Example Exam Report

email:d.lassig@t-online.de

DAVID LASSIG

2018-05-26

Contents

Introduction

This reports holds all achievements and findings Pentester David was able of to find during the assessment for the EvilCorp Network. I was confronted with the exploit of multiple machines.

Objective

The objective of this assessment is to perform an internal penetration test against the EvilCorp network. The Pentester is tasked with following methodical approach in obtaining access to the objective goals.

```
A) Target IP: 192.168.100.1
--------------------------------------

Main Objectives:
- Get shell on machine
- Obtain Account of Domain Controller

B) Target IP: 192.168.100.2
--------------------------------------

Main Objectives:
- Get root shell access to machine
- Dump full Database
```

Report: High-Level Summary

David Lassig was tasked with performing an internal penetration test towards EvilCorp Network. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate EvilCorps internal netowrk. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to EvilCorp.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on EvilCorps network. When performing the attacks, I was able to gain access to multiple machines, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. All systems were successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- **Objective A)** - Got into 192.168.100.1 Windows Machine through outdated FTP Server.
- **Objective B)** - Got in 192.168.100.2 through misconfigured Apache Web Server.

Report: Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

Especially for the windows machines it should be avoided to use such old software versions (Windows Server 2003). The effort to patch these systems are much higher than migrate to newer windows machines.

Report: Methodologies

Procedure of Pentesting

I use tmux for getting a organised step-by-step pentesting environment. I have tmux multiple windows in my session. Every window holds only panes for specific tasks. Every of this named window hold multiple panes to do multiple tasks at the same time.

Report Format

I use Pandoc with a Latex template to generate my report. This gives me great flexibility. For terminal outputs, code and config files I use several color schemes for giving a quick classification. Hence we're working on multiple machines the same time this should give the reader a better understanding.

Attacker Machine Linux Prompt

```
root@kali:~#
```

Attacker Metasploit Prompt

```
msf >
```

Attacker Machine Windows Prompt

```
C:\Users\ADMINI~1\Desktop\Tools>
```

Victim Machine Linux Prompt

```
admin@victimlinux:~$
```

Victim Machine Windows Prompt

```
C:\Program Files\>
```

Report: Information Gathering

During this penetration test, I was tasked with exploiting the EvilCorp network. The specific IP addresses were:

Internal Network

Internal Local Subnet 192.168.100.0/24

- 192.168.100.1
- 192.168.100.2
- …

Report: Service Enumeration Summary

As it's very repetitive I will step over the first step of enumeration in the individual machine description. I did on every machine the same:

```
root@kali:~/exam# nmap -Pn -p- -vv <objective-ip> | tee
↪  nmap_<objective-ip>.txt
root@kali:~/exam# nmap -Pn sU -p- -vv <objective-ip> | tee
↪  nmap_<objective-ip>_udp.txt
```

I will step into more detailed enumeration by filtering these outputs.

Host	Ports	Suspicious
192.168.100.1	21	Windows FTP Server 5.0
	143	Netbios
	139	
	445	
192.168.100.2	80	Apache2 Webserver 2.3
	8080	webdav

Report: Machine Penetration

192.168.28.161

OS	Windows Server 2013
Network Name	dc.evilcorp.local
Access Exploit	Outdated Windows FTP Server

Information Gathering

Lorem Ipsum

Service Enumeration

Lorem Ipsum

nmap

Lorem Ipsum

FTP

Lorem Ipsum

Exploiting - Getting Access

Lorem Ipsum

Post Exploitation

Lorem Ipsum

192.168.100.2

OS	Linux Debian 5
Network Name	database.evilcorp.local
Access Exploit	RCE and LFI on Apache Web Server
Local Privilege Escalation	DirtyCow Exploit

Information Gathering

Lorem Ipsum

Service Enumeration

Lorem Ipsum

nmap

Lorem Ipsum

nikto

Lorem Ipsum

Exploiting - Getting Access

Lorem Ipsum

Internal Information Gathering

Lorem Ipsum

Download interesting files

Lorem Ipsum

Open command shell

Lorem Ipsum

File Transfer

Lorem Ipsum

Network Connections

Lorem Ipsum

Services

Lorem Ipsum

Exploiting - Local Privilege Escalation

Lorem Ipsum

Post Exploitation

Lorem Ipsum