ILLINOIS INSTITUTE
OF TECHNOLOGY

Penetration Test Report

By Timothy Kang

ITMS 543-02

11/23/2018

Contents

I. Executive Summary

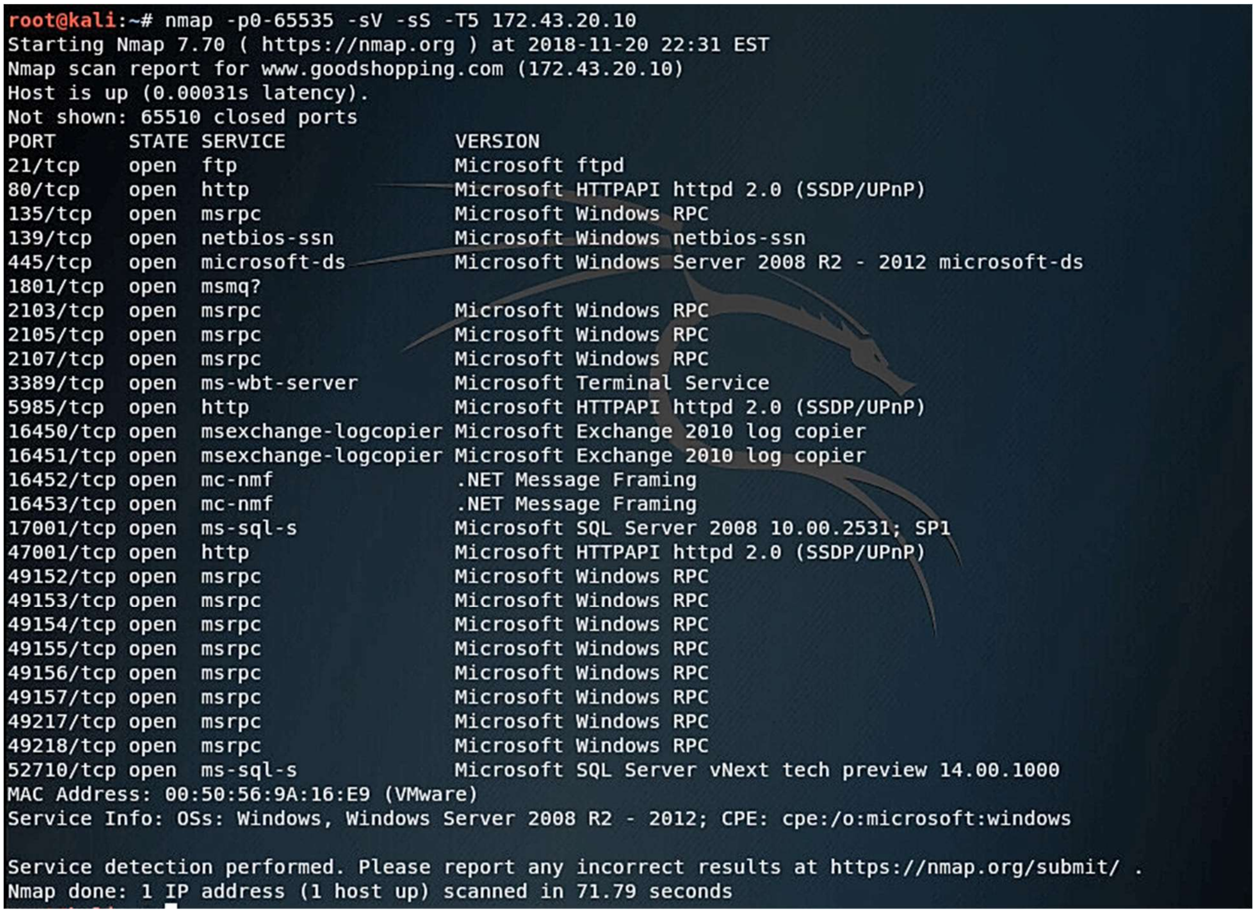
Timothy Kang from ITMS 543-02 was “contracted” by the startup company “Good Shopping” to conduct a vulnerability analysis and penetration test. The target will be the company’s 2 websites: www.goodshopping.com and www.moviescope.com. A series of tools will be used in order to test the websites, find and analyze vulnerabilities, and attempt at penetrating the target. Identifying such vulnerabilities and attack vectors will be used to understand the level of security of the websites and what an outside attacker can potentially do. No information other than the two website links, the IP address, and the names of the company president, CIO, and CFO have been provided. This information is similar to what an outside attacker might come across and begin with. Scans and vulnerability analysis tools will first be conducted to understand what openings are available for the attacker and any vulnerabilities that are spotted by either the application or myself. The easy ports such as FTP, SSH, and telnet could be used to connect with the server if proper credentials are found. If this cannot be accomplished, observing the other open ports and the versions associated with them can be used to find exploits as another way to gain elevated privileges. The end goal of this penetration test is to gain access onto the server with a high enough privilege to do necessary tasks.

II. Testing

This section will go over the different test scans that have been conducted to test the websites and the IP address. The purpose will be to find any vulnerabilities that can be analyzed and categorized in the following section.

Nmap

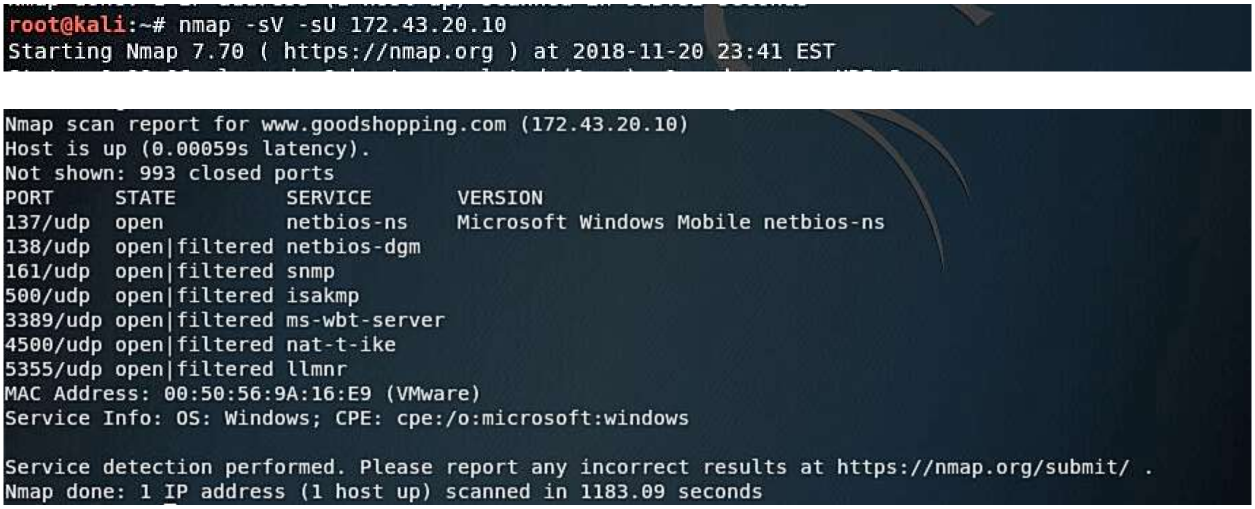
As stated earlier, open ports should be observed since this can serve as a weakness that an attack can exploit. Therefore, two nmap scans will be conducted: One for TCP ports and other for UDP ports.



```
root@kali:~# nmap -p0-65535 -sV -sS -T5 172.43.20.10
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-20 22:31 EST
Nmap scan report for www.goodshopping.com (172.43.20.10)
Host is up (0.00031s latency).
Not shown: 65510 closed ports
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
80/tcp    open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1801/tcp  open  msmq?
2103/tcp  open  msrpc                Microsoft Windows RPC
2105/tcp  open  msrpc                Microsoft Windows RPC
2107/tcp  open  msrpc                Microsoft Windows RPC
3389/tcp  open  ms-wbt-server        Microsoft Terminal Service
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
16450/tcp open  msexchange-logcopier Microsoft Exchange 2010 log copier
16451/tcp open  msexchange-logcopier Microsoft Exchange 2010 log copier
16452/tcp open  mc-nmf                .NET Message Framing
16453/tcp open  mc-nmf                .NET Message Framing
17001/tcp open  ms-sql-s             Microsoft SQL Server 2008 10.00.2531; SP1
47001/tcp open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  msrpc                Microsoft Windows RPC
49154/tcp open  msrpc                Microsoft Windows RPC
49155/tcp open  msrpc                Microsoft Windows RPC
49156/tcp open  msrpc                Microsoft Windows RPC
49157/tcp open  msrpc                Microsoft Windows RPC
49217/tcp open  msrpc                Microsoft Windows RPC
49218/tcp open  msrpc                Microsoft Windows RPC
52710/tcp open  ms-sql-s             Microsoft SQL Server vNext tech preview 14.00.1000
MAC Address: 00:50:56:9A:16:E9 (VMware)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.79 seconds
```

Fig 1: TCP port nmap scan of all known ports

There is a total of 65,535 ports and this nmap scan will find every open TCP port and the corresponding version for each open port. We can clearly see that there are many open ports. Most are for the msrpc service but there are quite a few others that can serve as a vulnerability.



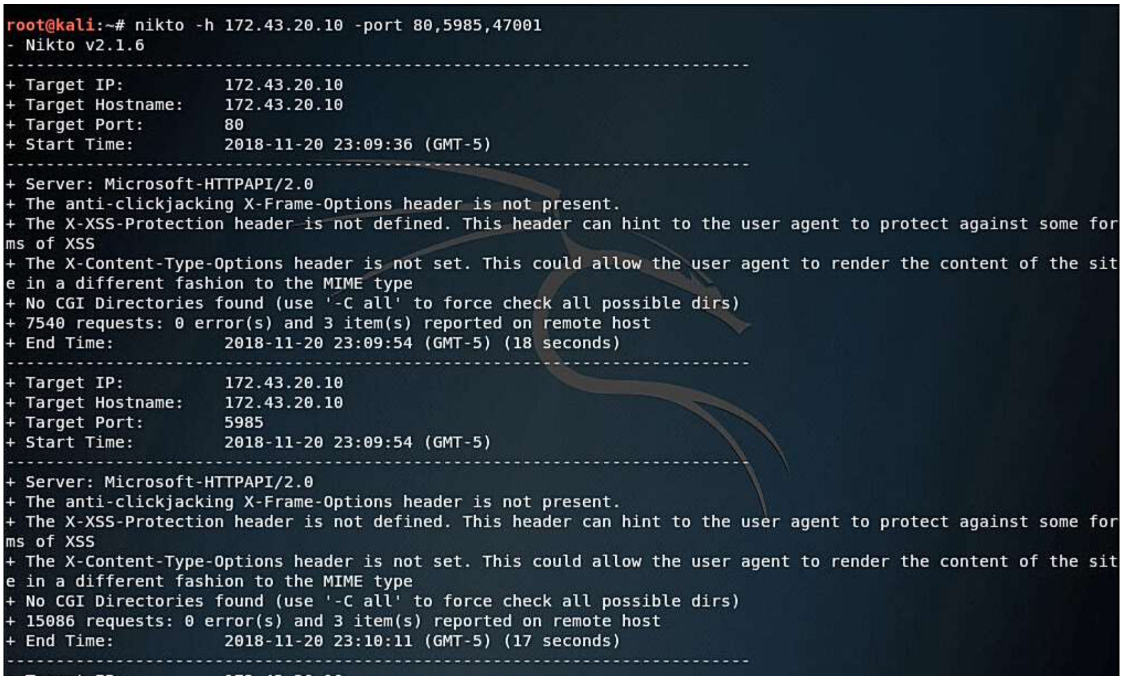
```
root@kali:~# nmap -sV -sU 172.43.20.10
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-20 23:41 EST
```

```
Nmap scan report for www.goodshopping.com (172.43.20.10)
Host is up (0.00059s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE       VERSION
137/udp  open          netbios-ns    Microsoft Windows Mobile netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
500/udp  open|filtered isakmp
3389/udp open|filtered ms-wbt-server
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:50:56:9A:16:E9 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1183.09 seconds
```

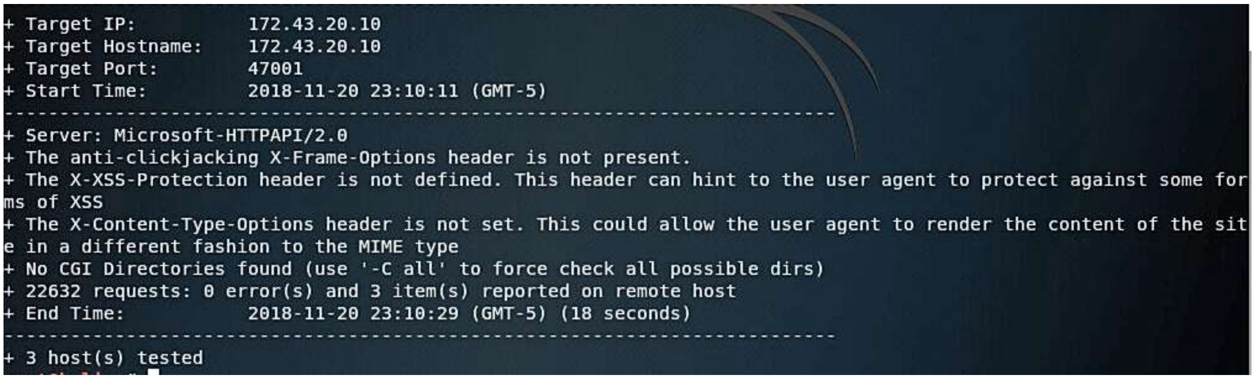
Fig 2: UDP port nmap scan

Since the first scan only looks for TCP open ports, another scan was conducted so only UDP open ports can be spotted. Now there are more open ports can could be possibly be used in an attack.

Nikto



```
root@kali:~# nikto -h 172.43.20.10 -port 80,5985,47001
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.43.20.10
+ Target Hostname:    172.43.20.10
+ Target Port:        80
+ Start Time:         2018-11-20 23:09:36 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7540 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2018-11-20 23:09:54 (GMT-5) (18 seconds)
---------------------------------------------------------------------------
+ Target IP:          172.43.20.10
+ Target Hostname:    172.43.20.10
+ Target Port:        5985
+ Start Time:         2018-11-20 23:09:54 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 15086 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2018-11-20 23:10:11 (GMT-5) (17 seconds)
---------------------------------------------------------------------------
```

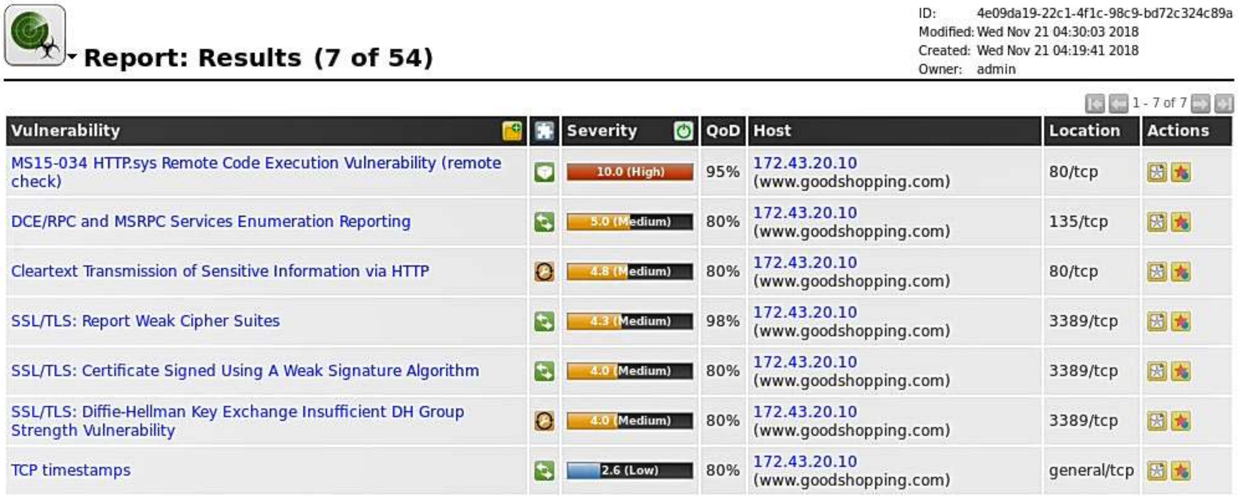


```
+ Target IP:          172.43.20.10
+ Target Hostname:    172.43.20.10
+ Target Port:        47001
+ Start Time:         2018-11-20 23:10:11 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 22632 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2018-11-20 23:10:29 (GMT-5) (18 seconds)
---------------------------------------------------------------------------
+ 3 host(s) tested
```

Fig 3: Nikto scan on port 80, 5985, 47001

The next scan that was used was Nikto which is used for web servers. From the open ports, we can see that there are three TCP open ports that have the HTTP service. These ports are 80, 5985, and 47001. This scan will show the server for these ports and any headers that are not present, defined, or set which can be a vulnerability.

OpenVAS



Report: Results (7 of 54)

ID: 4e09da19-22c1-4f1c-98c9-bd72c324c89a
Modified: Wed Nov 21 04:30:03 2018
Created: Wed Nov 21 04:19:41 2018
Owner: admin

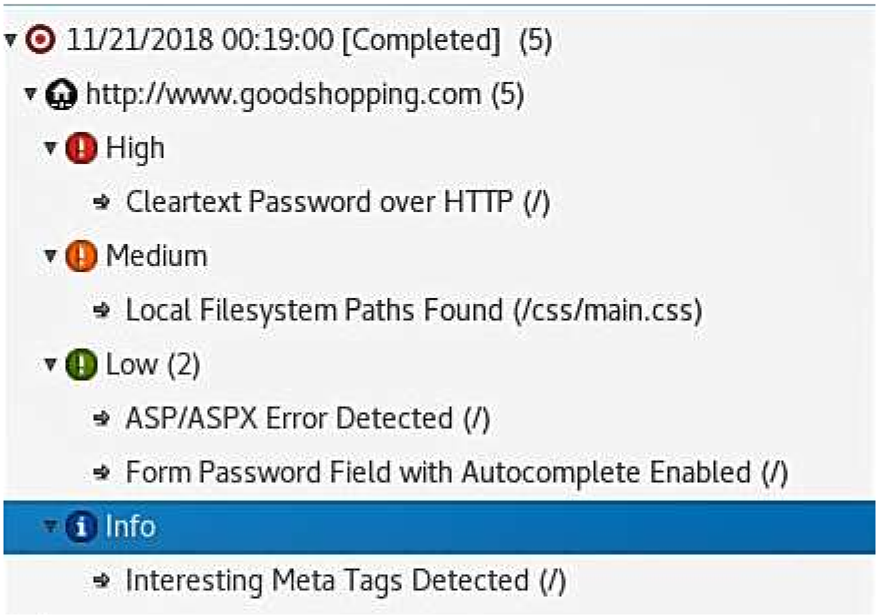
1 - 7 of 7

Vulnerability		Severity	QoD	Host	Location	Actions
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)		10.0 (High)	95%	172.43.20.10 (www.goodshopping.com)	80/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	172.43.20.10 (www.goodshopping.com)	135/tcp	
Cleartext Transmission of Sensitive Information via HTTP		4.8 (Medium)	80%	172.43.20.10 (www.goodshopping.com)	80/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	172.43.20.10 (www.goodshopping.com)	3389/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	172.43.20.10 (www.goodshopping.com)	3389/tcp	
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability		4.0 (Medium)	80%	172.43.20.10 (www.goodshopping.com)	3389/tcp	
TCP timestamps		2.6 (Low)	80%	172.43.20.10 (www.goodshopping.com)	general/tcp	

Fig 4: OpenVAS vulnerability report results

OpenVAS generates a report with many vulnerabilities and shows the severity, the ports involved, and actions that can be taken to combat the vulnerability. Section III will go into further detail on this.

Vega



- 11/21/2018 00:19:00 [Completed] (5)
  - http://www.goodshopping.com (5)
    - High
      - Cleartext Password over HTTP (/)
    - Medium
      - Local Filesystem Paths Found (/css/main.css)
    - Low (2)
      - ASP/ASPX Error Detected (/)
      - Form Password Field with Autocomplete Enabled (/)
    - Info
      - Interesting Meta Tags Detected (/)

Fig 5: Vega results

Last but not least, the Vega scanner was used as another source of finding vulnerability, specifically ones dealing with the web applications. The results will be explained in the next section.

III. Vulnerability Analysis

Analysis of Findings of each Tool

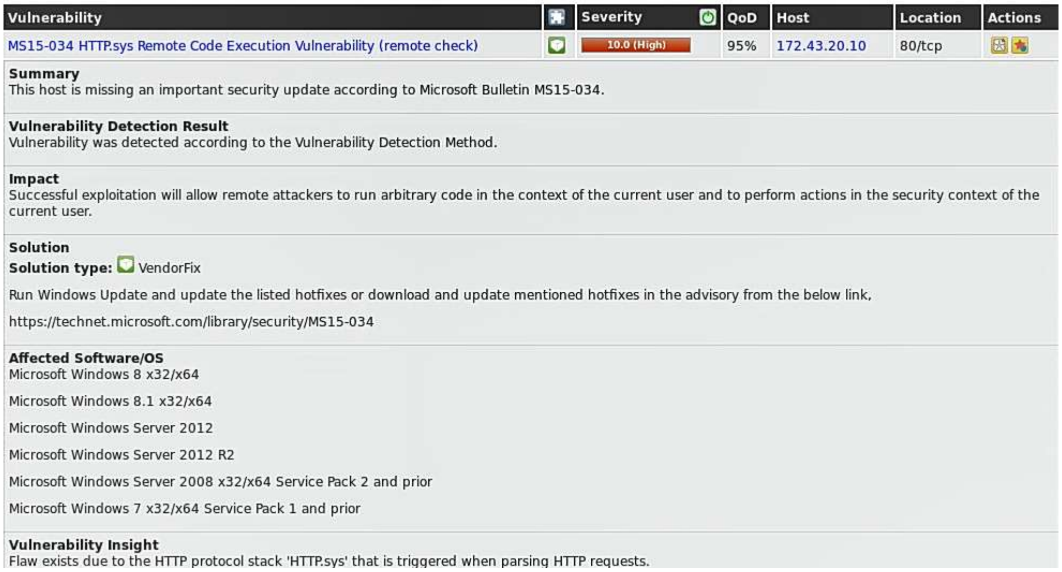
Nmap

First off, one thing to note is that the target is a Windows Server. This should be kept in mind especially during the penetration process. Also, the fact that port 21 for FTP is open means that we can possibly FTP into the server if we have the correct credentials. The HTTP service ports can be skipped for now since Nikto was used to look at those in-depth. Majority of the open ports are for Windows Microsoft RPC so this opening can be further researched using Rapid 7's vulnerability and exploit database to see if there is anything to use for exploitation.

Nikto

Nikto shows that each HTTP service port has anti-clickjacking X-Frame-Options header as not being present, X-XSS-Protection header as not being defined, and X-Content-Type-Options header as not being set. These headers can protect from clickjacking, cross-site scripting, and MIME sniffing. These vulnerabilities can be detrimental to the company so they should be addressed and fixed accordingly.

OpenVAS



Vulnerability		Severity	QoD	Host	Location	Actions
MS15-034 HTTP.sys Remote Code Execution Vulnerability (remote check)		10.0 (High)	95%	172.43.20.10	80/tcp	

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution
Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,

https://technet.microsoft.com/library/security/MS15-034

Affected Software/OS
Microsoft Windows 8 x32/x64

Microsoft Windows 8.1 x32/x64

Microsoft Windows Server 2012

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Fig 6: In-depth details of most severe vulnerability in OpenVAS

The #1 vulnerability for this IP address according to OpenVAS deals with a vulnerability on port 80. You can clearly see the dangers of this vulnerability since it allows remote attackers to run malicious code. Another vulnerability on port 80 is the fact that HTTP is being used. These sites are used by people to buy products and log in with their credentials. Transmitting sensitive data in cleartext can be easy pickings for a man-in-the-middle attack. Next on the list deals with port 135 and MSRPC. While this might not be a devastating attack, it can be used as a way for an attacker to get more information on the target which can work together with other exploits. The next 3 that are listed are on port 3389 and deal with weak cipher suites, weak signature algorithms, and weak key size. These vulnerabilities will serve as a weakness that make it easier for the attacker to decrypt communications. The last result deals with TCP as a whole since timestamps can be seen. These timestamps can be used to compute uptime.

Vega

Similarly to OpenVAS, Vega shows that cleartext passwords over HTTP is a vulnerability that shouldn't be ignored. After all, we wouldn't want the attackers to discretely be stealing sensitive information. A local filesystem path was also found by Vega. This could allow an attacker to understand filesystem layout which could be used in unison with other attacks. ASP/ASPX error message was detected which could give sensitive information. Lastly, the autocomplete attribute for passwords was not turned off so passwords could be stored locally which can be dangerous.

List of Vulnerabilities based on Priority and Solutions

High priority

1. HTTP.sys Remote Code Execution Vulnerability (spotted by OpenVAS)
   a. Solution: Windows Update and hotfixes provided by Microsoft for MS15-034
2. Cleartext Transmission of Sensitive Information via HTTP (spotted by OpenVAS and Vega)
   a. Solution: Make use of HTTPS and enforce transmission via an encrypted SSL/TLS connection
3. FTP open port 21 (spotted by nmap)
   a. Solution: Either prevent anyone from connecting via FTP or ensure that all usernames and passwords are unique and strong
4. Weak cipher suites, signature algorithm, and key size (spotted by OpenVAS)
   a. Solution: Use strong ciphers, use strong hashing algorithm instead of SHA-1, and use Elliptic-Curve Diffie-Hellman or something with 2048 or greater bit key size

Medium priority

1. DCE/RPC and MSRPC Services Enumeration Reporting (spotted by OpenVAS)

    a. Solution: Filter traffic going to any Microsoft Windows RPC ports

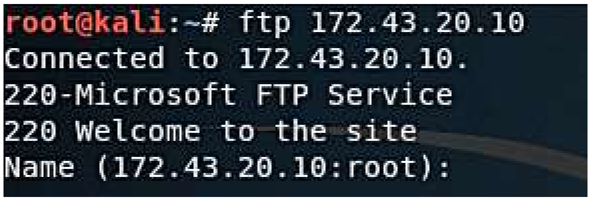
2. Heads not properly set, defined, or present (spotted by Nikto)
    a. Solution: should be set, defined, and present to prevent attacks
3. Local Filesystem Path Found (spotted by Vega)
    a. Solution: Set it so that output is sent to an error log that is visible for only system administrators and developers

Low priority

1. TCP timestamps (spotted by OpenVAS)
    a. Solution: try to disable TCP timestamps
2. ASP/ASPX Error Detected (spotted by Vega)
    a. Solution: disable such error messages for remote users
3. Form Password Field with Autocomplete Enabled (spotted by Vega)
    a. Solution: set to “off”

IV. Penetration of Target

Now we can observe the vulnerabilities that were listed above and attempt to break into the target in order to achieve our goal of accessing the server. As stated in the Executive Summary, our first point of access will be to getting in with an open port such as FTP or SSH. In this case, FTP is open so that will be used to our advantage. When we FTP to the IP address, we are required to enter a username and password.



```
root@kali:~# ftp 172.43.20.10
Connected to 172.43.20.10.
220-Microsoft FTP Service
220 Welcome to the site
Name (172.43.20.10:root):
```

Fig 7: result of FTPing into server

Since we were not given any credentials, some hunting must be done. If we take a look at the virtual machine of the server, we can already spot 2 things.

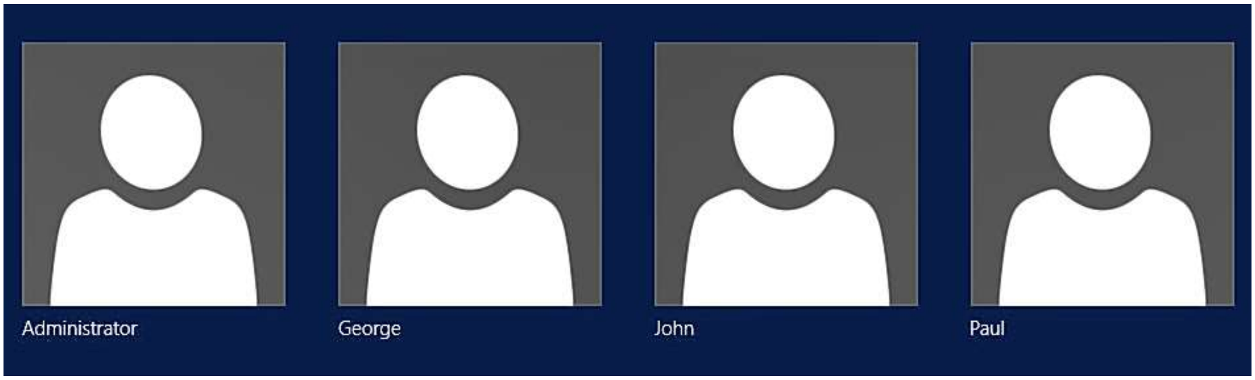
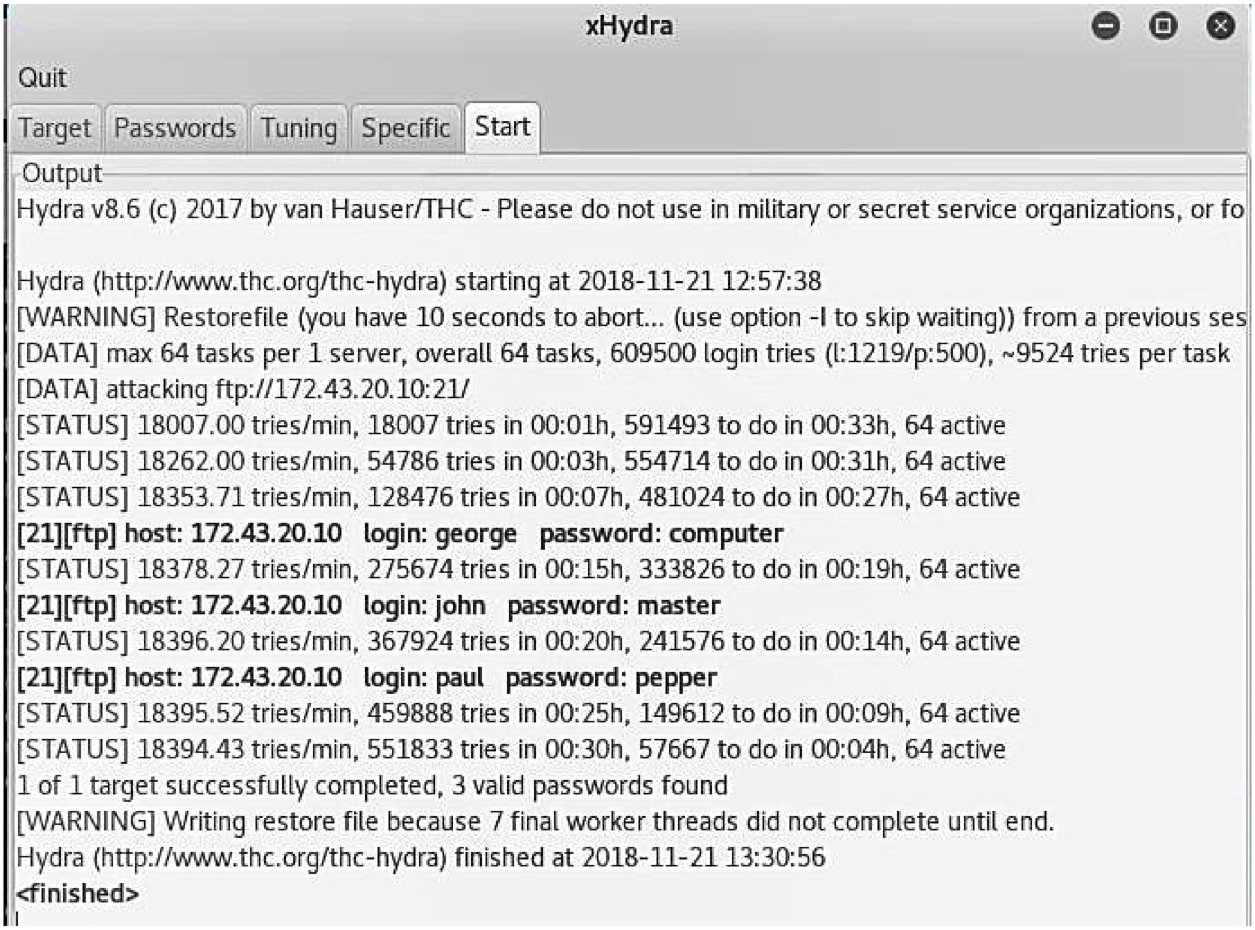


Fig 8: Usernames for server

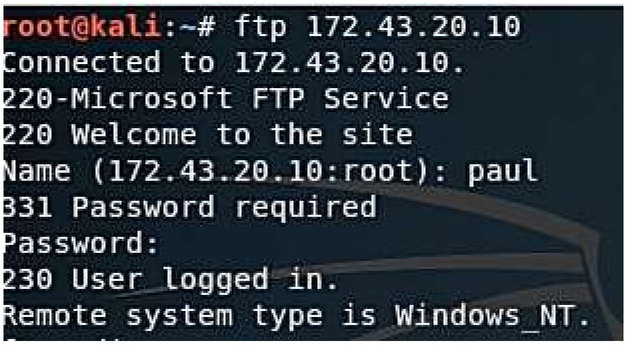
First thing is that there are 4 possible usernames: Administrator, George, John, and Paul. The second thing is that aside from Administrator, the other three are the first names of a person. With this in mind, I decided that a brute force can be possible. I created two custom word lists, one with a list of possible first names, and the other is a word list that is a shortened version of the rockyou.txt wordlist. I can now use Hydra using these two word lists.



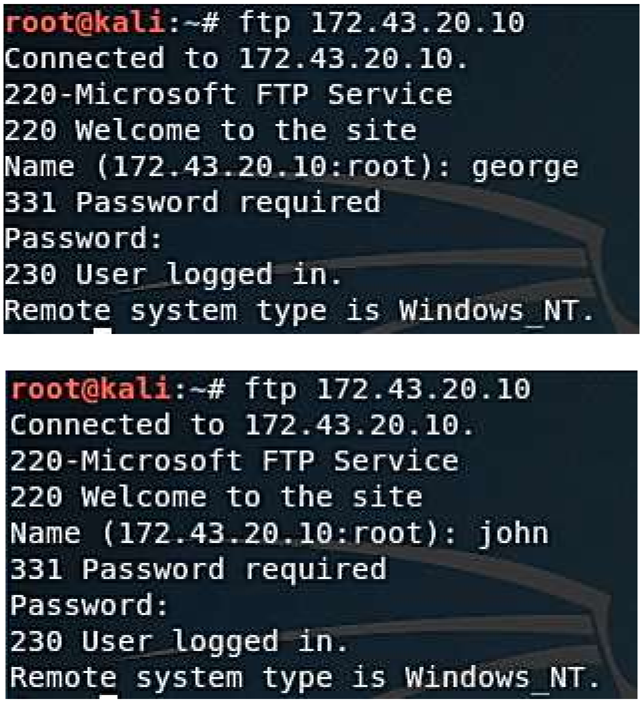
```
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or fo

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-21 12:57:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
[DATA] max 64 tasks per 1 server, overall 64 tasks, 609500 login tries (l:1219/p:500), ~9524 tries per task
[DATA] attacking ftp://172.43.20.10:21/
[STATUS] 18007.00 tries/min, 18007 tries in 00:01h, 591493 to do in 00:33h, 64 active
[STATUS] 18262.00 tries/min, 54786 tries in 00:03h, 554714 to do in 00:31h, 64 active
[STATUS] 18353.71 tries/min, 128476 tries in 00:07h, 481024 to do in 00:27h, 64 active
[21][ftp] host: 172.43.20.10   login: george   password: computer
[STATUS] 18378.27 tries/min, 275674 tries in 00:15h, 333826 to do in 00:19h, 64 active
[21][ftp] host: 172.43.20.10   login: john   password: master
[STATUS] 18396.20 tries/min, 367924 tries in 00:20h, 241576 to do in 00:14h, 64 active
[21][ftp] host: 172.43.20.10   login: paul   password: pepper
[STATUS] 18395.52 tries/min, 459888 tries in 00:25h, 149612 to do in 00:09h, 64 active
[STATUS] 18394.43 tries/min, 551833 tries in 00:30h, 57667 to do in 00:04h, 64 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 7 final worker threads did not complete until end.
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-21 13:30:56
<finished>
```

Fig 9: Result of using Hydra

From this tool, I successfully got ahold of the passwords for 3 of the 4 accounts. Now I can search around for any files that might seem interesting.



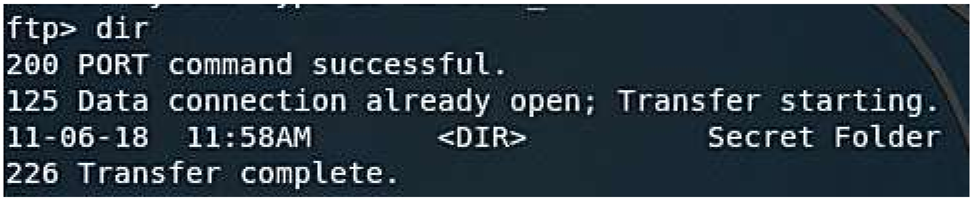
```
root@kali:~# ftp 172.43.20.10
Connected to 172.43.20.10.
220-Microsoft FTP Service
220 Welcome to the site
Name (172.43.20.10:root): paul
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
```



```
root@kali:~# ftp 172.43.20.10
Connected to 172.43.20.10.
220-Microsoft FTP Service
220 Welcome to the site
Name (172.43.20.10:root): george
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
```

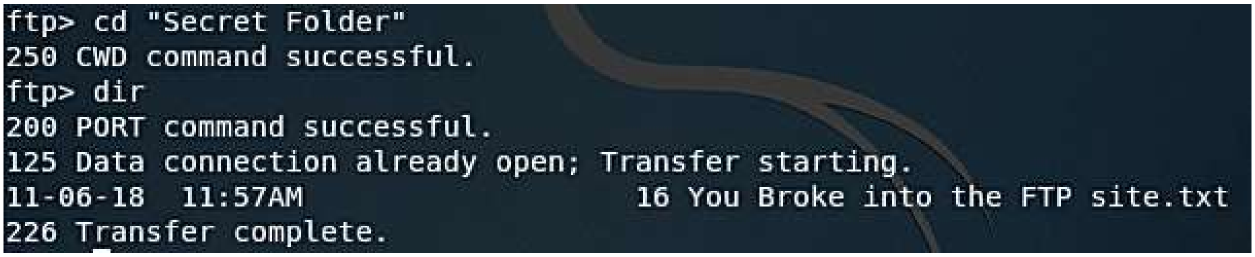
```
root@kali:~# ftp 172.43.20.10
Connected to 172.43.20.10.
220-Microsoft FTP Service
220 Welcome to the site
Name (172.43.20.10:root): john
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
```

Fig 10: Successfully logging with each username/password combination



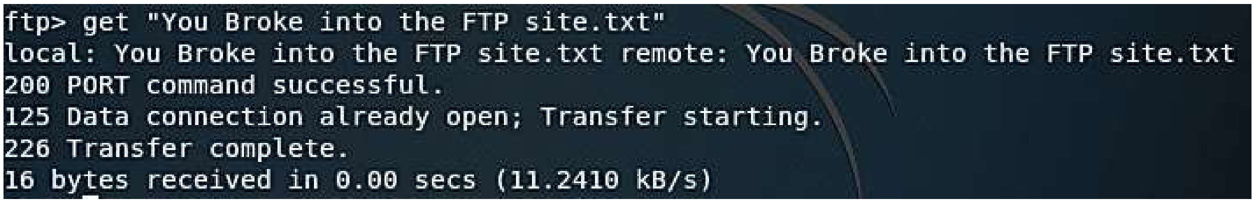
```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-06-18  11:58AM       <DIR>          Secret Folder
226 Transfer complete.
```

Fig 11: Dir command to see any directories or files



```
ftp> cd "Secret Folder"
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-06-18  11:57AM                   16 You Broke into the FTP site.txt
226 Transfer complete.
```

Fig 12: Going into directory and seeing a txt file

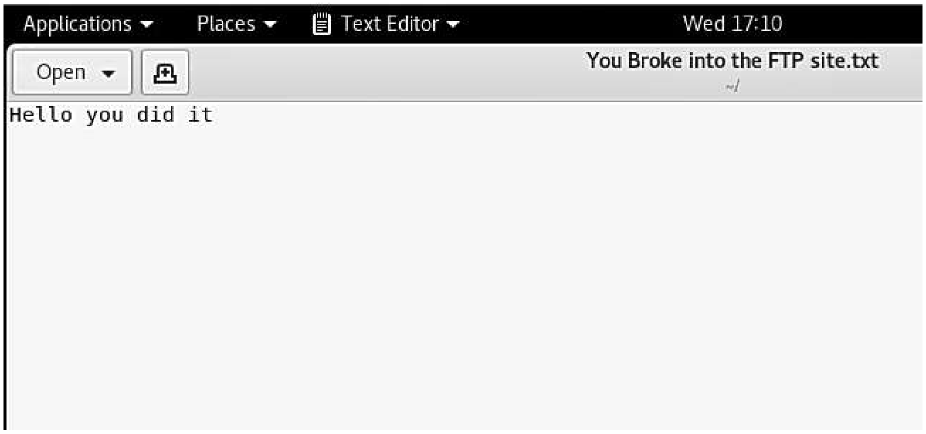


```
ftp> get "You Broke into the FTP site.txt"
local: You Broke into the FTP site.txt remote: You Broke into the FTP site.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
16 bytes received in 0.00 secs (11.2410 kB/s)
```

Fig 13: Using get command to bring txt file to my machine

I can see that there is a directory called "Secret Folder" and when I use cd to get into it, there is a txt file called "You Broke into the FTP site." I can use the get command to download the file onto my virtual machine.

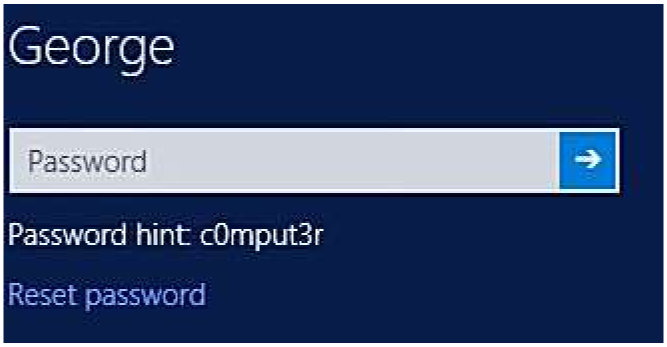
Fig 14: File on my Kali box



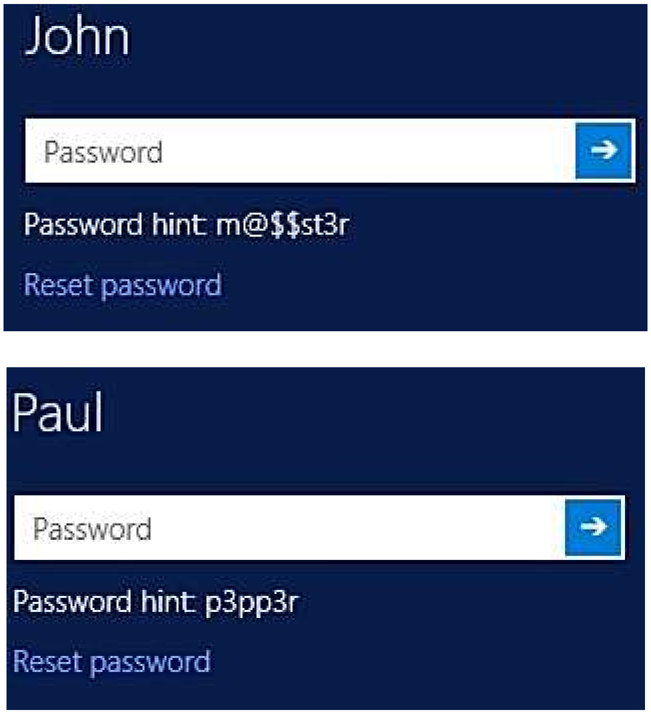
```
Hello you did it
```

Fig 15: When txt file is opened.

This penetration attempt was a success. I was able to get into the server, find information that I wanted, and transfer it back to my own machine.



Password hint: c0mput3r



John

Password

Password hint: m@$$st3r

Reset password

Paul

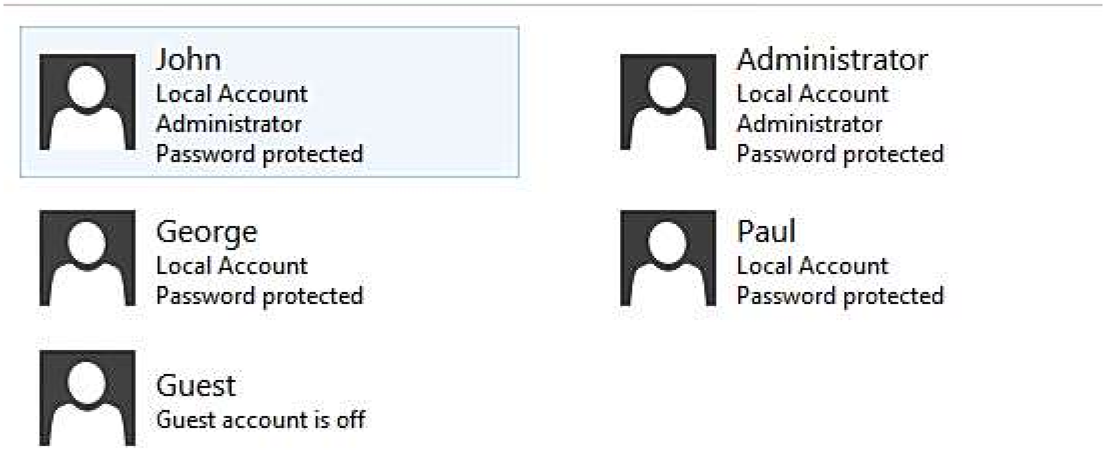
Password

Password hint: p3pp3r

Reset password

Fig 16: If server credentials are inputted incorrectly

One thing I noticed is that if someone were to put wrong passwords for any of these logins on the server, they are greeted with a password hint that is basically the password. This is extremely dangerous practice and should be avoided at all cost. The hint should be unique so that only the authorized user can understand. All-in-all, strong passwords, unique usernames, and unique passwords should be implemented.



John
Local Account
Administrator
Password protected

Administrator
Local Account
Administrator
Password protected

George
Local Account
Password protected

Paul
Local Account
Password protected

Guest
Guest account is off

Fig 17: Control Panel User Permissions

When I signed into the machine and went to user accounts in the control panel, I was able to see whether or not each user was an administrator or local account. So not only are the passwords easy to find but without doing any extra work, I can have administrator level privileges when signing into John.

V. Summary and Conclusion

Many possible vulnerabilities can be spotted just from doing a quick scan of what the open ports are. From those open ports, other tools were used to further understand how vulnerable these ports were. Nikto, OpenVAS, and Vega found vulnerabilities that ranged from code-related problems to weaknesses due to something being outdated. However, this does not spell doom for "Good Shopping." These vulnerabilities have been categorized based on severity and the solutions have been stated. I would recommend all of them to be addressed and fixed accordingly but that is up to the company to decide based on their resources. Updates and hotfixes provided by Microsoft should be continuously done on a regular basis to prevent easy-to-fix yet devastating vulnerabilities. Security must not be thought of lightly so utilizing strong encryption practices should be implemented. Some easy fixes include disabling, setting, and defining certain things just to ensure extra layer of security. I have attempted to break into the device and succeeded using FTP as an attack vector. Unique usernames and passwords should be enforced so my actions cannot be repeated by an unauthorized user. Having a username of a person's first name and a hint that essentially tells the exact password is a bad idea. A company dealing with customer credentials and payment information are especially at risk and should be careful. In conclusion, action must be taken so that the company can prosper without any security-related issues.