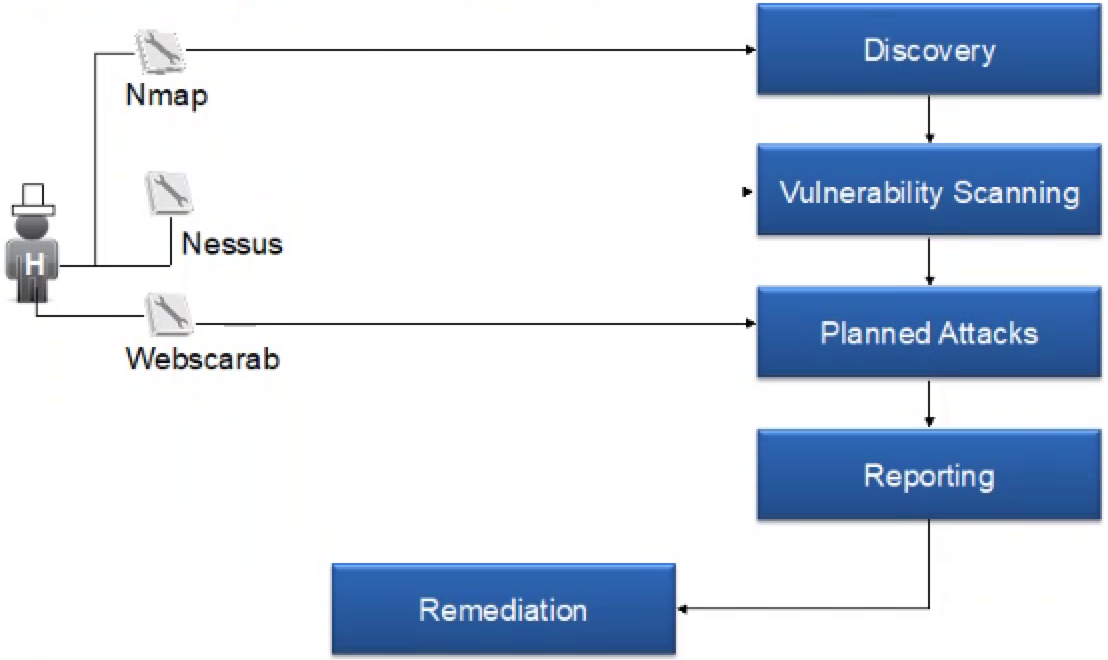
Security Assessment



Nmap

Nessus

Webscarab

Discovery

Vulnerability Scanning

Planned Attacks

Reporting

Remediation

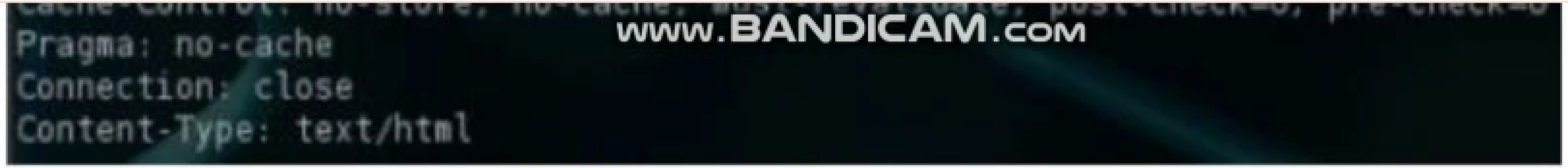
Image Source: *Security Strategies in Web Applications and Social Networking, 2015*

Task

Discovery by Fingerprinting

Fingerprinting

1. Manual fingerprinting using telnet and netcat
    1. Obtain the header information from the web server using telnet and nmap
    2. How to enable Telnet client on Windows 10
        1. Enabling the telnet client

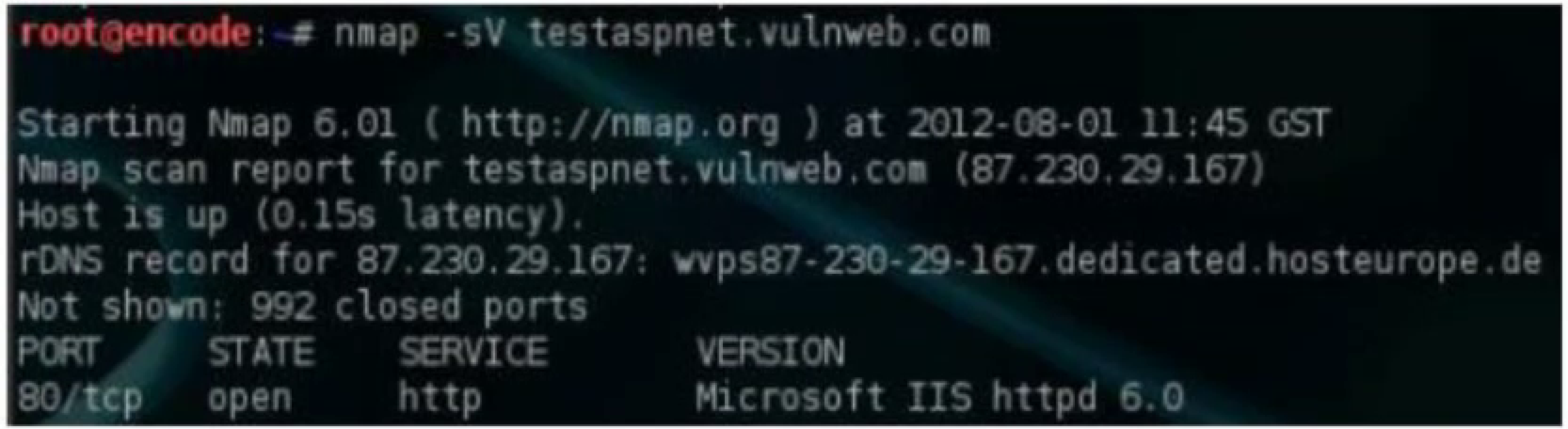


```
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html
```

HTTP Response Header – Telnet

Screenshot of a black screen code indicating: HTTP response header using telnet

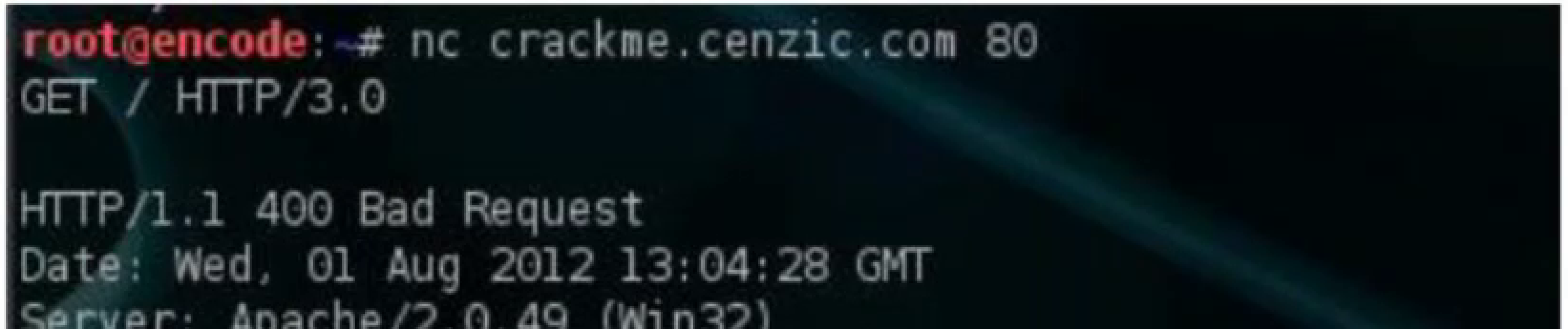
ng our port scan with **Nmap** on the remote host to use the command - sV which will obtain as well erver that is running. For example in the image below we can see from the output that **Nmap** sion 6.0.



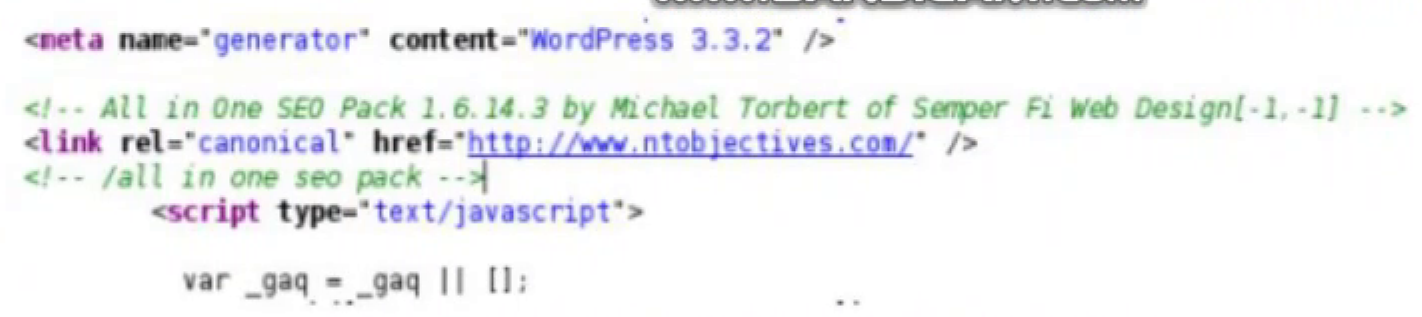
```
root@encode:~# nmap -sV testaspnet.vulnweb.com

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-01 11:45 GST
Nmap scan report for testaspnet.vulnweb.com (87.230.29.167)
Host is up (0.15s latency).
rDNS record for 87.230.29.167: wvps87-230-29-167.dedicated.hosteurope.de
Not shown: 992 closed ports
PORT      STATE    SERVICE        VERSION
80/tcp    open     http           Microsoft IIS httpd 6.0
```

Web Server Fingerprinting – Nmap

Another method is to send a malformed request to the web server that will cause the web server to produce an error page which will contain in the response header the version of the web server.



```
root@encode:~# nc crackme.cenzic.com 80
GET / HTTP/3.0

HTTP/1.1 400 Bad Request
Date: Wed, 01 Aug 2012 13:04:28 GMT
Server: Apache/2.0.49 (Win32)
```



```
<meta name="generator" content="WordPress 3.3.2" />

<!-- All in One SEO Pack 1.6.14.3 by Michael Torbert of Semper Fi Web Design[-1,-1] -->
<link rel="canonical" href="http://www.ntobjectives.com/" />
<!-- /all in one seo pack -->
          <script type="text/javascript">

            var _gaq = _gaq || [];
```

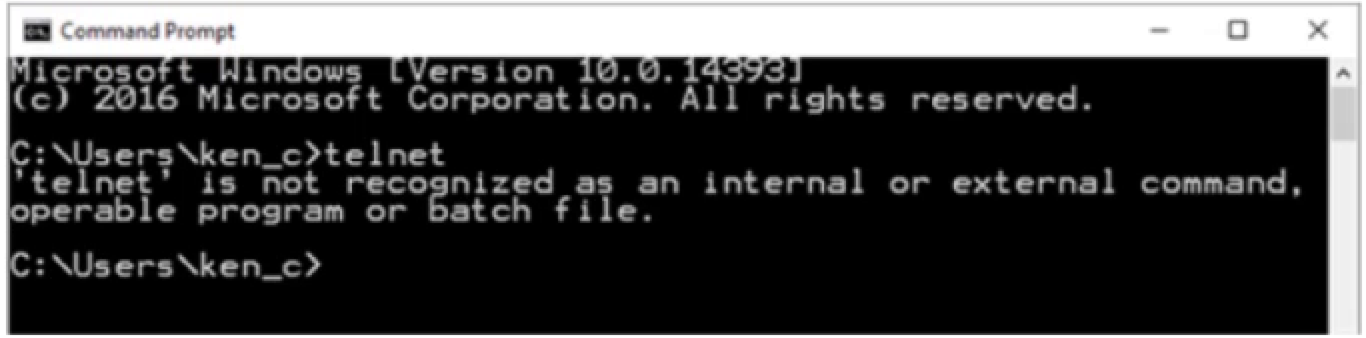
Discovering the version via source code inspection

Code screenshot: showing Discovering the version via source code inspection, It shows the application is WordPress 3.2.2

aded. You may do it you want but no need to submit it.

ent on Windows 10?

The Telnet Client is a great tool for developers and administrators to help manage and test network connectivity. However, the Telnet Client application is disabled by default in Microsoft Windows 10. Attempts to use it before activation returns the error message 'not recognized as an internal or external command, operable program or batch file'.

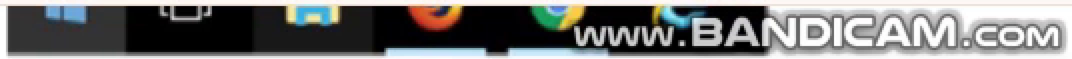


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\ken_c>telnet
'telnet' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\ken_c>
```

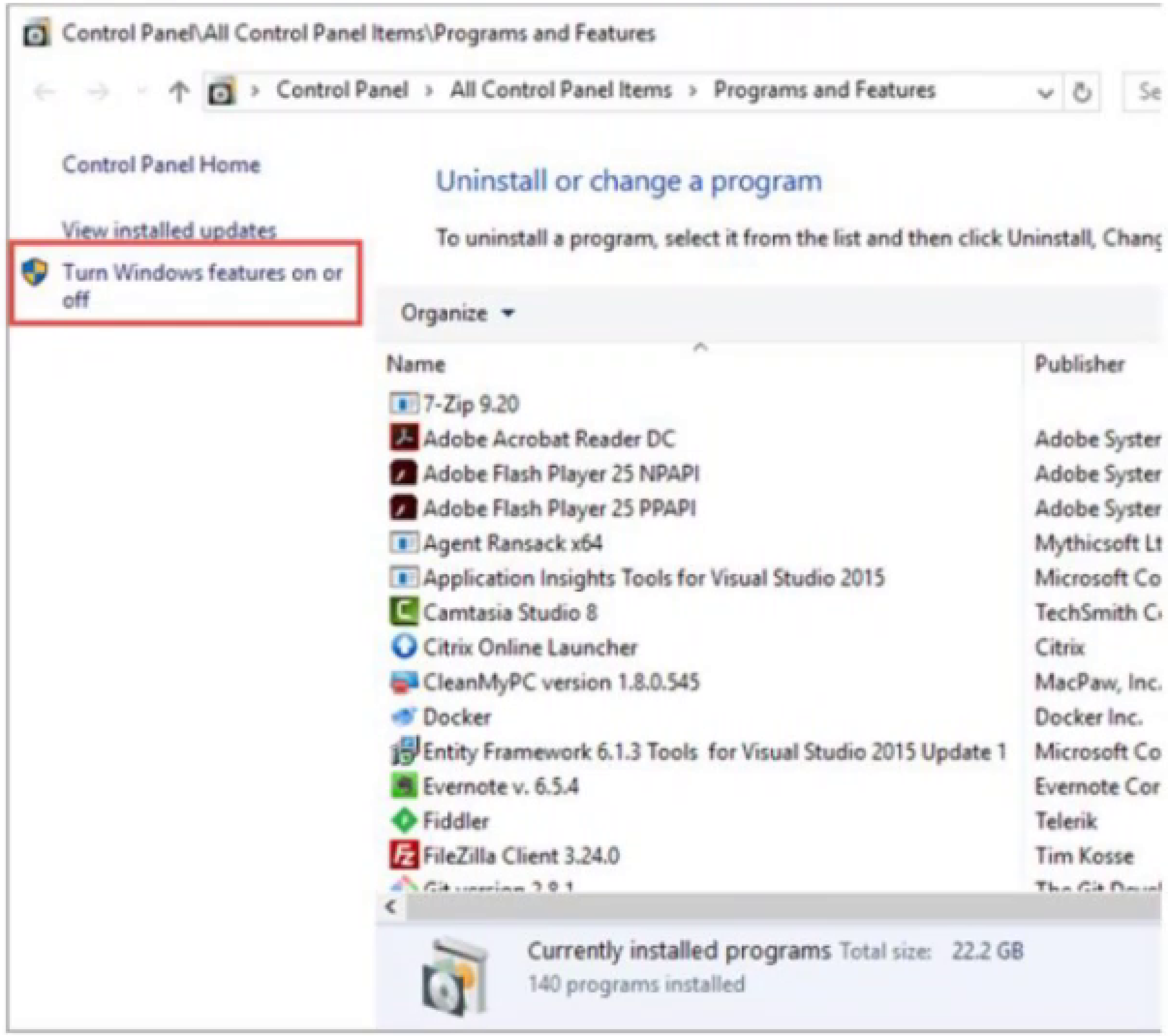
The following step-by-step shows you how to enable Telnet.

1.2.1 Enabling the Telnet Client

To enable Telnet Client on Windows 10, follow these step:



2. Click **Turn Windows features on or off** from the left-hand menu.



Control Panel\All Control Panel Items\Programs and Features

Control Panel › All Control Panel Items › Programs and Features
Se
Control Panel Home
View installed updates
Turn Windows features on or off
Organize

Uninstall or change a program

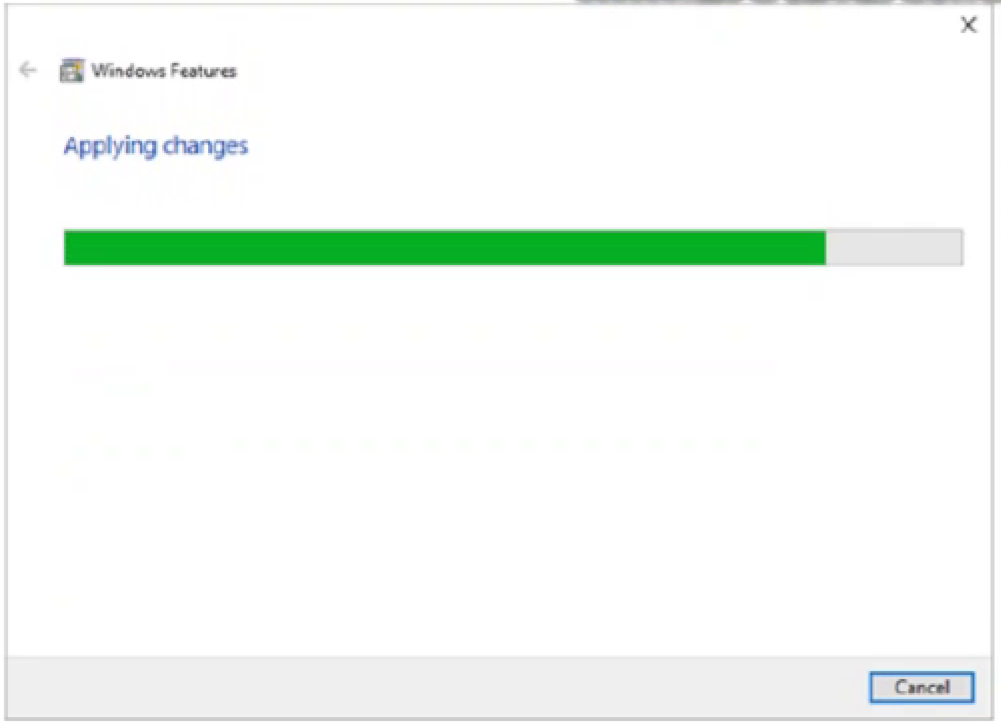
To uninstall a program, select it from the list and then click Uninstall, Chang

Name	Publisher
7-Zip 9.20	
Adobe Acrobat Reader DC	Adobe Syster
Adobe Flash Player 25 NPAPI	Adobe Syster
Adobe Flash Player 25 PPAPI	Adobe Syster
Agent Ransack x64	Mythicsoft Lt
Application Insights Tools for Visual Studio 2015	Microsoft Co
Camtasia Studio 8	TechSmith C
Citrix Online Launcher	Citrix
CleanMyPC version 1.8.0.545	MacPaw, Inc.
Docker	Docker Inc.
Entity Framework 6.1.3 Tools for Visual Studio 2015 Update 1	Microsoft Co
Evernote v. 6.5.4	Evernote Cor
Fiddler	Telerik
FileZilla Client 3.24.0	Tim Kosse
Git version 2.8.1	The Git Devel

Currently installed programs Total size: 22.2 GB
140 programs installed

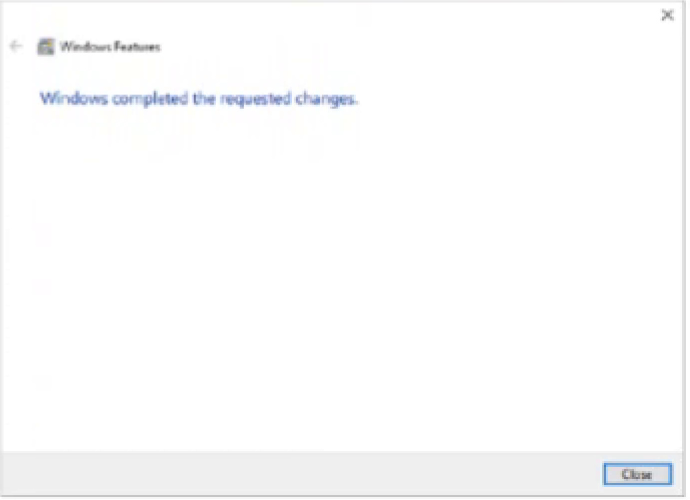
3. Control Pane|\All Control Panel Items\Programs and Features Screenshot: Click Turn Windows features on or off from the left-

appears. Scroll down and select **Telnet Client**. Click **OK**.



Applying changes

5. Once complete, a success message appears.

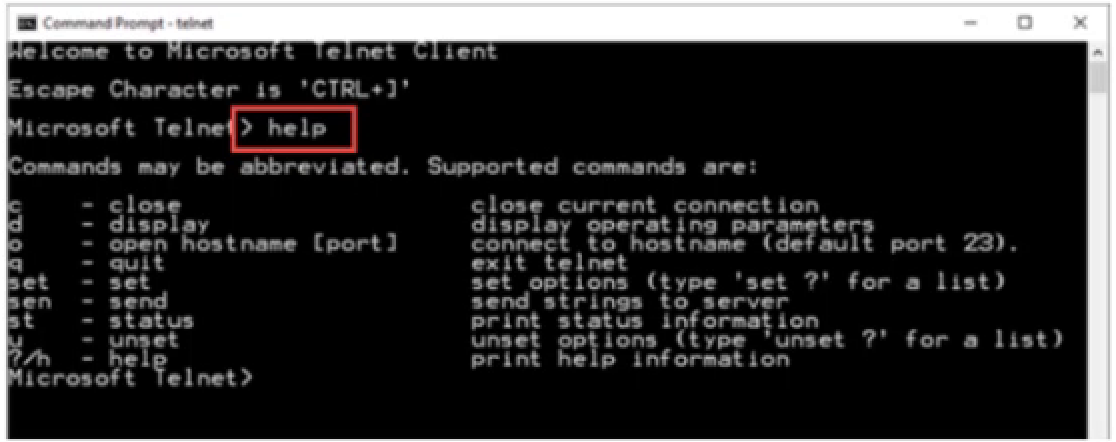


Windows completed the requested changes.

1.2.2 Verify the install

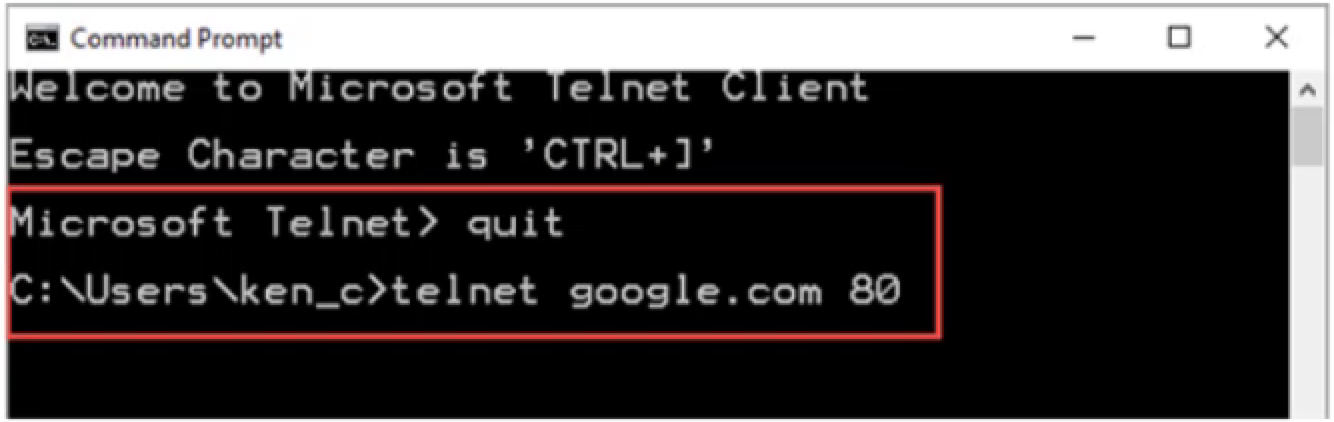
Once the installation completes, we can use the Telnet Client.

1. Launch the Command Prompt by typing **Command Prompt** into the search box on the menu bar and clicking the app returned.
2. Alternatively, you can also type **Windows Key + R** to open the **Run** command dialogue. Type **cmd** and hit the**Enter** key.
3. Type **telnet** and hit **Enter** to access the Telnet Client
4. Type **help** to see the supported Telnet commands.



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> help

Commands may be abbreviated. Supported commands are:

c    - close                    close current connection
d    - display                  display operating parameters
o    - open hostname [port]     connect to hostname (default port 23).
q    - quit                     exit telnet
set  - set                      set options (type 'set ?' for a list)
sen  - send                     send strings to server
st   - status                   print status information
u    - unset                    unset options (type 'unset ?' for a list)
?/h  - help                     print help information
Microsoft Telnet>
```

5. Screenshot of the black screen command- typed help to see the supported Telnet commands
6. nto Google on port 80



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> quit

C:\Users\ken_c>telnet google.com 80
```

2. **Install Nmap**

   Run the installer once it is finished downloading. You will be asked which components you would like to install. To get the full benefit of Nmap, keep all of those checked. Nmap will not install any adware or spyware.

3. Run the "**Nmap - Zenmap**" **GUI Program**
   If you left your settings at default during installation, you should be able to see an icon for it on your desktop. If not, look in your Start menu. Opening Zenmap will start the program.

4. **Enter in the target for your scan**

   The Zenmap program makes scanning a fairly simple process. The first step to running a scan is choosing your target. You can enter a domain (exampl.com) an IP address (127.0.0.1), a network (192.168.1.0/24), or a combination of those.

   - Depending on the intensity and target of your scan, running a Nmap scan may be against the terms of your internet service provider, and may land you in hot water. Always check your local laws and your ISP contract before performing Nmap scans on targets other than your won network.

5. **Choose your Profile**

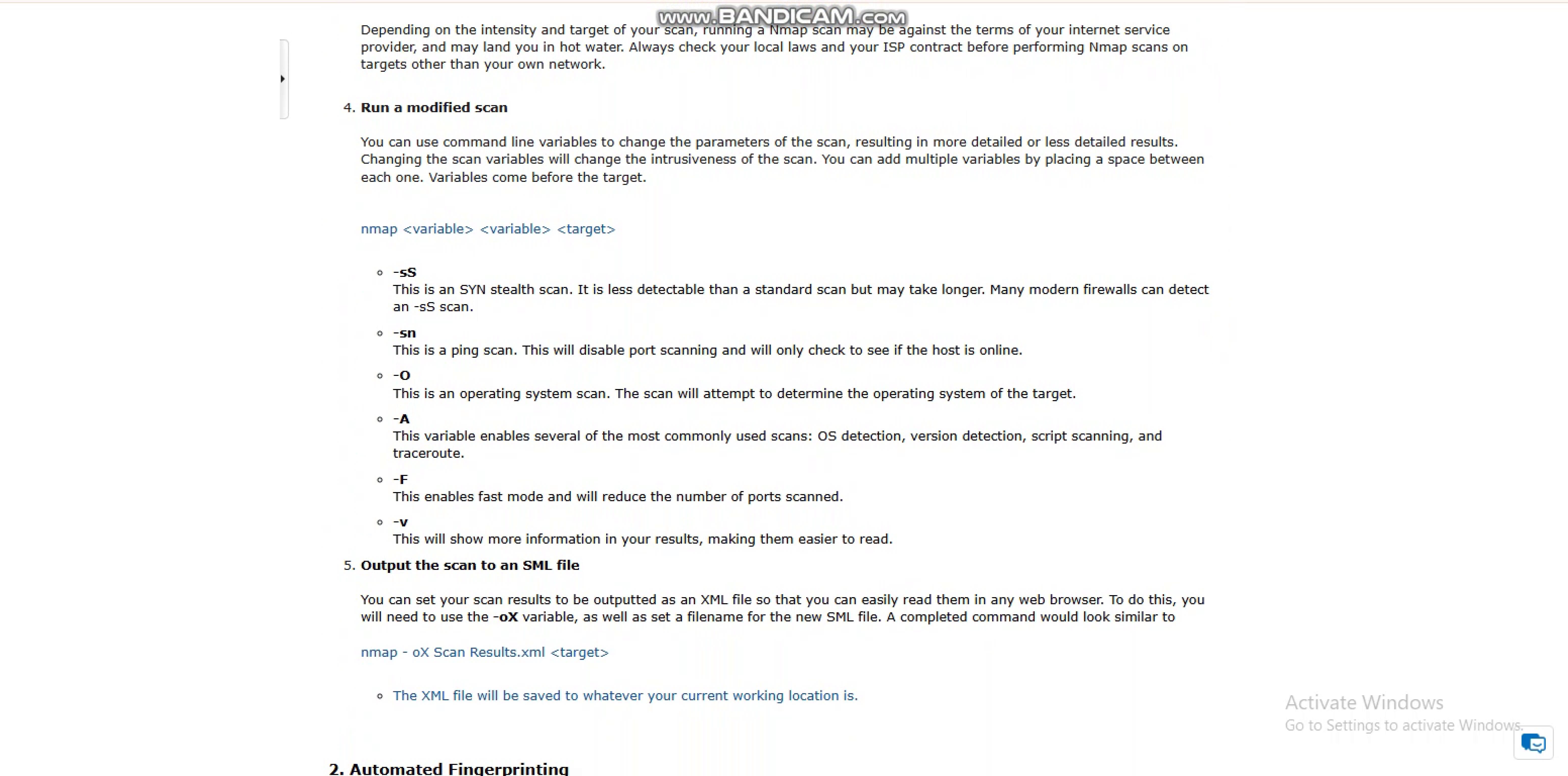
   Profiles are preset groupings of modifiers that change what is scanned. The profiles allow you to quickly select different types of scans without having to ty0pe in the modifiers on the command line. Choose the profile that best fits your needs:

   - **Intense scan**
     A comprehensive scan. Contains Operating System (OS) detection, version detection, script scanning, traceroute, and has aggressive scan timing. This is considered an intrusive scan.
   - **Ping scan**
     This scan simply detects if the targets are online, it does not scan any ports.
   - **Quick scan**
     This is quicker than a regular scan due to aggressive timing and only scanning select ports.
   - **Regular scan**
     This is the standard Nmap scan without any modifiers. It will return ping and return open ports on the target.

6. **Click Scan to start scanning**

   The active results of the scan can be displayed in the Nmap Output tab. The time the scan takes will depend on the scan profile you choose, the physical distance to the target, and the target's network configuration.

7. **Read your results**



Depending on the intensity and target of your scan, running a Nmap scan may be against the terms of your internet service provider, and may land you in hot water. Always check your local laws and your ISP contract before performing Nmap scans on targets other than your own network.

4. **Run a modified scan**

   You can use command line variables to change the parameters of the scan, resulting in more detailed or less detailed results. Changing the scan variables will change the intrusiveness of the scan. You can add multiple variables by placing a space between each one. Variables come before the target.

   ```
   nmap <variable> <variable> <target>
   ```

   - **-sS**
     This is an SYN stealth scan. It is less detectable than a standard scan but may take longer. Many modern firewalls can detect an -sS scan.
   - **-sn**
     This is a ping scan. This will disable port scanning and will only check to see if the host is online.
   - **-O**
     This is an operating system scan. The scan will attempt to determine the operating system of the target.
   - **-A**
     This variable enables several of the most commonly used scans: OS detection, version detection, script scanning, and traceroute.
   - **-F**
     This enables fast mode and will reduce the number of ports scanned.
   - **-v**
     This will show more information in your results, making them easier to read.

5. **Output the scan to an SML file**

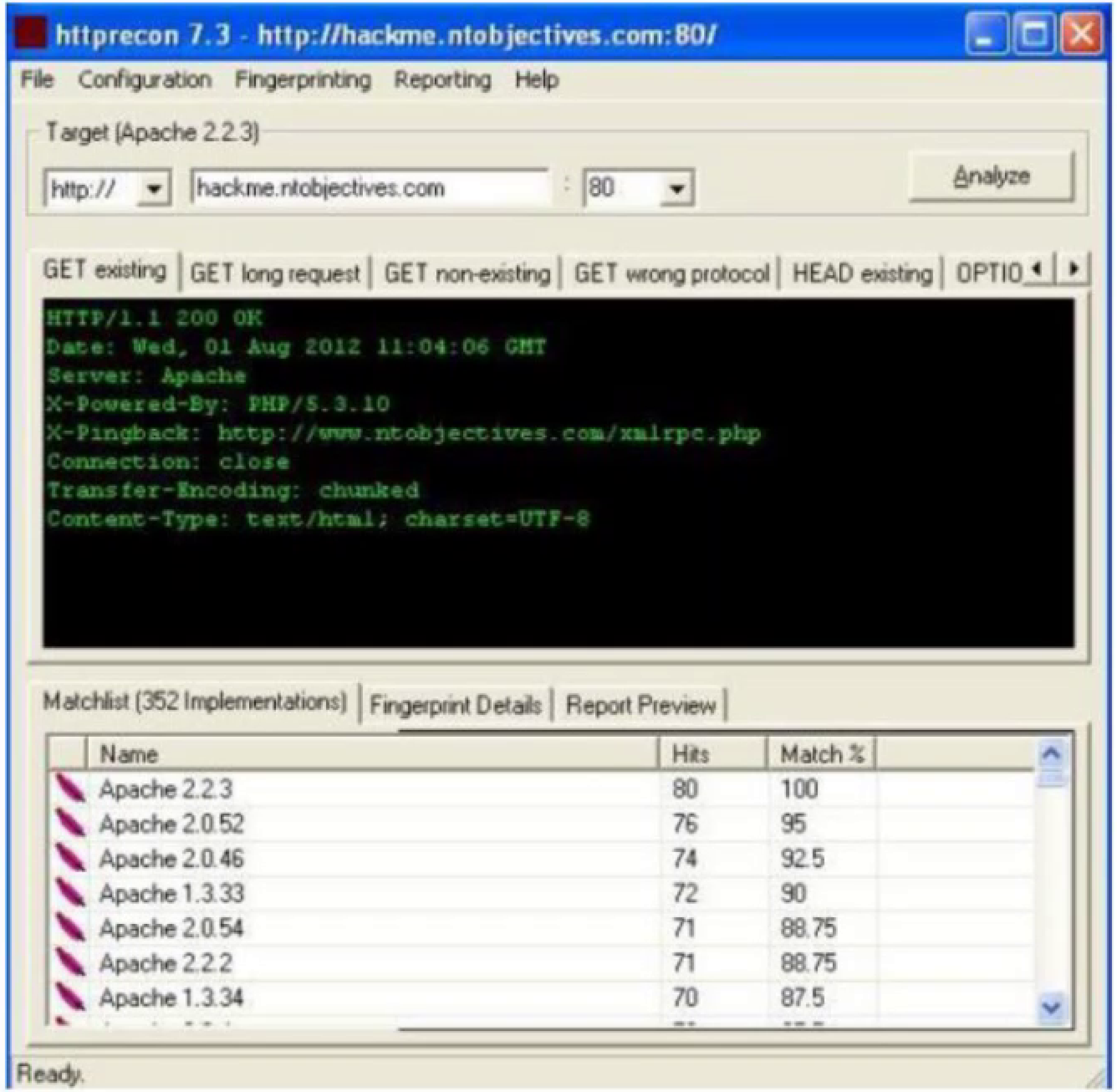
   You can set your scan results to be outputted as an XML file so that you can easily read them in any web browser. To do this, you will need to use the **-oX** variable, as well as set a filename for the new SML file. A completed command would look similar to

   ```
   nmap - oX Scan Results.xml <target>
   ```

   - The XML file will be saved to whatever your current working location is.

2. Automated Fingerprinting

Another tool that performs pretty much the same job as the **httprint** is the **httprecon**. This tool is for Windows platforms and it sends a different kind of request to the target web server to identify its version. The image below is showing that we have a match of 100% that the host that we have scanned is running Apache 2.2.3 version.



```
HTTP/1.1 200 OK
Date: Wed, 01 Aug 2012 11:04:06 GMT
Server: Apache
X-Powered-By: PHP/5.3.10
X-Pingback: http://www.ntobjectives.com/xmlrpc.php
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

Name	Hits	Match %
Apache 2.2.3	80	100
Apache 2.0.52	76	95
Apache 2.0.46	74	92.5
Apache 1.3.33	72	90
Apache 2.0.54	71	88.75
Apache 2.2.2	71	88.75
Apache 1.3.34	70	87.5

Web Server Fingerprinting – httprecon