PAPER ON INFORMATION GATHERING TOOLS

I. Introduction

Dmitry is part of a subset of information gathering tools included in Kali Linux. The purpose of these tools is to help attackers identify information about a target, to assist with locating potential attack vectors that may work on the system. Dmitry is great for revealing information that exists through search engines about the owner and the host of a web page. This information can be really valuable for social engineering attacks as it provides the attacker with potential points of contact. It can also help the attacker seem more credible if they are able to give information about the web page or domain that the owner is using.

II. Ease of Use

Dmitry or Deepmagic Information Gathering Tool, is a command line utility included in Kali Linux. It is designed to allow a user to collect public information about a target host. It can be used to gather a number of valuable pieces of information such as:

- The whois details of a target host. This will provide information about a registered domain such as the name, address, and contact information of the person who registered it.
- The netcraft data for a target host. This can include details such as the operating systems , web server release and uptime information of a web host.
- A subdomain search of a target, which will locate any subdomains that exist on the main domain.
- A search of email addresses that exist on the domain

for you.

- A TCP scan of the target to reveal any open ports and services running on the server.

How Dmitry is used? :

To start , you can navigate to Dmitry through the main menu of kali Linux. Alternatively, you can also type "Dmitry" into the command line of kali Linux to see the the available options and help for the application. Once Dmitry is launched, you will be able to execute a command against a target in the following format

.

Dmitry [flags] [-t 0-9] [-o] target

Let's break down the command and discuss each of the options. Parameters that are in square brackets are optional, and only need to be included if the user wishes to have them. Dmitry has the following flags available:

1. –o: Allows the user to specify a location to write the output of the application to. If this parameter is not specified, the output is written to the command line window. This parameter must be the last one given, and must be followed by a file path.
2. –i: Performs a whois lookup on the IP address of the target. Use this option when you want to do a whois lookup, and want to use the IP instead of a domain name.
3. –w: Performs a whois lookup on the domain name of the host. Use this option when you want to do a whois lookup and want to use the domain name of a target instead of the IP.
4. –n: Retrieves all available Netcraft information for a given target.
5. –s: Does a search for all subdomains of a target.
6. –e: Does a search for all emails of a target domain.
7. –p: Performs a TCP port scan of the target.

WHOIS against IP addresses and hostnames

"Who-is" (as pronounced) is a protocol running on port TCP/43 that's used to query databases of ownership information regarding internet assets—such as domain names, autonomous systems, and internet protocol addresses block numbers.

Contrary to what one might think, IP addresses also have information regarding reverse pointer records about ownership and several other details (such as name servers), which could be obtained from WHOIS records.

While the truthfulness of this information depends on the owner of the IP range, we often find obsolete information that can be misleading. In some cases, however, it could also be treated as historical information that can be used for competitive advantage in case of a company's attack surface reduction endeavors (forgotten and vulnerable services come to mind).

DMitry, when used with the flag "**-i**", will query IP addresses to gather WHOIS information, and if you include a hostname it will solve the corresponding A record. After this, it will query the server and display information

Harvesting subdomains

An interesting feature included with this exploratory software is subdomain retrieval capability; it scraps the entire World Wide Web to search for possible hostnames within a certain specified registered name. This is possible by using the "**-s**" flag before the domain name:

Information Gathering means gathering different kind of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) tries to gather all the information about the target, in order to use it for Hacking. To obtain more relevant results, we have to gather more information about the target to increase the probability of a successful attack.There are so many tools which is as same as Dmitry and each tool has its own special feature.

NMAP and ZenMAP

NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP and ZenMAP are practically the same tool, however NMAP uses command line while ZenMAP has a GUI.

NMAP is a free utility tool for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

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

How it works? :

Step 1 − To open, go to Applications → 01-Information Gathering → nmap or zenmap.

Step 2 − The next step is to detect the OS type/version of the target host. Based on the help indicated by NMAP, the parameter of OS type/version detection is variable "-O".

The command that we will use is –

```
nmap -O 192.168.1.101
```

Step 3 − Next, open the TCP and UDP ports. To scan all the TCP ports based on NMAP.

The command that we will use is –

```
nmap -p 1-65535 -T4  192.168.1.101
```

Where the parameter "–p" indicates all the TCP ports that have to be scanned. In this case, we are scanning all the ports and "-T4" is the speed of scanning at which NMAP has to run.

Stealth Scan

Stealth scan or SYN is also known as **half-open scan**, as it doesn't complete the TCP three-way handshake. A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it is assumed the port isn't active or is closed.

The command that we will use is –

```
nmap -sS -T4 192.168.1.101
```

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyzes the responses in order to produce the desired results. It could even be used for host discovery, operating system detection, or scanning for open ports. It is one of the most popular reconnaissance tools.

Zenmap: It is another useful tool for the scanning phase of Ethical Hacking in Kali Linux. It uses the Graphical User Interface. It is a great tool for network discovery and security auditing. It does the same functions as that of the Nmap tool or in other words, it is the graphical Interface version of the Nmap tool. It uses command line Interface. It is a free utility tool for network discovery and security auditing. Tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime are considered really useful by systems and network administrators.

Discussion

These tools are of same use that is to gather the information. Dmitry tool main purpose is to extract information about a target website.

Nmap- ("Network Mapper") is a free and open source utility for network exploration and security auditing.

Many systems and network administrators also find it useful for tasks such as network inventory, managing service

upgrade schedules, and monitoring host or service uptime. Nmap uses 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. Nmap runs on all

major computer operating systems, and both console and graphical versions are available [8].

Unicornscan- It is an open source (GPL) tool designed to assist with information gathering and security auditing.

It is an attempt at a User-end Distributed TCP/IP stack for information gathering and their interrelation. It provides a superior interface for introducing a stimulus into and measuring a response from a TCP/IP enabled devices. The various

features of this scanner includes asynchronous stateless TCP scanning with all variations of TCP flags, asynchronous stateless banner grabbing, and active/passive remote OS and component identification by analysing responses [13]. It provides Scalable, Accurate, and Efficient system scan. It is released for the community to use under the terms of the GPL license [14].

Dmitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. Dmitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible sub domains, email addresses, uptime information, tcp port scan, whois lookups, and more.

Conclusion

Penetration testing is one of the most efficient approaches for the process of security assessment. It can accurately examine the effectiveness of security measures implemented on the system being inspected. With a wide variety of supporting tools available in the market, it is confusing for practitioners to make proper informed decisions when looking for suitable tools. The research aims to provide the community more reliable references regarding the tools' effectiveness by carrying out an evaluation on the performance of some particular tools. The experiment results have indicated that nmap is more powerful than the other selected tools owing to broad coverage, easy to use interface, fairly fast response time and highest number of detected open ports. Information gathering is an art that every penetration-tester (pen-tester) and hacker should master for a better experience in penetration testing. It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learnability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Whois, nslookup that can help hackers to gather user information. This step is very important because while performing attacks on any target information (such as his pet name, best friend's name, his age, or phone number to perform password guessing attacks(brute force) or other kinds of attacks) is required.

REFERENCES

[1] Geeksforgeeks.*org)*

[2] Tutorialspoint.com

[3] Researchgate.net

[4] Networkworld.com