Footprinting: Techniques, Tools and Countermeasures for Footprinting

Article *in* Journal of Critical Reviews · July 2020

DOI: 10.31838/jcr.07.11.311

CITATIONS
3

READS
15,111

4 authors, including:

N. Suresh Kumar
GITAM (Deemed to be University)
66 PUBLICATIONS **225** CITATIONS

SEE PROFILE

JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 11, 2020

Footprinting: Techniques, Tools and Countermeasures for Footprinting

[1]Shruti Shreya, [2]N. Suresh Kumar, [3]Konda Srinivasa Rao, *[4]Bheesetty Srinivasa Rao

[123]Department of Computer Science and Engineering, GITAM Institute of Technology, Visakhapatnam

*[4]Department of Computer Science, GITAM Institute of Science, Visakhapatnam

nskgitam2009@gmail.com

Received: 22 March 2020 Revised and Accepted: l6 May 2020

Abstract: The business organizers allow the ethical hackers to go deep in the network to reach the target area to identify the flaws in the network. Footprinting is one of the ethical hacking tool helps many organizations and companies to analyse and detect their network vulnerabilities and the loopholes for security breach. Footprinting is one of the approachable tools for hackers to reach them close to the target area and get the target information for cyber-attacks. Many different tools are existing to help the hackers inorder to alert the organization about the vulnerabilities in the network.

keywords: Footprinting, Ethical hacking, vulnerabilities, attacking

I. Introduction

Footprinting is one of the methods applied to retrieve the information about the target system. Footprinting technology mostly speaks of phases at pre-attacks at the network. The Footprinting usually gathers network related information such as Network ID, domain name along with internal domain name, access control mechanisms, IP address, protocols, VPNs, permissions, user and group information, routing tables, system banners, press releases and news articles, remote system types, web server links etc. If the attacker gathers the sensitive information they may use the data for fraud, creating the fake profiles, etc. The attacker by gathering more similar type of information related to target interests and activities, the attacker can join several other social media and groups which further leads further Footprinting [1][2].

According to the functioning Footprinting is mainly categorised into two types. One is active and the second one is passive foot printing. In real time applications, there exists different Footprinting technologies like spam Footprinting, email Footprinting, Website Footprinting etc. The information gathered by different types of Footprinting tools such as traceroute, Whois lookup, Nmap tool, etc. Out of which Nmap is one of the regularly used tool to gather service and host information on the network. Zenmap is a security scanner officially used as supporting GUI for Nmap. The Zenmap is easy to install and to use by the users. The Zenmap is an open source freely available application[4].

Traceroute is one of the techniques which is used to track the packet information that is moving between different IP addresses. It provides the packet information such as response time to a ping, IP address, and host name. The above two techniques Nmap and traceroute are most widely used tools inorder to gather the network information. In order to protect the data the user need to monitor some countermeasures while using Footprinting [5].

Footprting is one of the key stages applied in Ethical hacking. Footprinting is one of the point in investigation phase of ethical hacking, where the attacker gathers system information. Hence, doing the Footprinting the technique provides the system or application information in reconnaissance phase, hence it explore the path in prior to know the attacking techniques and loop hole in the area of attack [6]. It narrow down the possible impact of attacking space. Monitoring and knowing about the information about the system and application program is important to the ethical hackers for analyse the techniques and suitable vulnerabilities types are impacting. The Footprinting can be implemented in two methods; they are active and passive Footprinting [7][8].

i. Active Footprinting: In active Footprinting the hackers directly interacts with the system or application to gather the information about the system. In the case of active Footprinting there is a high possibility that the target system saves the information such as IP address

ii. Passive Footprinting: In this technique the hackers can collect system or application information without interacting with the system directly. Here, the search engines or public records help the hacker in collecting the information from the system.

II Information Gathering

Now-a-days information is available on different platforms and the attackers are always tries to collect the confidential and private information of the users. In the sense, the user's personal information is gathered from social sites like Facebook, Twitter, etc. Similarly, the share values, company profiles, relationships, patents, formulas, and many policy details are targeted in many cases. Hence, it advisable to be cautious before get attacked. Before get attacked, it is very use-full to get the information about the scope of attacking technique and area of attack. Several techniques of Footprinting discussed in the following sections.

i. Footprinting through Search Engine: In general, the search engines like Google chrome, Bing, and yahoo are the best tools in collecting the information about the entity for which the user searching. The search engines gather different types of information via internet. The cache and archives in the system saves all the sensitive data. This is where the place is, the attackers get the information about the history or pattern of the browsing data. This will help the attackers to hack the user's personal information and social data.

The attacker collects organizational official information, restricted private data, website data, and etc. The attacker can also gather physical location of the system, different services like Netcraft as shown in figure 1, and other online information from online search engines. There are some financial search engines such as google, yahoo etc., through which the attacker may get financial information of the target system. Hence, it is possible just by knowing the targeted organization information the attacker can know the financial information of the targeted system.

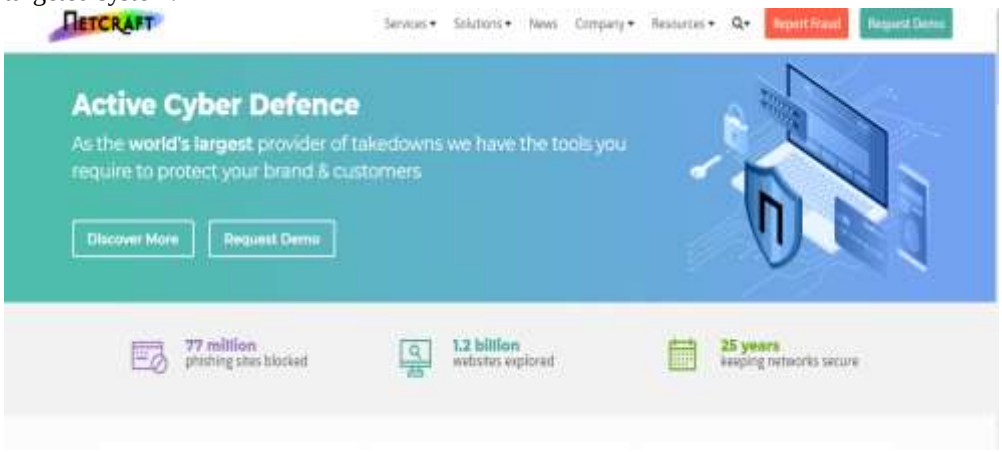

Figure 1: A tool for Website Footprinting

ii. Footprinting through Job sites: Most of the companies recruit their staff by posting vacancy details and company information on several job sites like linkedIn, naukari.com, monster.com and etc. The information contains location, contact information, job requirement, salary, hardware and software details. The fake job sites can collect individual targeted personal information. Similarly groups, forums, blogs, and communities contain sensitive information and there is chance of theft with sensitive information.

iii. Footprinting using Advanced Google Hacking Techniques: The hackers use search engine creatively to gather sensitive information. For instance, the use of google search engine to retrieve the information is named as google hacking. The following are few commands effectively used in google search engine inorder to retrieve the targeted information; 'filetype' derives the type of file which the hacker wants to search; for instance 'site' help in accessing the web site after colon; 'link' helps to identify the search page; 'cache' identifies the version of the webpage using; 'intitle' retrieves a word from the title of the document; 'inurl' searches for a word from an Unified Resource Locator (URL).

iv: Footprinting through social engineering: Social engineering is one of the art of retrieving one's personal information such as date of birth, credit card numbers, usernames, NetworkId, passwords, personal identification numbers, and their social interaction. In the view of security issues, Footprinting through social engineering can permit the attacker to go in deep individual social life. The impact of such Footprinting is catastrophic.

There are some basic social engineering tools effectively used in Footprinting, such as phishing, dumpster diving, eavesdropping, and shoulder surfing.

ISSN- 2394-5125 VOL 7, ISSUE 11, 2020

a. Phising: In the phising, emails will be sent to targeted system or systems containing message which looks authentic. As it looks authentic and legitimate the user tries to open the link present in the message body. Once the user clicks the link, it executes the background programs and retrieve all the sensitive information such as usernames and passwords and redirected to fake addresses.
b. Dumpster: It is one of the oldest social engineering technique gathers information from the target system trash. For instance attacker collects monthly bills, financial information, and other sensitive information from trash.

c. Eavesdropping: In this process the attacker collects all the information be listening conversation surreptitiously. It is one of the social engineering where the attacker gathers all information by listening, reading, accessing documents from the target system without any intimation or notification.
d. Shoulder surfing: The attacker hide back to the target system and gathers private information when the target user is dealing with the sensitive information. The attacker can gather information such as username, password, one time passwords, credit card details and other details.
v. WHOIS Footprinting: Thhe WHOIS Footprinting shown in figure 2 retrieves the information such as Domain names, IP address, Netblock data, Domain Name Server, and etc. Grographical regions which are outside the countries or regions maintains the Regional Internet Registers (RIR). The RIRs maintain the database for WHOIS. The RIRs such as LACNIC (Latin American and Caribbean Internet Addresses Registry), and APNIC (Asia Pacific Network Information Centre) maintains the database.
For instance, an URL contains the information regarding domain name and host name. Then the Internet Corporation for Assigned Names and Numbers (ICANN) ensures that only single company holds that particular domain name. The ICANN ensures that by having unique registration of domain names. For instance, the North America RIR of static IP addresses is maintained by ARINA (American Registry for Internet Numbers). The WHOIS tool queries the registration database for gathering the domain related information.

Figure 2: WHO is tool for Footprinting

vi. Footprinting through Social Networking: It is found that popular social sites are easy to vulnerable and it is quite easy to get to know about the basic personal information of the users. The arrackers can get one's sensitive information through some social sites such as LinkedIn, Facebook, Twitter, etc. Attackers apply social engineering techniques to gather sensitive information for fraud and hacking. The basic personal information may contain like a photo, name, address of the target person.
vii. Website Footprinting: It gathers the information related to organizations website to hack the background softwares. The background information such as version, Script Information, Operating System, data bases, last updated, sub-directories, connection type, etc., can be collected from targeted organization. There are several online services available to gather such information for instance Website informer, Zaproxy, Firebug, BurpSuite and many other. By getting details like last update and status the attacker can gather target information such as their file structure, source code, etc.
Mirroring a website is processing of downloading an image of a website. Form downloading the target website on the local system has many advantages like analysing vulnerabilities. The process can be used to gather information such as structure of directories, HTML files and other server files into local system.

ISSN- 2394-5125 VOL 7, ISSUE 11, 2020

viii. Competitive Intelligence: Competitive Intelligence is a process of gathering information related to competitors in non-interfacing mode. The method gathers in different sorces such as official websites, press releases, advertisings, reviews, annual reports, catalogues, etc. The competitive information can be gathered with Business wire as shown in figure 3, EDGAR, Lexis Nexis, and CNBC. These tools gathers information such as website statics, daily visited the page, user analytics and many more.

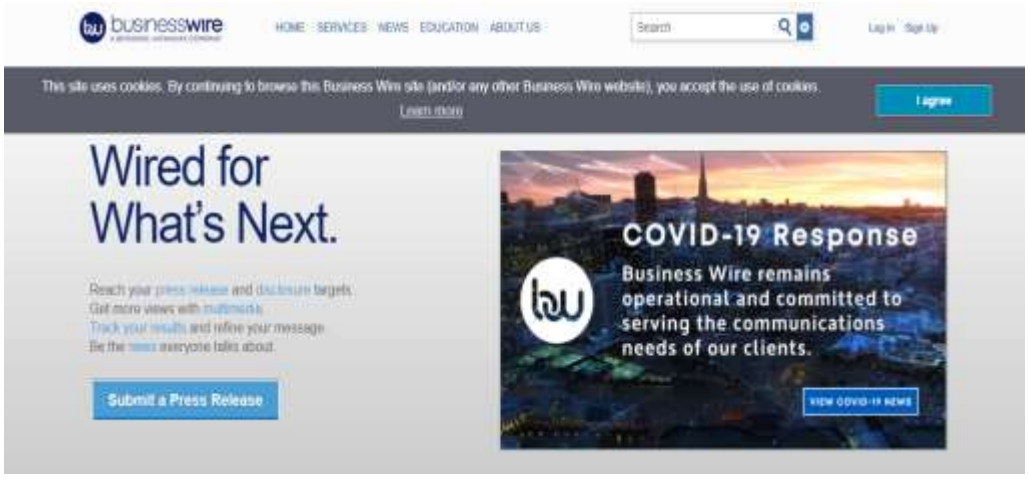

Figure 3: Foot printing using Business wire tool

ix. Email Footprinting: Polite Mail tool is used to gather information present in the mail communication between target systems. With the help of Microsoft Outlook it traces the target mails. By sending list of target addresses a malicious link will be forwarded to gather the important events. The Polite Mail gathers emails header which can reveal sensitive information such as time and date of communication, target address, sender's IP address, and etc.

x. DNS Footprinting: The DNS Footprinting is a process of identifying the name os the DNS and used to target the zone transfers. The DNS servers update their information by transferring the database via zone transfer mechanism. When, a hacker requested for DNS information the request will be uploaded through hierarchical structure of the DNS. This can solve the problem of identifying domain name request NsLookup as shown in figure 4 is one of the fundamental tool used to put a query to DNS server. The tool gathers DNS information such as address information and machine name. The Nslookup can be run at command prompt of either Windows or Linux Operating systems. The NsLookup is executed by specifying either IP address or system name. The process will gathere all CNAMEs (Canonical Names) of the target system. When there are multiple number of domain name servers only one will act as server. The other will be the secondary server.

Figure 4: NsLookup tool

The four step process of Zone transfer is similar to DHCP which are shown below.

Step 1: The secondary server starts the process by sending Start of Authority (SOA) record request to primary server.

Step 2: Up on receiving the request, the primary server authorises the secondary server if the secondary server name is present in the names list, then requested SOA record will be sent.

Step 3: Upon receiving SOA record from primary server, the secondary server matches for the duplicate record. If a match is found the process will stop, if higher serial number is found the SOA at secondary server will be updated. Generally AXFR request is send by secondary server if an update is required.

Step 4: If an updated request received by primary server, then the entire zone will be sent to secondary server.

xi. Network Footprinting: There are few tools used to get the target network information. Gaining such information the hacker can create network map of targeted system. The network map can be obtained by extracting information such as host name, IP address, range of addresses, application versions, exposed hosts, etc. Whois, Nslookup, tracert are some of the popular tools used for Network Footprintg. The attacker get the information such as network range and targeted system's subnet mask. The IP address can be retrived from Internet registers. The geographic location of the target system can be identified by verifying the route message sent to the destination. This can be achieved by tools like traceroute, NeoRoute, visual Route, and etc. The GUI interface of the map is provided by Visual Route and NeoTrace.

xii. Maltego Footprinting: Maltego is a data mining tool gathers online information through various sources lies on the internet. The gathered information is analysed with graphical representations. The Maltego automatically gathers the information via different data sources and the retrived information is represented with nodes in the graphs.

III. Working with Tool

3.1 Traceroute Tool: In most of the operating systems the Traceroute tool as shown in figure 5 is used to reach the destination address by sending the Internet Control Message Protocol (ICMP) to each hop through a gateway [9]. The hacker can determine the number of hops a router from the sender. If a firewall is encountered in the target system, the Traceroute will be timeout. But, the traceroute will send the firewall details to the hacker. Then, the hacker can use another method to bypass the firewall [10]. For instance the tracert command in Traceroute packet tracking tool is used to locate the destination's network route contains the routers.

Figure 5: Location map with Trace Route

The traceroute can identify hop limit and port used at the target system network. The traceroute identifies the firewalls or incorrect routing table which causing ICMP traffic blocking. The traceroute is also used to gather information related to IP address range and network infrastructure to help penetration testers [11].

3.2 Nmap Tool: Nmap is an open source tool mostly used to explore the network and auditing security. Although Nmap designed to scan large size networks, it performs optimistic at single hosts. It is used in many cases like network inventory, host monitoring, and to control service upgrade schedules. The Nmap identifies hosts running on operating system by using IP packets in different ways [12].

The Phases of nmap Scan :

The Nmap scan runs in different phases such as Script scanning, Script pre-scanning, Script post-scanning, trace routing, Ping scanning, OS detection, Target enumeration, Reverse DNS resolution, version detection, and port scanning. The Nmap script engine is used to gain remote system information by suing special purpose scripts. This phase is used when the scripts are executed single time per Nmap execution. The target enumeration phase is very important and can- not be skipped. In this phase the user retrieves the host specifiers such as IP address, CIDR network notations, DNS name, etc. These specifiers are resolved into IPv4 or IPv6 address.

In Script post scanning phase the final results of statistics and reports are generated after completing the Nmap scanning of the system. The Nmap Script Engine (NSE) runs at main script scanning phase. The

ISSN- 2394-5125 VOL 7, ISSUE 11, 2020

information is gathered by Lua programming powered by NSE. It interacts with port number of each target host. The scipt scanning is run at each target host. In this phase the information suchas vulnerabilities, network services, versions, etc., are detected.

In output phase the Nmap writes output in several formats, for example in XML format. The Nmap scans each group completely and produces the output and moves to the next group for scanning. Each phase is repeated on groups in large networks.

The Nmap is used in auditing the network system and in detecting new servers. It can also retrieve domain names and sub domain names. The NSE has an advantage of interacting with target system. It can also retrieve the information regarding the host's nature of service.

IV Results

In this section few of the footprint results are shown for user perspective. The figure 6 is showing WHOIS footprint implications. The figure depicts website information such as domain information, expiration, current status and etc. Similarly the figure 7 is showing procedure for advance google Footprinting.

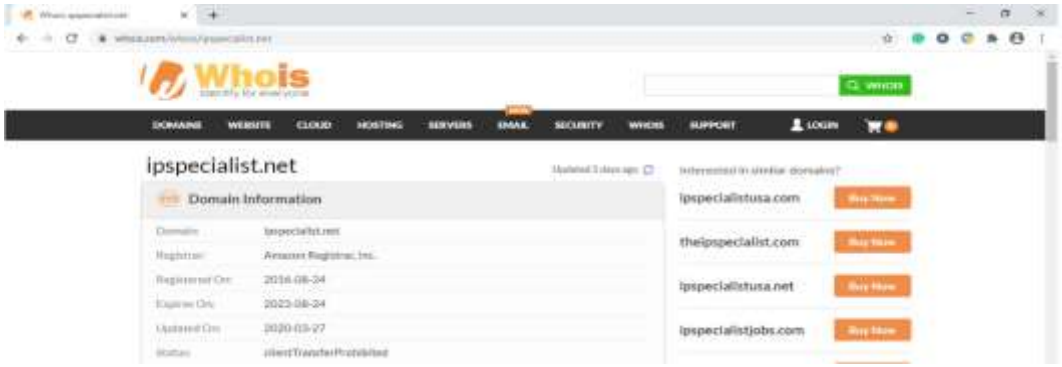

Figure 6: results of WHOIS Footprinting

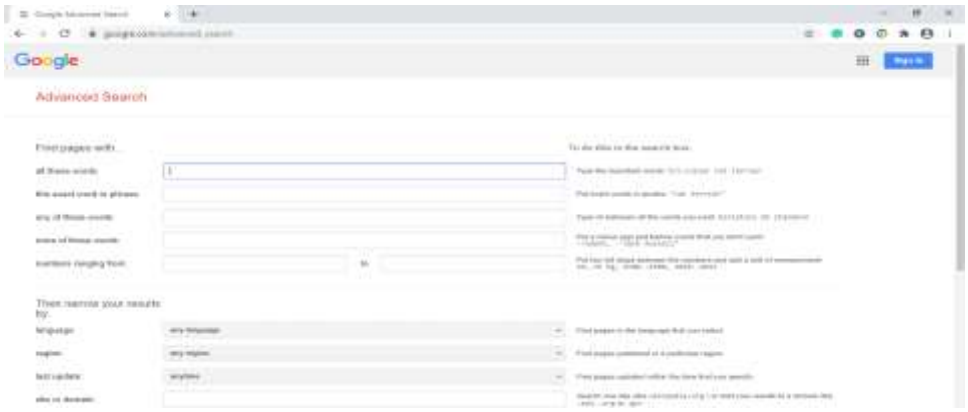

Figure 7: Information gathering with google Footprinting

The figure 8 is showing an instance when *'tracert'* command is executed at Traceroute tool. Similarly figure 9 is showing a screenshot when nslookup is executed at DNS Footprinting tool.

```
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

Figure 8: Output after tracert command

ISSN- 2394-5125 VOL 7, ISSUE 11, 2020

Figure 9: A screenshot at DNS foot printing

V. Conclusion

The Footprinting tool helps to avoid post sensitive and private information on social media. The tool identifies and avoids unwanted friend requests and stops unknown requests. Footprinting also alerts about type of vulnerabilities. The help in setting proper configurations and also avoids leak of target system configurations and file sharing information. There are many Footprinting tools and techniques for gathering a target system's data. No software is made with zero vulnerability. So it is better to understand how a system's information is gathered before hacking the target system. In this way, various measures can be developed to prevent system attacks. In coming years drastic changes can be seen in the development of Footprinting tools. If a user is able to understand the different techniques of Footprinting and also follow countermeasures of Footprinting then the user will be able to protect the personal data from getting hacked. A user must update the system security regularly. By improving the system's security, attacks on the system can be prevented.

VI. References

[1] Footprinting and Scanning, Chapter 3, http://ptgmedia.pearsoncmg.com/images/9780789735317/samplechapter/ 0789735318_CH03.pdf
[2] Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering, chapter , 2 http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/02_gathering_target_info.pdf
[3] Ric Messier, "Foot Printing and Reconnaissance", Chapter 4, Wiley Online Library, May 2019, (https://doi.org/10.1002/9781119533245.ch4)
[4] David Galas and Albert Schmitz, "DNAase footprinting: Simple method for detection of protein-DNA binding specificity", Nucleic Acids Research, Vol 5(9), Oct, 1978
[5] Stanford University. 2007. Information Security Review Preliminary Questionnaire. Luettu 6.11.2013. http://www.stanford.edu/group/security/securecomputing/SU_Security_Assess_v3.html
[6] Eddie Sutton, "Footprinting: What is it and How Do You Erase Them", https://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf
[7] https://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf
[8] http://www.securityfocus.com/infocus/1224—Passive fingerprinting
[9] www.sys-security.com/archive/papers/ICMP_Scanning_v2.5.pdf—ICMP usage in scanning
[10] Vesaria Network Security Specialists. 2013. Firewall Testing From Eye of the Hacker. Luettu 9.11.2013. http://www.vesaria.com/Firewall/Testing/eye_of_hacker.php
[11] Wai, C. 2002. Conducting a Penetration Test on an Organization. Luettu 13.6.2013. http://www.sans.org/reading_room/whitepapers/auditing/conducting-penetration-testorganization_67
[12] Nmap.org. 2013. Nmap Reference Guide. Luettu 15.11.2013. http://nmap.org/book/man.html