Reconnaissance

Module #15

Reconnaissance : Definition

The term Reconnaissance by definition comes from the military warfare strategy of exploring beyond the area occupied by friendly forces to gain information about the enemy for future analysis or attack.

Reconnaissance of computer systems is similar in nature, meaning typically a Penetration Tester or hacker will attempt to learn as much as possible about a target's environment and system traits prior to launching an attack.

This is also known as establishing a Footprint of a target. Reconnaissance is typically passive in nature and in many cases not illegal to perform as long as you don't complete a three-way handshake with an unauthorized system

Reconnaissance : Examples

Examples of Reconnaissance include anything from researching a target on public sources such as Google, monitoring employee activity to learn operation patterns, and scanning networks or systems to gather information, such as manufacture type, operating system, and open communication ports.

The more information that can be gathered about a target brings a better chance of identifying the easiest and fastest method to achieve a penetration goal, as well as best method to avoid existing security.

Also, alerting a target will most likely cause certain attack avenues to close as a reaction to preparing for an attack. Kali's official slogan says this best: "The quieter you become, the more you are able to hear"

Reconnaissance : Services

Reconnaissance services should include heavy documentation, because data found may be relevant at a later point in the penetration exercise. Clients will also want to know how specific data was obtained, and ask for references to resources.

Examples are what tools were used to obtain the data or what public facing resources; for example, the specific search query in Google that was submitted to obtain the data. Informing a customer "you obtained the goal" isn't good enough, because the purpose of a Penetration Test is to identify weakness for future repairs.

Reconnaissance : Objectives

- **Target background**: What is the focus of the target's business?
- **Target's associates**: Who are the business partners, vendors, and customers?
- **Target's investment in security**: Are security policies advertised? What is the potential investment security, and user security awareness?
- **Target's business and security policies**: How does the business operate? Where are the potential weaknesses in operation?
- **Target's people**: What type of people work there? How can they become your asset for the attack?
- **Define targets**: What are the lowest hanging fruit targets? What should be avoided?
- **Target's network**: How do the people and devices communicate on the network?
- **Target's defenses**: What type of security is in place? Where is it located?
- **Target's technologies**: What technologies are used for e-mail, network traffic, storing information, authentication, and so on? Are they vulnerable?

Reconnaissance : Initial research

Reconnaissance should begin with learning as much as possible about people and business associated with the target.

Sun Tzu is credited with the phrase, "know your enemy" in the book, “The Art of War”. As a Penetration Tester, you need to know your target. If your target happens to be a website, you should look at all aspects of that website.

It will give you a better understanding of how the site is maintained and run. Great Reconnaissance returns more possible vulnerabilities.

Reconnaissance : Initial research (Contd)

It is scary how much information is available on public sources. Some of the shocking unimaginable details that have been found:

a) classified documents,

b) passwords,

c) vulnerability reports,

d) access to security cameras.

Many Penetration Testing project objectives start with leveraging information off public sources.

Reconnaissance : Info from Company Website

There is a lot of valuable information that can be obtained from a target's website.

Most corporate websites list their executive team, public figures, and members from recruiting and human resource contacts. These can become targets for other search efforts and social engineering attacks.

Reconnaissance : Regional Internet Registries (RIRs)

Look at: www.arin.net

Network	
Net Range	50.76.50.112 - 50.76.50.127
CIDR	50.76.50.112/28
Name	FACEBOOK
Handle	NET-50-76-50-112-1
Parent	CBC-SFBA-17 (NET-50-76-32-0-1)
Net Type	Reassigned
Origin AS	
Customer	FACEBOOK (C03029402)
Registration Date	2012-06-10
Last Updated	2013-12-09
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-50-76-50-112-1
See Also	Upstream network's resource POC records.
See Also	Upstream organization's POC records.
See Also	Related delegations.

Reconnaissance : Web History Sources

Wayback Machine @ archive.org:

Collects older version of the target website, e.g. outdated organizational charts, phone numbers, customer intelligence, systems information listed in fields, such as view source or /robots.txt , older business partnerships, vulnerabilities fixed in later versions, and other useful data

It is important to understand that the publicly available information is hard to remove completely, making historical sources a valuable place for Reconnaissance research.

Reconnaissance : Web History Sources

Look at: https://archive.org/web/

Reconnaissance : Social media engineering

HUGE cache of information available in different social media sites in today's internet:

Facebook.com

Youtube.com

Linkedin.com

Twitter.com

Instagram

Etc. etc.

Look at www.shodan.io for getting any hw/sw resource details in Internet that is available

Thank You