**“Social Engineering: The art of Human Hacking”**

**Table of Contents:**

*Introduction…………………………………………………...(1)*

*Tools for Footprinting:………………………………………(1-2)*

1. *whois………………………………………………….(1-2)*
2. *nslookup……………………………………………...(2)*
3. *dig…………………………………………………….(2)*
4. *whatweb……………………………………………..(2)*
5. *theHarvester………………………………………..(2-3)*
6. *p0f……………………………………………………(3)*
7. *recon-ng…………………………………………….(3)*

*What is Social Engineering?……………………………...(3-4)*

*Types of Social Engineering………………………………(4)*

*Insider Attack……………………………………………….(4)*

1. *Human Based Social Engineering………………(4)*
2. *Phishing……………………………………(4-5)*
3. *Piggybacking ……………………………...(5)*
4. *Baiting………………………………………(5)*
5. *Vishing……………………………………....(5)*
6. *Computer Based Social Engineering…………….(5)*
7. *Mobile Based Social Engineering………………..(5)*

*Citations………………………………………………………(6)*

Daniel Rao

Feb 22nd, 2021

Vince Skinner

**Social Engineering: The art of Human Hacking**

**Introduction**

The process for pentesting for any ethical hacker starts from its root which is the ‘Reconnaissance‘ Layer. The reconnaissance in simple words stands for gathering of intelligence or data to conduct a successful pentest to a company. The more data we have as an ethical hacker, the better will be able to understand the flow and structure of an organization to break into the system.

This brings us to another word which is ‘Footprinting’. In the world of ethical hacking footprinting simply stands for, gathering of computer systems and entities they belong to.

To use this method a hacker might use various tricks and technologies.This type of information is quite important for the hacker to break into the system. As mentioned by greycampus, Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected. (greycampus)

In this paper I am going to discuss some of the tools that a hacker might use to gather some intelligence along with some of the social engineering tools used for the reconnaissance step.

**Tools for Footprinting :**

Some of the widely used tools for footprinting are:

1. **whois:** This tool gives the information about the domain registration of a particular organization. This tool provides some of the general information about the organization like email address , phone number and that how many DNS servers the organization has .To use this tool the user simply has to put this command into the terminal:

Whois <domain name>

Eg. whois micrposoft.com

1. **nslookup:** This tool is normally used to query the DNS/ Domain Name server. It provides all the ip addresses owned by a particular organization.

Usage:

nslookup <domain name>

Eg. nslookup microsoft.com

1. **dig:** dig is a very similar tool to nslookup, along with its usage, except that it’s a little more descriptive.
2. **whatweb:** It's a very informative tool that gives information about the organization website. For example it can tell us about if the website is using jquery along with its version number, or wordpress.

Usage:

whatweb <domain name>

1. **theHarvester:**  grabs the ips, host name, sub domains, email addresses and positions of employees in the company or organization.

Usage:

theHarvester -d <domain name>

theHarvester -d <domain name> -l <limit result> -b <source> -f <resultFile>

Another most common tool is called **sublist3r** which is also called sublister. This tool uses the same approach as that of the Harvester to gather intelligence about the organization. The total will be able to obtain total unique sub domains of an organization.

It can be installed on the Kali Linux using the command given below:

apt-get install sublist3r

1. **P0f:** Running this command on the terminal**,** it starts listening to the traffic of the host by the attacker. The attacker can possibly see how the traffic looks like as the internet is being accessed.

Usage:

P0f **Or** P0f -i <interface>

Example:

P0f -i eth0

1. **recon-ng:** This tool is able to gather information that is publicly available information from the internet. It has several modules that can be used to obtain vulnerabilities of websites and information about the organization website.

**What is Social Engineering?**

So now that we know some of these tools, their purposes along with their use lets try to understand what exactly is social Engineering?

If we put it in simpler words it is the most powerful attacking tool. It often requires no equipment or technology, and often minimal expense. Only proper awareness and education can prevent it and even then, the errors in judgement can still be exploited,

**Social engineering is the art of convincing people to reveal confidential information.** Social Engineering often depends on the fact that people are unaware of their valuable information and are careless about protecting their confidential data.

**Types of Social Engineering Attack:**

**Insider Attack:** An insider is an employee who has access to critical assets of an organization. An insider attack involves using privileged access to intentionally violate rules or cause threat to the organization’s information or e information systems in any form. These attacks are usually performed by disgruntled employee, terminated employee, third party, untrained staff etc. One of the reasons can be financial gain, revenge, becoming a competitor or performing competitor bidding.

As mentioned in one of the articles, “Social engineering has proven to be a very successful way for a criminal to "get inside" your organization. Once a social engineer has a trusted employee's password, he can simply log in and snoop around for sensitive data. With an access card or code in order to physically get inside a facility, the criminal can access data, steal assets or even harm people” (Fruhlinger). Below are some of the general and famously used social engineering attacks:

1. **Human Based Social Engineering (Gathering information by interaction):**

Impersonation, Vishing, Shoulder surfing, Reverse social engineering, dumpster diving, piggybacking, tailgating & Eavesdropping.

1. **Phishing:** Phishing is the leading form of social engineering attack. It is usually in the form of an email, chat, web ad, or website that has been designed by the attacker to impersonate a system, person or an organization. Phishing messages are usually crafted to deliver a sense of urgency of fear with the end goal of capturing the end user sensitive data.
2. **Piggybacking:** Which is also called tailgating, is when an unauthorized person physically follows an authorized person into a restricted corporate area or system.
3. **Baiting:** This is similar to phishing, which involves offering something enticing to an end user in an exchange for user login and password.
4. **Vishing:** Voice phishing is in which an attacker uses voice technology to trick individuals revealing their financial and personal information and use it for gain.
5. **Computer based Social Engineering (using computer tools or scripts):**

Phishing, Spam mail, pop-up window attack, Instant Chat Messenger, Hoax Letters, Chain Letters.

1. **Mobile based Social Engineering (Help of mobile application):**

Publishing malicious apps, repacking legitimate apps, using Fake security applications, Smishing (SMS Phishing)

*One of the famous tools that is used in Kali Linux is the Social Engineering toolkit found in the Social Engineering tools.*

**Citations:**

Fruhlinger, J. (2019, September 25). Social engineering explained: How criminals exploit human behavior. Retrieved February 23, 2021, from <https://www.csoonline.com/article/2124681/what-is-social-engineering.html>

Greycampus. (n.d.). Retrieved February 23, 2021, from https://www.greycampus.com/opencampus/ethical-hacking/what-is-footprinting