Penetration Test Report

for

DinoBank

Northeastern-1

Oct 12, 2019

Table of Contents

Table of Contents

Executive Summary

Northeastern-1 was tasked with evaluating the security of DinoBank's network. We were provided network access to three of the five subnets in scope with two subnets unaccessible directly. Our initial focus for the assessment was to identify as many exploitable machines as possible, but we also ended up evaluating points of sensitive information disclosure. Given that the company was aware of the testing taking place and given the time constraints, we decided to take an aggressive approach to discover as much as possible. One important thing to note was our discovery of a system running the file transfer protocol. We did not need special user privileges in order to read all of the files on that system. In addition, other potential vulnerabilities were discovered and elaborated on in the technical part of our report.

Overview of Penetration Testing Process

For the initial reconnaissance, Nmap was used to scan available ports on 10.0.1.0\24, 10.0.2.0\24, 10.0.10.0\24. With that, service identification, versions, operating system information were made available. All ports made visible by Nmap on the IP's inside the 10.0.2.0\24 subnet were only running OpenSSH. These could not be brute forced as they did not allow password authentication.

The first discovery we made was the FTP server on 10.0.1.12 that allowed anonymous access. Anyone could access this FTP server remotely. Additionally, all windows directory services allowed guest access. This could allow the enumeration of samba mounts.

Overview of Findings

The majority of our focus revolved around the 10.0.1.0/24 subnet, which contained the dinobank.us domain controller and exchange server. The most significant security risk we observed was through the Windows Update server located at 10.0.1.12. Filezilla was installed and configured to allow anonymous read access to the entire system. Through this entry point we were able to determine that the server was used to facilitate updates to the rest of the servers. Furthermore, we were able to confirm the existence of Splunk and Salt daemons used to manage the network.

Aside from local system access, we found that Filezilla allowed ftp proxy connections, or ftp bounces. This misconfiguration allows remote users to request connections to other hosts through the ftp server. Since Filezilla is installed on a server facilitating Windows Updates, it can be used to scan large segments of the internal network while staying hidden.

The Windows Update server did secure its web endpoints through SSL, but OpenVAS did report that many of the ciphers used were of insufficient strength or unsupported. While not immediately an issue, this can make it easier for attackers to intercept or hijack network traffic.

Several machines including the exchange server and update server permitted guest access to their samba services. This allowed us to retrieve the workgroup information and domain controller identifiers, allowing us to better identify potential targets. Using this information, we were able to successfully identify 10.0.1.50 as warehouse.dinobank.us and 10.0.1.20 as corp-exch-01.dinobank.us. On some servers, we were even able to pull shared folder names. Even if inaccessible, the amount of information we were able to disclose without authenticating was enough to be dangerous.

The exchange server on 10.0.1.20 also ran a large set of applications. Several RPC ports were exposed which would allow authenticated users to easily enumerate through configured users. Several SMTP ports were opened, allowing both unencrypted and encrypted sessions. Open relay tests were not run on the exchange server, and should be investigated in the future.

The 10.0.10.0/24 subnet covered another independent network that supported a remote branch with the prefix “gotham”. This network consisted of 2 workstations, 1 domain controller, 3 unknown Windows machines and 1 Ubuntu server. The Ubuntu server used Apache/PHP instance which ran a splash page for “Crusty Croissants”. This web application contained a function that allowed an unauthenticated user to edit the site source code. This allowed remote users to attack clients through cross-site scripting and gave them the ability to freely deface the site. The 6 computers appeared to be running no remote accessible services with the exception of RDP on the Windows computers.

The 10.0.11.0/24 and 10.0.12.0/24 subnets were inaccessible from our network. An attempt was made to scan them by using the Filezilla ‘bounce’ port scan vulnerability to gain scanning abilities in either subnet but failed to find anything in a timely manner.

Assessment Factor: Preventative Controls

Infrastructure Management – Status: Baseline

We found several services running on 10.0.1.20 ranging from SMTP to .NET APIs. Clustering of services increases the impact factor of vulnerabilities as a single attack can expose several different applications. By spreading services out, less information is lost as a result of a breach or loss of uptime. More restrictive networking policies should also be enforced to prevent network traversal. When properly enforced, attacks like the FTP proxy scan can not only be prevented, but detected and a proper response can be carried out quickly.

Access and Data Management – Status: Evolving

The Filezilla FTP vulnerabilities permitted unauthenticated read access to all files on the server. Under normal circumstances, this should not happen unless the user or program has administrator access. Proper steps should be taken to ensure that services are reduced to the smallest amount of permissions possible. For Filezilla, the removal of the anonymous user would be a good first step. For the remainder of the machines, disabling the guest account for Directory logins will easily hide much of the information we obtained.

Device/End-Point Security

On Gotham's internal network, there is an Ubuntu Linux server running Apache and PHP that facilitates the Crusty Croissant website. This website has a PHP application that allows unauthenticated clients read-write access to the site pages. While some sanitation is done to prevent server side modification, no checks are done against client scripting. This allows attackers to target site clients using Cross Site Scripting and similar variants. Open source tools like Beef XSS help facilitate attacks. Unauthenticated page modifiers should either be secured or removed from public facing sites to prevent attacks.

Assessment Factor: Detective Controls

Threat and Vulnerability Detection

During our tests many of our exploits, including the payloads, went undetected throughout the duration of the attack. Proper Antivirus programs can detect memory corruption or privilege escalation attempts. For web servers, Web Application Firewalls can detect both injection exploits and common payloads. Both methods immediately alert on-site administrators, further bolstering the defensive ability of the network.

Anomalous Activity Detection

If a proper Intrusion Detection System was deployed, many of our attacks would have been detected or failed before any damage could be done. With a reactive security team, successful breaches can be suppressed before an attacker can cause further damage. Snort is a good, open-source example that can be configured to cover a wide variety of services and can be configured to automatically block traffic or notify administrators.

Event Detection

There was very little in terms of logging on the network. Given that this was an authorized penetration test, we were able to access a large portion of the network with very little stealth in our information gathering. Tools such as OpenVAS, Nmap, DirBuster, and more were able to run without any automated measures to prevent further intrusion.

Assessment Factor: Corrective Controls

Technical Summary

Operating Systems Security Issues

Details of Findings

We found many operating systems that were a lower version, such as windows server 2008. it would be recommended to update to newer versions of windows server, either 2012 or to the newest version, 2019.

The Windows Update server was running Microsoft Server 2008. Recently, CVE 2019-0708 was disclosed that demonstrated how attacks on RDP could be executed without authenticating. Machines inside of the 10.0.1.0/24 subnet did not appear to employ any mitigations or updates needed to address the flaw, and almost every machine in this subnet had RDP enabled. However, we were unable to confirm its existence due to unknown factors in the environment. This vulnerability should be further investigated, or a remediation step should be taken as disclosed in the next section.

Recommendation and fixes

For CVE 2019-0708, security update KB4499180 was given for Microsoft Server 2008. This update can be downloaded from the Microsoft Windows Catalog and installed locally. If this update cannot be installed, RDP can be disabled or Network Level Authentication (NLA) can be required for RDP connections to be established.

Annexes

Nmap Scan Results – Linux server

10.0.1.33

```
Nmap 10.0.1.33 -sV -O
Nmap scan report for northeastern-t1-corp-corp-web-03.c.security-
competitions.internal (10.0.1.33)
Host is up (0.00018s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=10/12%OT=22%CT=1%CU=41687%PV=Y%DS=1%DC=I%G=Y%TM=5DA1F5
OS:EE%P=x86_64-pc-linux-gnu)SEQ(SP=FF%GCD=1%ISR=109%TI=Z%CI=Z%TS=A)SEQ(SP=F
OS:F%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M58CST11NW7%O2=M58CST11NW7%O3
OS:=M58CNNT11NW7%O4=M58CST11NW7%O5=M58CST11NW7%O6=M58CST11)WIN(W1=6E00%W2=6
OS:E00%W3=6E00%W4=6E00%W5=6E00%W6=6E00)ECN(R=Y%DF=Y%T=40%W=6EF0%O=M58CNNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

10.0.2.0\24

```
Nmap scan report for core-01.bank.dinobank.us (10.0.2.100)
Host is up (0.000067s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for bankweb-01.bank.dinobank.us (10.0.2.101)
Host is up (0.000063s latency).
Not shown: 999 closed ports
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for reports-01.bank.dinobank.us (10.0.2.103)
Host is up (0.000073s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for wires-01.bank.dinobank.us (10.0.2.200)
Host is up (0.000077s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

10.0.10.5

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-12 13:35 UTC
Nmap scan report for northeastern-t1-branch-gotham-gotham-bakery-01.c.security-
competitions.internal (10.0.10.5)
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http   Apache httpd 2.4.29 ((Ubuntu))
OS: Linux
```

Nmap Scan Results – Windows Servers

10.0.1.10

```
Nmap scan report for northeastern-t1-corp-corp-dc-01.c.security-
competitions.internal (10.0.1.10)
Host is up (0.00027s latency).
Not shown: 988 closed ports
PORT   STATE SERVICE       VERSION
53/tcp   open  domain?
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2019-10-12
19:49:41Z)
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
```

```
389/tcp  open  ldap       Microsoft Windows Active Directory LDAP (Domain:
dinobank.us, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
(workgroup: DINO)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap       Microsoft Windows Active Directory LDAP (Domain:
dinobank.us, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port53-TCP:V=7.80%I=7%D=10/12%Time=5DA22E59%P=x86_64-pc-linux-gnu%r(DNS
SF:VersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version
SF:\x04bind\0\0\x10\0\x03");
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/12%OT=53%CT=1%CU=37142%PV=Y%DS=1%DC=I%G=Y%TM=5DA22E
OS:E8%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS
OS:=A)OPS(O1=M58CNW8ST11%O2=M58CNW8ST11%O3=M58CNW8NNT11%O4=M58CNW8ST11%O5=M
OS:58CNW8ST11%O6=M58CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=20
OS:00)ECN(R=Y%DF=Y%T=80%W=2000%O=M58CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y
OS:%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0
OS:%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: CORP-DC-01; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.01 seconds
```

10.0.1.11

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-12 13:24 UTC
Nmap scan report for northeastern-t1-corp-corp-dfs-01.c.security-
competitions.internal (10.0.1.11)
Host is up (0.00031s latency).
```

```
Not shown: 995 closed ports
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  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
(workgroup: DINO)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8089/tcp open  ssl/http      Splunkd httpd
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/12%OT=135%CT=1%CU=41527%PV=Y%DS=1%DC=I%G=Y%TM=5DA1D
OS:425%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S%T
OS:S=A)OPS(O1=M58CNW8ST11%O2=M58CNW8ST11%O3=M58CNW8NNT11%O4=M58CNW8ST11%O5=
OS:M58CNW8ST11%O6=M58CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2
OS:000)ECN(R=Y%DF=Y%T=80%W=2000%O=M58CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=
OS:Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=
OS:0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U
OS:1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DF
OS:I=N%T=80%CD=Z)

Network Distance: 1 hop
Service Info: Host: CORP-DFS-01; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.88 seconds
```

10.0.1.12

```
PORT   STATE SERVICE VERSION
21/tcp   open  ftp FileZilla  0.9.60 beta
80/tcp   open  http Microsoft IIS httpd 10.0
135/tcp  open  msrpc Microsoft Windows RPC
139/tcp  open  netbios-ssn Microsoft netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8089/tcp open  unknown Splunkd httpd
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

10.0.1.20

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-12 15:01 UTC
Nmap scan report for northeastern-t1-corp-corp-exch-01.c.security-
competitions.internal (10.0.1.20)
Host is up (0.00013s latency).
Not shown: 974 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft Exchange smtpd
80/tcp   open  http          Microsoft IIS httpd 10.0
81/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  ssl/http      Microsoft IIS httpd 10.0
444/tcp  open  ssl/http      Microsoft IIS httpd 10.0
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
465/tcp  open  smtp          Microsoft Exchange smtpd
587/tcp  open  smtp          Microsoft Exchange smtpd
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
808/tcp  open  ccproxy-http?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
2525/tcp open  smtp          Microsoft Exchange smtpd
3389/tcp open  ms-wbt-server Microsoft Terminal Services
3800/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3801/tcp open  mc-nmf        .NET Message Framing
3828/tcp open  mc-nmf        .NET Message Framing
5060/tcp open  sip?
6001/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
6547/tcp open  msrpc         Microsoft Windows RPC
6789/tcp open  msrpc         Microsoft Windows RPC
7001/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: corp-exch-01.dinobank.us; OSs: Windows, Windows Server 2008 R2
- 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.35 seconds
```

10.0.1.50

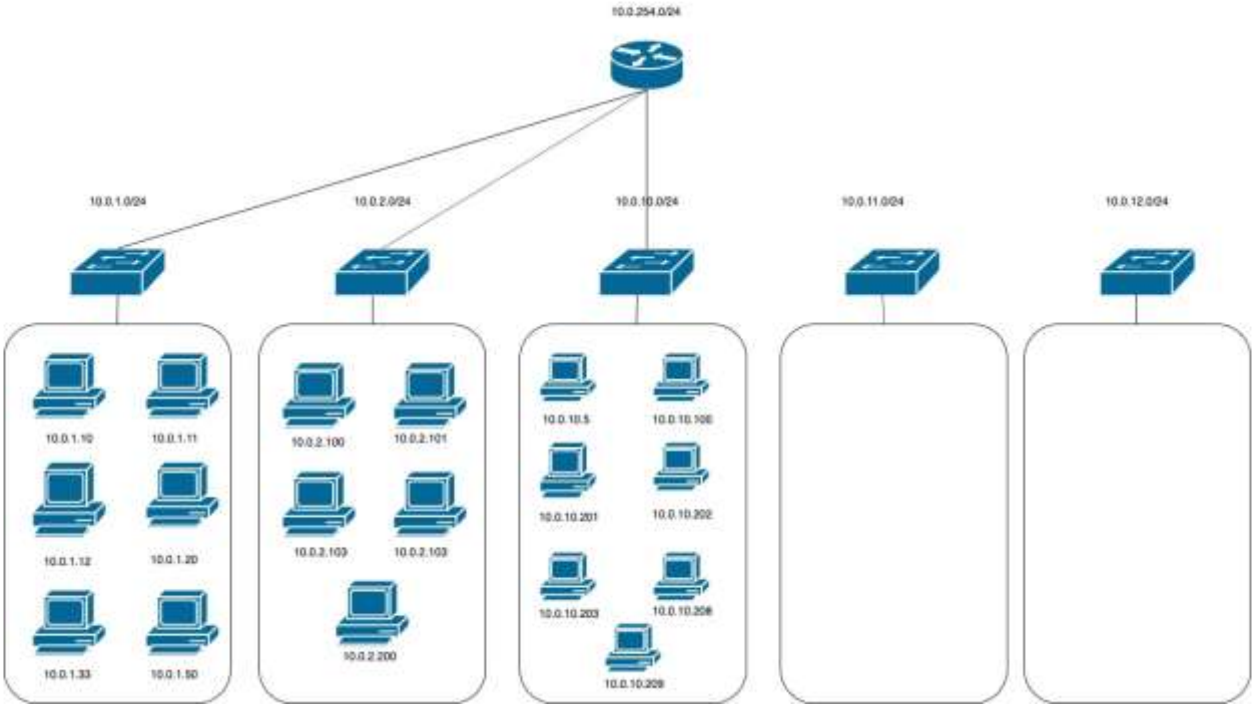
```
Nmap scan report for northeastern-t1-corp-warehouse.c.security-
competitions.internal (10.0.1.50)
Host is up (0.00022s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE       VERSION
135/tcp  open  msrpc      Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2016 Datacenter 14393 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=warehouse.dinobank.us
| Issuer: commonName=warehouse.dinobank.us
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-10-11T09:46:18
| Not valid after:  2020-04-11T09:46:18
| MD5:   94ee 9cd2 c0aa f9d8 d04a c8d9 ff3a ece8
|_SHA-1: 8b0c 9934 77b3 c4e2 ab47 b067 9f78 55e8 c4c8 2d97
|_ssl-date: 2019-10-12T19:50:04+00:00; 0s from scanner time.
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=10/12%OT=135%CT=1%CU=42450%PV=Y%DS=1%DC=T%G=Y%TM=5DA22
OS:E75%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=I%CI=I%TS=A)SEQ(SP
OS:=101%GCD=1%ISR=10A%TI=I%CI=RD%II=I%SS=S%TS=A)SEQ(SP=101%GCD=1%ISR=10A%TI
OS:=I%TS=A)OPS(O1=M58CNW8ST11%O2=M58CNW8ST11%O3=M58CNW8NNT11%O4=M58CNW8ST11
OS:%O5=M58CNW8ST11%O6=M58CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%
OS:W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M58CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y
OS:%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%
OS:O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=8
OS:0%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:Y%DFI=N%T=80%CD=Z)


|   OS: Windows Server 2016 Datacenter 14393 (Windows Server 2016 Datacenter 6.3)
|   Computer name: warehouse
|   NetBIOS computer name: WAREHOUSE\x00
|   Domain name: dinobank.us
|   Forest name: dinobank.us
|   FQDN: warehouse.dinobank.us
|_  System time: 2019-10-12T19:50:06+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-10-12 19:50:05
|_  start_date: 2019-10-12 09:46:18
TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   0.16 ms northeastern-t1-corp-warehouse.c.security-competitions.internal
(10.0.1.50)
```

10.0.10.100 - 10.0.10.209

```
Nmap scan report for northeastern-t1-branch-gotham-gotham-dc.c.security-
competitions.internal (10.0.10.100)
Host is up (0.000095s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for northeastern-t1-branch-gotham-gotham-tlr-01.c.security-
competitions.internal (10.0.10.201)
Host is up (0.000055s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap scan report for northeastern-t1-branch-gotham-gotham-tlr-02.c.security-
competitions.internal (10.0.10.202)
Host is up (0.000067s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for northeastern-t1-branch-gotham-gotham-tlr-03.c.security-
competitions.internal (10.0.10.203)
Host is up (0.00011s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap scan report for northeastern-t1-branch-gotham-gotham-wk-01.c.security-
competitions.internal (10.0.10.208)
Host is up (0.000062s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
8089/tcp open  unknown

Nmap scan report for northeastern-t1-branch-gotham-gotham-wk-02.c.security-
competitions.internal (10.0.10.209)
Host is up (0.000095s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
8089/tcp open  unknown



Nmap done: 256 IP addresses (7 hosts up) scanned in 5.18 seconds
```

Network Diagram


10.0.254.0/24
10.0.1.0/24
10.0.2.0/24
10.0.10.0/24
10.0.11.0/24
10.0.12.0/24
10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.20
10.0.1.33
10.0.1.50
10.0.2.100
10.0.2.101
10.0.2.103
10.0.2.103
10.0.2.200
10.0.10.5
10.0.10.100
10.0.10.201
10.0.10.202
10.0.10.203
10.0.10.208
10.0.10.209