. Full details can be provided to CUPS on request, but highlights include:

- Automatic updates for WordPress core software and security updates
- Daily backups
- Malware scanning
- 24/7 Intrusion Detection Monitoring

All plans include		
✓ Access to 1,000s of free themes and plugins	✓ Free daily backups & 1-click restore	✓ Premium WordPress Hosting platform ?
✓ Free domain with annual plan ?	✓ One-click migration tool	✓ Free 24/7 support
✓ Automatic WordPress core software and security updates	✓ 99.9% uptime promise and money-back guarantee ?	✓ Free (1) Microsoft Office 365 email with the purchase of any annual plan. ?
	✓ Temporary domain name ?	

Figure 42 Features included in all GoDaddy WordPress hosting plans

Key features



Managed means marvelous-ness

We handle the technical stuff – automatic account setup and core updates, nightly backups with 1-click restore, DDoS protection, server optimization and more – so you can focus on building awe-inspiring sites.



Built for performance

Host your website on the platform built expressly to optimize WordPress, with high-performance coolness like load-balanced servers and SSD drives.



Award-winning support

As the world's largest WordPress hosting provider, we have award-winning, 24/7 support ready to solve your toughest hosting issues, plus hundreds of WordPress videos and interactive walkthroughs.



Keep bad guys at bay

Your site gets the personal bodyguard treatment, 24/7. Our security team monitors, thwarts, and deflects so you can rest easy.

Figure 43 Key features of GoDaddy WordPress hosting



Malware scan & removal

Hackers can inject malicious code — malware — into your site to deface it or steal sensitive info. With our continuous scans (included with Ultimate plan), malware's found and destroyed before it harms you or your customers.



Spammers, beware!

Nothing mucks up the gears like comment spammers. We stop them before they ever reach your site so your comments stay clean.



Standing guard

Our 24/7, award-winning security team meticulously monitors your site so they can thwart suspicious activity and deflect DDoS attacks with extreme prejudice.



Automatic updates

Having the latest version of WordPress's core software keeps your site happy and safe, so we automatically patch and update as soon as they're available.



Keep on walking, bots

We give bots das boot when they blast your site with phony requests. Keeping bots away lets the legitimate traffic get in.



Pre-screened plugins

We screen thousands upon thousands of [WordPress plugins](#). Why? So you never have to worry whether you're installing a well-behaved plugin or one that eats the last slice of pizza and leaves the box.

Figure 44 GoDaddy security features

Tecomex-Forensics recommends continuation of their hosting contract with GoDaddy, but are available to assist CUPS if assistance is required with contract renewal or amendments.

- When is the hosting contract due for renewal?
- Is it set to auto-renew?
- Is there a more suitable hosting plan currently available?

6. Conclusion

A proactive approach to computer system security is an essential aspect of ensuring a company's IT infrastructure, systems and applications are secure against external attack. Cyber-attacks are becoming more and more commonplace and the perpetrators of these attacks are becoming increasingly sophisticated and determined. Security breaches can be costly – in traditional monetary costs, but also extremely costly in terms of loss of data, reputational damage and loss of customer trust. Whilst it is impossible to design a system so that it is 100% impenetrable, regular penetration testing can alert system administrators to any newly detected vulnerabilities in their systems and allow risk reduction measures to be implemented. Repeat scheduled penetration testing should occur at regular intervals so these vulnerabilities can be detected and addressed before an attacker exploits them.

Using recognised industry testing methodology, penetration testing was carried out on the website of Citizens United for Peace and Stability (CUPS) – cupstv.com

Implementation of security measures in use were found to be acceptable, but there were a number of small items discovered that need addressing – notable items included use of out-of-date plugins and misconfigured error logging. Recommended measures to remedy these issues were documented and reported back to CUPS.

7. References and Bibliography

- [1] D. I. Ahmed, “The CUPS Organisation – CUPSTV.COM,” 2016. [Online]. Available: <http://cupstv.com/2016/11/04/the-cups-organisation/>. [Accessed: 29-Nov-2017].
- [2] S. Türpe and J. Eichler, “Testing Production Systems Safely: Common Precautions in Penetration Testing,” in *2009 Testing: Academic and Industrial Conference - Practice and Research Techniques*, 2009, pp. 205–209.
- [3] K. P. Haubris and J. J. Pauli, “Improving the Efficiency and Effectiveness of Penetration Test Automation,” in *2013 10th International Conference on Information Technology: New Generations*, 2013, pp. 387–391.
- [4] OWASP, “OWASP - Top 10 - 2017,” 2017.
- [5] “LulzSec’s Sony Hack Really Was as Simple as It Claimed - The Atlantic,” 2011. [Online]. Available: <https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/>. [Accessed: 07-Dec-2017].
- [6] A. Russo and A. Sabelfeld, “Securing Timeout Instructions in Web Applications,” in *2009 22nd IEEE Computer Security Foundations Symposium*, 2009, pp. 92–106.
- [7] D. Tomescu, “XML Based Attacks.”
- [8] A. A.-E. (secgeek), “Delete Credit Cards from any Twitter Account in ads.twitter.com,” 2014. [Online]. Available: <https://hackerone.com/reports/27404>.
- [9] C. Koliass, G. Kambourakis, A. Stavrou, J. Voas, and I. Fellow, “DDoS in the IoT,” *Computer (Long. Beach. Calif.)*, vol. 50, no. 7, pp. 80–84, 2017.
- [10] Ying Zhao, Pingke Yi, Y. Zhao, and P. Yi, “Modeling the propagation of XSS worm on social networks,” *2013 IEEE Globecom Work. GC Wkshps 2013*, pp. 207–210, Dec. 2013.
- [11] P. Chaudhary, “Cross-Site Scripting (XSS) Worms in Online Social Network (OSN): Taxonomy and Defensive Mechanisms,” pp. 2131–2136, 2016.
- [12] J. De Vries, H. Hoogstraaten, J. van den Berg, and S. Daskapan, “Systems for detecting advanced persistent threats: A development roadmap using intelligent data analysis,” *Proc. 2012 ASE Int. Conf. Cyber Secur. CyberSecurity 2012*, no. SocialInformatics, pp. 54–61, Dec. 2013.
- [13] T. Murakami, S. Kumano, and H. Koide, “An implementation of tracing attacks on advanced persistent threats by using actors model,” in *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)*, 2014, pp. 1316–1320.
- [14] R. Vibhandik and A. K. Bose, “Vulnerability assessment of web applications - a testing approach,” *2015 Forth Int. Conf. e-Technologies Networks Dev.*, pp. 16–21, Sep. 2015.
- [15] “Offensive Security Introduces Kali Linux | Kali Linux,” 2017. [Online]. Available: <https://www.kali.org/offensive-security-introduces-kali-linux/>. [Accessed: 30-Nov-2017].

- [16] O. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," in *2017 International Conference on Cyberworlds (CW)*, 2017, pp. 222–225.
- [17] "Nmap: the Network Mapper - Free Security Scanner," 2017. [Online]. Available: <https://nmap.org/>. [Accessed: 30-Nov-2017].
- [18] "Nikto2 | CIRT.net," 2017. [Online]. Available: <https://cirt.net/Nikto2>. [Accessed: 30-Nov-2017].
- [19] "OWASP Zed Attack Proxy Project - OWASP," 2017. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. [Accessed: 30-Nov-2017].
- [20] "WPScan by the WPScan Team," 2017. [Online]. Available: <https://wpscan.org/>. [Accessed: 30-Nov-2017].
- [21] M. Hills, "Navigating the WordPress plugin landscape," in *2016 IEEE 24th International Conference on Program Comprehension (ICPC)*, 2016, pp. 1–10.
- [22] P. Kim, *The Hacker Playbook 2: Practical Guide To Penetration Testing*. 2015.
- [23] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," in *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, 2014, pp. 237–242.
- [24] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2017, pp. 179–181.
- [25] Microsoft, "Microsoft - Sample SLA," 2008. [Online]. Available: <https://technet.microsoft.com/en-us/library/cc543293.aspx>. [Accessed: 06-Dec-2017].
- [26] "Terms Of Service | NordVPN," 2017. [Online]. Available: <https://nordvpn.com/terms-of-service/>. [Accessed: 07-Dec-2017].
- [27] "Category:OWASP DirBuster Project - OWASP." [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project. [Accessed: 08-Dec-2017].
- [28] Y. Sun, I. G. Councill, and C. L. Giles, "The Ethicality of Web Crawlers," in *2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 2010, pp. 668–675.
- [29] "OWASP Top 10 2007-2017: The Fall of CSRF - nVisium Blog." [Online]. Available: <https://nvisium.com/blog/2017/11/30/owasp-top-10-2007-2017-the-fall-of-csrf/>. [Accessed: 08-Dec-2017].
- [30] X. Lin, P. Zavarisky, R. Ruhl, and D. Lindskog, "Threat Modeling for CSRF Attacks," in *2009 International Conference on Computational Science and Engineering*, 2009, pp. 486–491.
- [31] G. Avramescu, M. Bucicioiu, D. Rosner, and N. Tapus, "Guidelines for Discovering and Improving Application Security," in *2013 19th International Conference on*

Control Systems and Computer Science, 2013, pp. 560–565.

- [32] “WordPress Sahifa 2.4.0 Cross Site Request Forgery / Path Disclosure $\approx$ Packet Storm.” [Online]. Available: <https://packetstormsecurity.com/files/119191/>. [Accessed: 08-Dec-2017].
- [33] “Stop User Enumeration in WordPress | Perishable Press.” [Online]. Available: <https://perishablepress.com/stop-user-enumeration-wordpress/>. [Accessed: 08-Dec-2017].
- [34] “Domain Names | The World’s Largest Domain Name Registrar - GoDaddy UK.” [Online]. Available: <https://uk.godaddy.com/>. [Accessed: 11-Dec-2017].

8. Appendices

Appendices are in a separate document
P1705837 - M7X01701 - Network Security Appendices

- A. Appendix A - Scope of Work
- B. Appendix B - SLA
- C. Appendix C - VPN Policy
- D. Appendix D - Nmap Report
- E. Appendix E - Nikto Report and Results
- F. Appendix F - OWASP ZAP Report
- G. Appendix G - DirBuster Report
- H. Appendix H - WPScan Report
- I. Appendix I - WPScan Sahifa Vulnerability
- J. Appendix J - Discover Report
- K. Appendix K – Metasploit MySQL Results
- L. Appendix L – Nessus Scan Settings
- M. Appendix M – Nessus Scan Report