PENETRATION TESTING ON METASPLOITABLE 3

PROJECT SYNOPSIS

BACHELOR OF TECHNOLOGY

(Computer Science & Engineering) 2018 Batch

Project In-charge

Er. Simarjot Kaur

Project Team Members

Simranjit Singh (1800920)

Sarpreet Singh (1800916)

Shubi Khjuria (1800918)

Sandeep Singh (1800914)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

BABA BANDA SINGH BAHADUR ENGINEERING COLLEGE, FATEHGARH SAHIB

CANDIDATE'S DECLARATION

We hereby declare that we have undertaken project at **ETHICAL HACKING**. The project entitled **PENETRATION TESTING ON METASPLOITABLE 3** in partial fulfillment of the requirement for the award of degree of the B. Tech. (Computer Science and Engineering) submitted in Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib is an authentic record of our work carried out during this semester. The matter presented in this project has not formed the basis for the award of any other degree, diploma, fellowship or any other similarities.

Project team members

SIMRANJIT SINGH

(University Roll No: 1800920, College Roll No: 181024)

SARPREET SINGH

(University Roll No: 1800916, College Roll No: 181001)

SANDEEP SINGH

(University Roll No: 1800914, College Roll No: 181147)

SHUBI KHJURIA

(University Roll No: 1800918, College Roll No: 181119)

Project In-charge

Er. SIMARJOT KAUR

INDEX

INTRODUCTION

Metasploitable3 is a free virtual machine that allows you to simulate attacks largely using Metasploit. It has been used by people in the security industry for a variety of reasons: such as training for network exploitation, exploit development, software testing, technical job interviews, sales demonstrations, or CTF.

Metasploitable2 back then was more of a test environment heavily for Metasploit. It was straight-forward to play, and it didn't take long to find the right exploit to use, and get a high privileged shell.First off, not every type of vulnerability on Metasploitable3 can be exploited with a single module from Metasploit, but some can. Also by default, the image is configured to make use of some mitigations from Windows, such as different permission settings and a firewall.

For example, if you manage to exploit a service in the beginning, you will most likely be rewarded with a lower privileged shell. This part shouldn't be too difficult for young bloods who are new to the game. But if you want more than that, higher privileged services tend to be protected by a firewall, and you must figure out how to get around that.

One very common thing about performing a penetration test is going after corporate data. Well, developers can't shove any real corporate data in Metasploitable3 without any legal trouble, therefore they have introduced flags throughout the whole system. They serve as "data you want to steal", and each is in the form of a poker card image of a Rapid7/Metasploit developer and is packaged in one of more of these ways:

- Obfuscation
- Strict permission settings
- File attributes

- Embedded files

LITERATURE SURVEY

2.1) Passive Reconnaissance

This is also known as Open Source Intelligence (OSINT) or simply Information Gathering, the idea behind passive reconnaissance is to gather information about a target using only publicly available resources.

Some references will assert that passive reconnaissance can involve browsing a target's website to view and download publicly available content whereas others will state that passive reconnaissance does not involve sending any packets whatsoever to the target site.

2.1.1) Types of passive reconnaissance

Passive Information Gathering: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.

Semi-passive Information Gathering: The goal for semi-passive information gathering is to profile the target with methods that would appear like normal Internet traffic and behavior. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, and we aren't searching for "unpublished" servers or directories. We aren't running network level port scans or crawlers and we are only looking at metadata in published documents and files; not actively seeking hidden content. The key here is not to draw attention to our activities. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.

Browsing web pages, reviewing available content, downloading posted documents or reviewing any other information that has been posted to the public domain would all be considered in-scope. It does not involve actions such as sending crafted payloads to test input validation filters, port scanning, vulnerability scanning, or other similar activities which would fall under the definition of active reconnaissance.

2.1.2) Scope and ROE

When we perform passive recon activities for a pentest or assessment we'll undoubtedly have an agreed upon target and scope Although all of the data is being gathered solely from the public domain without malicious intent, Following additional steps are taken to avoid exposing details of any discovered egregious vulnerabilities.

- First, as already stated, although a penetration test or security assessment would typically be scoped to a single or select few targets,
- Second, we'll be redacting identifying information that might disclose the exact location of a potentially damaging vulnerability or reveal a particular individual whose full name or contact information is inconsequential to understanding the demonstrated passive recon technique. Of course, the redaction doesn't completely de-identify the context of the discovery and it's still possible to determine what sites/organizations they belong to.
- Third, when appropriate/possible well be reporting discovered vulnerabilities to the respective organization for remediation. Again, any discovered vulnerabilities are already in the public domain for anyone to see, but I still felt an obligation as a security professional to have them remediated when possible.

Once again, none of these techniques involve maliciously scanning or probing a given website. All of this information has been gathered from the public domain using techniques and tools readily available to anyone. Also note that I use terms such as "attack" (e.g. "social engineering attack") throughout the post, but I am not at all suggesting malicious activity. Any active reconnaissance or testing activities should only be conducted within the scope of sanctioned penetration tests or security assessments

2.1.3) Tools used in Passive Reconnaissance Whois: This tools provides the where the site is located, who owns h ip block. Also there can be contacts listed.

- Nslookup: This tool provides the ip address of the target name address. This simply works on DNS queries.

- The-harvester: A python based tool that can be used to extract mail address on a domain by searching on Google and other social networking sites.

- Recong-ng: A gui tool for organizing and viewing all passive information gathering. Shodan: This site can give information about open ports and services on an internet device.

2.2) Active reconnaissance

Active reconnaissance involves actual integration with the target to get information about it .

This type of information gathering is more accurate than the the passive one . The only disadvantage is that it sometimes can damage the system and is more easy to be detected by the target machine. **2.2.1) hping3 tool**

This tool can craft packets at ip layer 3 and above [1]. This tool can be used to find the open ports on the target system. Perform small attacks on a target like smurf and land attacks.

Further this can be used to set tcp flags and do fuzzing on the target system .This tool is a command line tool and it can also perform idle scanning on target.

2.2.2)Scapy

This module is built in python and can be used to create custom packets at layer 2, layer3, layer 4 and other upper layers [2]. Further this tool can be combined with python to form scripts . This tool can be used to manually probe networks and identify the open ports and for banner grabbing.

2.3) Nmap

Nmap (*Network Mapper*) is a security scanner, originally written by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*) used to discover hosts and services on a computer network, thus building a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host(s) and then analyzes the responses.

The software provides a number of features for probing computer networks, including host discovery and service and operating-system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan. The Nmap user community continues to develop and refine the tool.

2.3.1)Nmap features:

- Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- Port scanning – Enumerating the open ports on target hosts [3].
- Version detection – Interrogating network services on remote devices to determine application name and version number.
- OS detection – Determining the operating system and hardware characteristics of network devices.
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

2.3.2)Typical uses of Nmap:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, and maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.

2.3.3) Nmap output format

- Interactive: This mode is interactive and it asks for users at times to enter various options and it is updated in realtime.
- XML: This format can be further processed by XML tools.It can be converted to a HTML report using XSLT.
- Normal: The output is seen when running Nmap from the command line,but saved to a file.
- Script Kiddie: Meant to be an amusing way to format the interactive output replacing letters with their visually alike number representations. For example, interesting ports be becomes Int3restIng pOrtz.

2.4) Metasploit

The **Metasploit Project** is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development [4].

Its best-known sub-project is the open source[2] **Metasploit Framework**, a tool for developing and executing exploit code against a remote target machine. Other important subprojects include the Opcode Database, shellcode archive and related research.

The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

2.4.1)Metasploit Framework

The basic steps for exploiting a system using the Framework include:

1. Choosing and configuring an *exploit* (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and Mac OS X systems are included);
2. Optionally checking whether the intended target system is susceptible to the chosen exploit;
3. Choosing and configuring a *payload* (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);
4. Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;
5. Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

Metasploit runs on Unix (including Linux and Mac OS X) and on Windows. The Metasploit Framework can be extended to use add-ons in multiple languages.

To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gleaned with port scanning and OS fingerprinting tools such as Nmap. Vulnerability scanners such as Nexpose, Nessus, and OpenVAS can detect target system vulnerabilities. Metasploit can import vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation.

2.4.2)Exploits

Metasploit currently has over 1613 exploits, organized in different categories like:

- Firefox is a collection of (mostly) remote code execution for this browser.
- Android and Apple's iOs are dedicated to mobile phone [5].
- Linux, Windows, BSD, Irix, Solaris, … are targeting specific operating systems
- Multi for exploits that aren't tied to a specific platform

2.4.3)Payloads

Metasploit currently has over 438 payloads. Some of them are:

- Command shell enables users to run collection scripts or run arbitrary commands against the host.

- Meterpreter enables users to control the screen of a device using VNC and to browse, upload and download files.

Dynamic payloads enables users to evade anti-virus defenses by generating unique payloads.

METHODOLOGY AND PLANNING OF WORK

The medothology of performing a penetration test contains the following phases:

Phase 1 - Reconnaissance

Reconnaissance is probably the longest phase, sometimes lasting weeks or months. The black hat uses a variety of sources to learn as much as possible about the target business and how it operates, including

- Internet searches
- Social engineering
- Dumpster diving
- Domain name management/search services
- Non-intrusive network scanning

The activities in this phase are not easy to defend against. Information about an organization finds its way to the Internet via various routes.

Phase 2 - Scanning

Once the attacker has enough information to understand how the business works and what information of value might be available, he or she begins the process of scanning perimeter and internal network devices looking for weaknesses, including

- Open ports
- Open services
- Vulnerable applications, including operating systems
- Weak protection of data in transit
- Make and model of each piece of LAN/WAN equipment

Phase 3 - Gaining Access

Gaining access to resources is the whole point of a modern-day attack. The usual goal is to either extract information of value to the attacker or use the network as a launch site for attacks against other targets. In either situation, the attacker must gain some level of access to one or more network devices.

Finally, encrypt highly sensitive information and protect keys. Even if network security is weak, scrambling information and denying attacker access to encryption keys is a good final defense when all other controls fail. But don't rely on encryption alone. There are other risks due to weak security, such as system unavailability or use of your network in the commission of a crime.

Phase 4 - Maintaining Access

Having gained access, an attacker must maintain access long enough to accomplish his or her objectives. Although an attacker reaching this phase has successfully circumvented your security controls, this phase can increase the attacker's vulnerability to detection.

Phase 5 – Covering Tracks

After achieving his or her objectives, the attacker typically takes steps to hide the intrusion and possible controls left behind for future visits. Again, in addition to anti-malware, personal firewalls, and host-based IPS solutions, deny business users local administrator access to desktops. Alert on any unusual activity, any activity not expected based on your knowledge of how the business works. To make this work, the security and network teams must have at least as much knowledge of the network as the attacker has obtained during the attack process.

FACILITIES REQUIRED

1. Laptop and an internet connection.
2. Metasploit Framework.
3. Metasploitable 3(Virtual Machine)

REFRENCES

- https://github.com/rapid7/metasploitable3
- https://blog.rapid7.com/2016/11/15/test-your-might-with-the-shiny-new-metasploitable3/
- https://www.hackingtutorials.org/metasploit-tutorials/setup-metasploitable-3-windows-10/
- https://www.offensive-security.com/metasploit-unleashed/requirements/