Footprinting

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.[1]

When used in the computer security lexicon, "Footprinting" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neotrace.[2]

Contents

Techniques used for Footprinting

- DNS queries
- Network enumeration
- Network queries
- Operating system identification
- Organizational queries
- Ping sweeps
- Point of contact queries
- Port Scanning
- Registrar queries (WHOIS queries)
- SNMP queries
- World Wide Web spidering
- ((net work edit)) wifi

Software used for Footprinting to get entity information

Wireshark

Uses of Footprinting

It allows a hacker to gain information about the target system or network. This information can be used to carry out attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed in order to get a complete and successful resolution of the attack. Footprinting is also used by ethical hackers and penetration testers to find security flaws and vulnerabilities within their own company's network before a malicious hacker does.[3]

Types of Footprinting

There are two types of Footprinting that can be used: active Footprinting and passive Footprinting. Active Footprinting is the process of using tools and techniques, such as performing a ping sweep or using the traceroute command, to gather information on a target. Active Footprinting can trigger a target's Intrusion Detection System (IDS) and may be logged, and thus requires a level of stealth to successfully do.[4] Passive Footprinting is the process of gathering information on a target by innocuous, or, passive, means. Browsing the target's website, visiting social media profiles of employees, searching for the website on WHOIS, and performing a Google search of the target are all ways of passive Footprinting. Passive Footprinting is the stealthier method since it will not trigger a target's IDS or otherwise alert the target of information being gathered.[5]

Crawling

Crawling is the process of surfing the internet to get the required information about the target. The sites surfed can include the target's website, blogs and social networks. The information obtained by this method will be helpful in other methods.

WHOIS

WHOIS[6] is a web application used to get information about the target website, such as the administrator's e-mail address and details about the registration. WHOIS is a very large database and contains information of approximately all clearnet websites. It can be searched by domain name. [7][8]

Search engines

Search engines such as Google can also be used to gather information about the target system. It depends on how well one knows how to use search engines to collect information. If used properly, the attacker can gather much information about a company, its career, its policies, etc.

Traceroute

Information can also be gathered using the command Tracert ("traceroute"), which is used to trace a path between a user and the target system on the networks. That way it becomes clear where a request is being forwarded and through which devices. In Linux systems, the tracepath and traceroute commands are also

available for doing traceroute operations.[9]

Negative web search

Negative web search will reveal some other websites when performed on the target website. Negative websites can act as resources for insight about the flaws of the target website.[10]

Information to be Gathered

If the attack is to be performed on a company, then the following information will be gathered.

- Company details, employee details and their email addresses.
- Relation with other companies.
- Project details involving other companies.
- Legal documents of the company.
- News relating company website.
- Patents and trademarks regarding that particular company.
- Important dates regarding new projects.[11]

See also

- Digital footprint
- Network Security

References

1. "What is footprinting? - Definition from WhatIs.com" (http://searchsecurity.techtarget.com/definition/footprinting). *SearchSecurity*. Retrieved 2016-06-09.
2. "FootPrinting-First Step Of Ethical Hacking" (http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html). *Ehacking.net*.
3. Hendricks, Beth. "What is Footprinting? - Definition, Uses & Process" (https://study.com/academy/lesson/what-is-footprinting-definition-uses-process.html). *Study.com*. Retrieved 23 January 2020.
4. Lazari, Chris. "Ethical Hacking Reconnaissance Plan: Active Footprinting" (https://chrislazari.com/ethical-hacking-reconnaissance-plan-active-footprinting/). *chrislazari.com*. Retrieved 23 January 2020.
5. Lazari, Chris. "Ethical Hacking Reconnaissance Plan: Passive Footprinting" (https://chrislazari.com/ethical-hacking-passive-footprinting/). *chrislazari.com*. Retrieved 23 January 2020.
6. http://www.whois.sc/
7. "What is Whois? - Definition from Techopedia" (https://www.techopedia.com/definition/2469/whois). *Techopedia.com*. Retrieved 2016-06-09.
8. "Whois Definition from PC Magazine Encyclopedia" (https://www.pcmag.com/encyclopedia/term/54442/whois). *www.pcmag.com*. Retrieved 2016-06-09.
9. "Footprinting and scanning tools" (https://home.ubalt.edu/abento/753/footscan/footscantools.html). *home.ubalt.edu*. Retrieved 2016-06-09.
10. "Negative web search" (https://teachmehacking.com/footprinting-reconnaissance-techniques/). *teachmehacking*. Retrieved 1 September 2017.

11. "Information to be gathered" (http://www.dummies.com/programming/networking/how-to-use-footprinting-to-plan-an-ethical-hack/). *dummies*. Retrieved 25 August 2017.
