

Executive Summary

Surface Analysis

Information

Penetration Test Report
for
DinoBank

Northeastern-1

Oct 12, 2019

Table of Contents

Table of Contents

Executive Summary	4
Overview of penetration testing process	5
Overview of FFIEC Cybersecurity Assessment Tool	6
Overview of findings	7
Assessment Factor: Preventative Controls	7
Infrastructure Management – Status: Baseline	7
Access and Data Management – Status: Evolving	7
Device/End-Point Security	7
Secure Coding	7
Assessment Factor: Detective Controls	7
Threat and Vulnerability Detection	7
Anomalous Activity Detection	7
Event Detection	7
Assessment Factor: Corrective Controls	7
Patch Management	7
Remediation	7
Technical Summary	8
Operating Systems Security issues	8
Details of findings	8
Recommendation and fixes	8
Annexes	9
Nessus scan results	9
Nmap scan results – Linux server	9
Nmap scan results – Windows server	9
Linux Firewall verification	9
Linux Apparmor verification	9
References	10

Executive Summary

While Northeastern-1 was tasked with investigating the security of the DinoBank network, we analyzed three subnets in particular. 10.0.1.0\24, 10.0.2.0\24, and 10.0.10.0\24. Although our original task was to investigate possible vulnerabilities in the network, we were instructed by Alex Faulkner to limit the analysis of 10.0.1.0\24 to all IPs except 10.0.1.250. Under the suggestion of Tom Dickson, we continued to analyze 10.0.1.250. What was discovered should, most likely, be investigated further by the appropriate authorities and may be going against the principles of DinoBank.

Overview of penetration testing process

- What was discovered from reconnaissance? How many IP's were there to break into to? What did it tell you about the IP's? Were there any blatantly obvious vulnerable OS's?
- Which IP's were you able to gain access to? Briefly explain what the vulnerability was and what you got from exploiting it? Did you brute force it?

Overview of FFIEC Cybersecurity Assessment Tool

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 entrypoint, 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

The 10.0.10.0/24 subnet covered another independent network that supported a remote branch with the prefix "gotham". This network consisted of 6 workstations and 1 Ubuntu server. The Ubuntu server ran an 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 workstations appeared to be running no remote accessible services with the exception of RDP.

Assessment Factor: Preventative Controls

Infrastructure Management – Status: Baseline

Blah blah blah

Access and Data Management – Status: Evolving

Blah blah blah

Device/End-Point Security

In the source code found on Alex's GitHub, there is a private key contained inside that is used to authenticate and secure https. If an attacker were to take the private key, they could use it in a Man In The Middle (MITM) Attack that will remove any ssl used. It is recommended that the RSA key be removed from the repo and make sure that the private key is regenerated on the website to ensure proper secrecy in the encryption.

Secure Coding

Assessment Factor: Detective Controls

Threat and Vulnerability Detection

Anomalous Activity Detection

Event Detection

Assessment Factor: Corrective Controls

Patch Management

Remediation

Technical Summary(conclusion)

Discuss the various issues discovered, in a very technical detail.

Operating Systems Security issues

Details of findings

Recommendation and fixes

Give specific details for recommendations to remediate the issues discussed in the previous subsection. For each issue discussed above, there should be an accompanying recommendation and/or fix.

Annexes

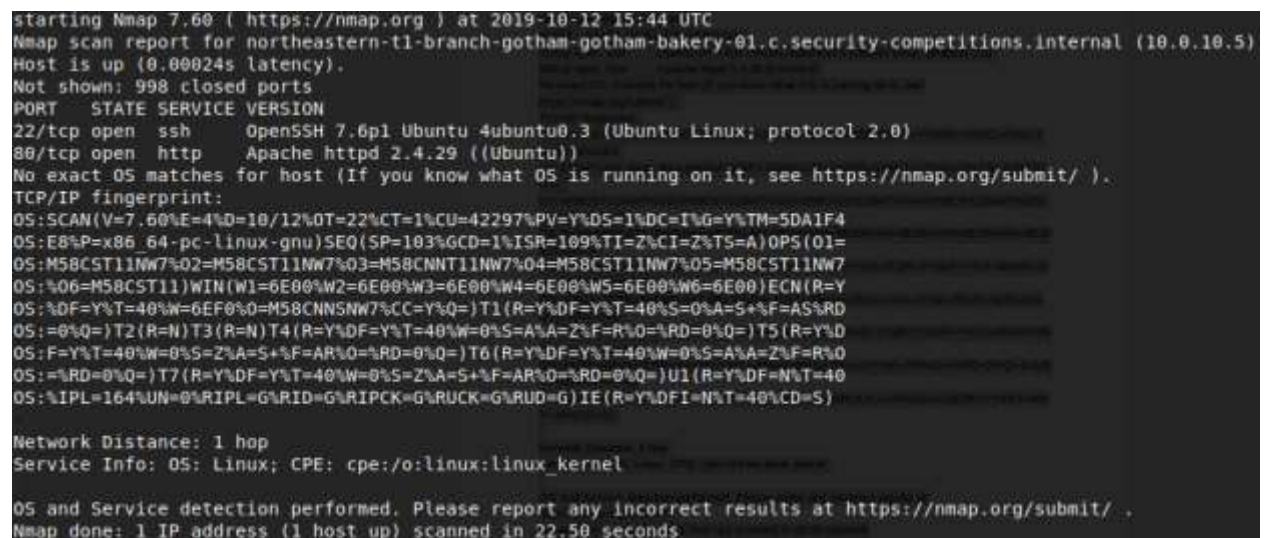
Annexes should be individually titled using the “Heading 2” format.

Nessus scan results

The “Summary” and “Details” section of the scan of both systems should be located here. This should display the breakdown of all vulnerabilities discovered by ranking, as well as the associated detail content of the Nessus report.

Nmap scan results – Linux server

A screencap of an Nmap scan of the Linux server, showing IP address and state of required services



```
starting Nmap 7.60 ( https://nmap.org ) at 2019-10-12 15:44 UTC
Nmap scan report for northeastern-t1-branch-gotham-gotham-bakery-01.c.security-competitions.internal (10.0.10.5)
Host is up (0.00024s 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=42297%PV=Y%D5=1%DC=I%G=Y%TM=5DA1F4
OS:E8%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=109%TI=Z%CI=Z%T5=A)OPS(O1=
OS:M58CST11NW7%O2=M58CST11NW7%O3=M58CST11NW7%O4=M58CST11NW7%O5=M58CST11NW7
OS:%O6=M58CST11)WIN(W1=6E00%W2=6E00%W3=6E00%W4=6E00%W5=6E00%W6=6E00)ECN(R=Y
OS:%DF=Y%T=40%W=6EF0%O=M58CST11NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD
OS:=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O
OS:=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40
OS:%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=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

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 22.50 seconds
```

Nmap scan results – Windows server

A screencap of an Nmap scan of the Windows server, showing IP address and state of required services

```

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-12 15:01 UTC
Nmap scan report for northeastern-tl-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
8080/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

```

Linux Firewall verification

A screencap of the default state of the INPUT chain, along with all rules contained in the chain

Linux Apparmor verification

A screencap of the Apparmor status of the Linux server

References

References should be in APA format