International Journal of Computer Networks and Communications Security

VOL. 6, NO. 12, DECEMBER 2018, 250–263
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

The Silent Art of Reconnaissance: The Other Side of the Hill

Usman Ali Dar[1] and Arsalan Iqbal[2]

[1, 2] Georgian College, IT Department, Barrie, L4M3X9, Canada

[1]usmanalidar@outlook.com, [2]arsallankhan@hotmail.com

ABSTRACT

The Internet has grown exponentially in the past 3 decades. This communication system includes networks owned by government, private parties, academia and individual networks. Any malicious move or outbreaks toward these infrastructures can become the reason for threat to its operations and this results in unbearable damages. Readily available information with fast access to internet resources online not only generates huge success and resources for any business but it also makes it fragile and vulnerable to a single hacker or a group of hackers. These cyber criminals possess a unique set of highly sophisticated tools and they are capable of breaking into systems and networks. The depth of their reachability is your information and presence online. A process of acquiring such information, which assists in exploiting the systems or networks called Recon or Reconnaissance. This paper explores different kind of reconnaissance techniques that are used by an attacker or hacker to collect information regarding the target. This study further determines which recon technique gathers the most information about the target while keeping its identity hidden.

Keywords: *Reconnaissance, Attacks, Hacking, Information, Network, Scanning*.

1 INTRODUCTION

Reconnaissance originated in 1800-1810 from French language that means, "act of surveying". Reconnaissance is an initial survey to gain data and are those processes that carry out to acquire information, either by visual surveillance, social engineering or any other methods that can reveal secure/ important / classified documents, events or resources of a target / enemy [1]. Traditionally, reconnaissance was a role, adopted by the cavalry (Military) to gain valuable information about the terrain and their enemy, so they can plan and design a robust attack. Internet is a big world of networks within the networks; it facilitates and data transportation between different infrastructures where distance does not matter. All part of this cyber world are linked with different array of devices and technologies wireless, wired, optical. Cyber world carries an extensive wide range of data information with resources and services and deliver it to us. This enormous amount data encapsulated and transported using different forms such as inter-linked hypertext documents, applications and database of World Wide Web (WWW), Moreover electronic mail, Voice, Video Communication and peer-to-peer networks and many more.

We live in the world of digits, where anyone's information is stowed in various digital forms and readily available online with the affluence of access. Virtually every network attack preceded by network reconnaissance. Hackers scan and probe networks before they attack in order to get information about the target"-[2]. Online Information Services include critical infrastructures like Armed Forces, Defense Organization, Technology, Communications, Health, Financial and Education Systems. As the information set its foot to online cyber world, it becomes risky and vulnerable, which led unauthorized personal /Attacker or hacker towards seeing what is on the "Other Side of the hill" to decide what types of attacks can be launched. It is all about knowing your targets, longer the time spent in knowing their targets and its online presence, the easiest It will be to find the effective methods to exploit that target [3].

Fig. 1. Phases of Attacks

It is the progression towards pursuit, trail, catalogue and spell out the attack on target, due to this risk factor, it is very important to mitigate this risk and secure our infrastructure to protect information data. To build cynical structure and strength to hold against these threats interceptive and preventive measures discussed in this paper.

2 *RECONNAISSANCE*

The process of reconnaissance, revolve around one simple idea "Information Gathering". By using different tool sets, techniques or methods for important information gathering and use for building a robust attack against the target. Reconnaissance has two main vectors: active and passive.

2.1 Types of Reconnaissance

In order to understand the process of the attack, we should be able to understand its myth behind the attack; there are two types of Reconnaissance. Figure "2" shows the two type of Reconnaissance methods.

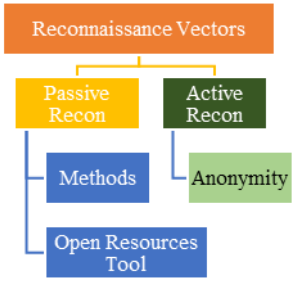

Fig. 2. Reconnaissance Vectors

2.1.1 Passive Reconnaissance

Performing recon is the art of surveillance of information gathering in stealth mode, on your target and knowing all about it strengths and weakness without traces [4]. Passive attacks also known as Pre-Sessions-Reconnaissance, where there is no direct contact of any sort between the target and attacker. Using different methods and techniques maximum information is loaded. Many times the information is all available online target websites such as DNS, Whois databases which gives out handy information for drafting a sketch, and then keeps fill in the blanks by using other tools, they are often refer to as open tools as they are freely available online for anyone use. Figure "3" explains some of the important points of passive reconnaissance.

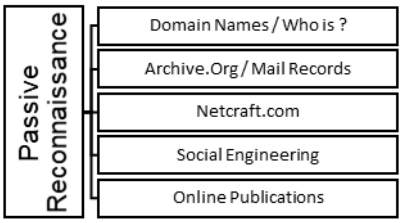

Fig. 3. Methods of Passive Reconnaissance

2.1.2 Active Reconnaissance

The next step is active which involves more preparation from the attackers. Leaving traces could led the target to start investigation or lead them to attacker. For this reason, the most common method used is Anonymity which means to stay anonymous or in stealth mode. [5]. Active reconnaissance can start with tools that send packets to learn the target system. One of the tool is traceroute to know the address of routers and firewall that protect the target hosts. It is all about gathering the important information. It can be as simple as reviewing target's website. Basic information can be acquired for example basic contact information, office location, type of business and resources email and support. Attacker can make a call to the target using public phone to get out the privileged information, which may include about departments, employee's specifics, floors, communication systems. Swindling is also one of the methods that manipulates the authorized personal, operator, and administrators in such a way that the information which is provided by the target is seems very formal information; however for the attacker that information is a magic stick that will help him opening other doors for more access [6].

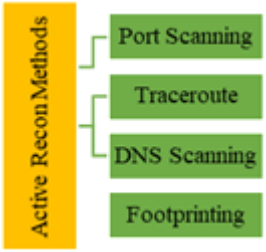

Fig. 4. Methods of Active Reconnaissance

3 METHODS OF RECONNAISSANCE

To reduce hacker / attacker anonymity or identity, different reconnaissance methods used between the level of risk, amount of information gathered and the anonymity of hacker / attacker.

3.1 Port Scanning

Port scanning is a simple query, which carry the request from the one source to destination and bring the response back to requester. This service is widely used for different purposes Network auditing, Recon, attacking, listening to services which are may be running and open. [7].

3.1.1 Traceroute

Traceroute is the network utility that records the route information (gateway, each hops, time taken), from source to destination. It is included in most of the used operating systems.

3.1.2 DNS Scanning

DNS is a distributed database among servers and it is queried by all different hosts and other servers for information. DNS servers with most of the important information which can play a very important role in building an attack against the target. The top level is the last label in the domain name. Top level domain can be two to three letter organizational designators

Table 1: DNS Hierarchal Chart.

Designator	Type
.COM	Commercial
.GOV	Government
.EDU	Education
.BIZ	Business
.NET	Network
.CA	Canada
.US	USA

The hierarchal chart shows the type of the designator; however, there are also two-letter labels which is designated for the country itself or the region it belongs locally.

3.1.3 Footprinting / Fingerprinting

Footprinting, fingerprinting are the same faces of same tool which provide a significant quantity of important information and opportunity to build more robust attack. This sort of reconnaissance tool also provide guidance for making the appropriate decisions to launch different types of attacks using different tools [8]. We should not mix our technology with process. "Security is a Process not technology" and that is where we lost our control and provide invitations to threats and other risks.

4 RECONNAISSANCE TOOLS

There a large of number of free and paid tools available online for network reconnaissance. Following are the set of tools, used to gather all information. Free/open tools can be downloaded or used online to get the information anonymously to build a strong and robust attack against the target/Victim without engaging target's attention. The open tools used to gather the information dns and network in table 2 below.

Table 2: Reconnaissance Tools

Passive Reconnaissance Tools	Active Reconnaissance Tools
Centeralops.net	Kali Linux
Dnsstuff.com	Nmap
Who.is	Zenmap
Mxtoolbox.com	Dnsrecon
Web.archive.org	Dnsenum
Wayback.archive-it.org	Dnsmap
Google Operator Search Engine	

5 PASSIVE INFROMATION TOOL SET

Information below will give a bird eye view of the information, which is gathered and processed.

Table 3: List Of Whois Information

Type	Information	
Target	• Who they are • Geographical presence • Main and site offices • Contact information	• Domain Name • Web Address • Associated Web Links
Domain	• Name Servers & Response • IP Address / Subnets • Network Path & TTL	• www info • TCP /UDP Response • Identical Records
Registration	• Registrant Contact Info • Administrative Contact Info • Billing/Financial Information	• Technical Contact • Dates for records, updates and expiry

5.1 DNS Records

Domain Records gives a great deal of presentation for network mapping. DNS Information include, Start of authority (SOA), it is the information stored in domain name system (DNS) zone about that zone and about other DNS

records. A DNS is a start of a domain for which an individual DNS server is responsible. Each zone contains a single SOA record [9]. Mail Exchange (MX) Records. MX record is in the DNS that specify a mail server accountable for accommodating emails messages on behalf of a receiver's domain. Preference value used to prioritize mail delivery if multiple mail servers are available. A name server is a computer Hardware or software server that implements a network service for providing replies to inquiries in contradiction of a directory service. It interprets an often humanly meaningful, text-based identifier to a system-internal, often numeric identification or addressing section. The server in response to a service protocol request performs this check. Beside, records like A and AAAA other records provide important information in table 4.

Table 4: DNS Records

Class Records	• IN (Internet) "1" • Unassigned "2"	• CH (chaos) "3" • Reserved "0"
Types of Records	• A , AAAA, AFSDB, APL Records • DMARC, DHCID, DLV, DNSKEY, DS, HINFO, ISDN Records • NS, NSEC & 3, NSEC3PARAM, MX Records • PTR, RRSIG, RP, SIG,SPF, SOA, SRV, SSHFP Records	• CAA, CDNSKEY, CDS, CERT, CNAME Records • IPSECKEY, KEY, KX, LOC Records • MX Records • TA, TKEY, TLSA,TSIG, TXT Records • URI, DNAME Records
Pseudo Resource	• * • AXFR	• IXFR • OPT

5.2 Search Engines

Today's internet is a big data space. There are many big names for search engines; however, we will use Google database. By using proper commands and operators, which simplify your search and produce effective results. Some of the general search segments listed in Table 5 below.

Table 5: Search Operators

Operator	Search Operator
Web Search	allinacnhor, allintext, allintitle, linurl, cache, define, filetype, id, inanchor, info, intext, intitle, related, site
Image Search	allintitle, allinurl, filetype, intitle, site
Groups	allintext, allintitle, allinurl, filetype, intext, intitle,
Directory	allintext, allintitle, allinurl, intext, intitle, inurl, location, source, ext
News	allintext, allintitle, allinurl, intext, intitle, inurl, location, source
Product	*Allintext, allintitle*

The table 1.D explains very general search operators. These operators used in different methods to filter the search according to our needs and requirements. The search results can further be refined for any vulnerability servers, files, network data or even files that contains other information, which can lead to a lethal attack. Some of the information, which can be refined from search engine.

5.3 Web Archiving

Web archiving is one of the best ways to understand and gather important information about target. It gives you a lifeline snapshot about target. The web-archiving tool will provide information like how many times the target has made changes with dates. Web archiving tool save pages before and after any change, which gives the opportunity to learn more about the target. Beside this all information, it also gives you information about any audio, video, documents, pictures related to the target [10].

6 ACTIVE INFORMATION TOOL SET

Following information is processed through active reconnaissance tools set.

6.1 Linux Distributions

There are some Linux distributions that is customized and build with comprehensive set of tools for forensics, auditing, penetration testing. These distributions are being used by both white and black hat hackers. We have used most the tools from the table 6 below for acquiring desire results

Table 6: Linux Distributions

Distribution	Type
Kali	Debain-Drived
Nmap	All OS
Zenmap	All OS
Dnsrecon	Linux
Dnsenum	Linux
Dnsmap	Linux
Backtrack	Linux Dist
Parrot Security	Linux
Pentoo	Gentoo Linux

6.1.2 Kali Linux Distribution

Kali Linux is a Debian-derived Linux distribution. Kali contain a comprehensive set of tools, used for digital forensic, penetration testing and security auditing.

6.1.3 Nmap

Nmap is famous for network scanning. This scan provides information regarding potential hosts and the services running on these hosts. These tools are completely customizable via scripting.

6.1.4 Zenmap

Just like Nmap, Zenmap also do the scanning of IP or FQDN of hosts from single to a complete list or range of networks/ host. Different formats are available for search result.

6.1.5 Dnsrecon

DNS reconnaissance tool provides the ability to check all Network Servers (NS) records for Zone Transfers. It also enumerate General DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF, TXT). This too also perform common SRV Record Enumeration with Top-level Domain Expansion (TLD).

6.1.6 Dnsenum

Dnsenum is a multithreaded pearl scripted tool to enumerate DNS information of a domain and to discover non-contiguous IP blocks. This tool has a multi-operation levels which are, host address (A Record), Name Server (Threaded), Mail Exchange Records (MX, Threaded). Beside these it also perform axfr queries on name servers and get BIND Version with parent and subdomains.

6.1.7 Dnsmap

Like other tools, Dnsmap is a well-known tool used for penetration testing and hacking. Most of the information provided by this tool is same, however, Dnsmap does differ from other tools and provide information like finding interesting remove access servers, badly configured / unpatched servers, new domains and discover embedded devices configured using dynamic services.

7 IMPLEMENTATION OF TOOLS

Most of tools comes with different Linux distribution, when we install the operating system. In our case we will be using Kali Linux. The remaining tools installed on windows desktop / virtual machine.

7.1 Stealth Mode Ready

Although we are not interacting directly with our target, still in any case traces would be harmful, which can lead to the source/ attacker. For this purpose covering your tracks is the most important point, there are many methods to hide your identity.

7.1.1 Process & Options for Stealth

- Use of Live CD / USB or Virtual Machine
- Use different Proxies and DNS services
- Use encrypted connection VPN, Hamachi can gives you that functionality
- In case of tools are online, use private browsing, browser in browser and other techniques

7.1.2 Central Ops.net

Centralops.net is a web-site which gives us a lot of important information, which is given below in table 7.

Table 7: Information from Centraops.net

Address Lookup	Whois Records Registry / Registrar
Name: hackthissite.org Address: 2610:150:8007:0:198:148: 81:135; 2610:150:8007:0:198:148: 81:137 2610:150:8007:0:198:148: 81:138; 2610:150:8007:0:198:148:	Domain Name: HACKTHISSITE.ORG; Registry Domain ID: D99641092-LROR; Registrar WHOIS Server:; Registrar URL: http://www.enom.com Updated Date: 2017-01- 19T00:22:27Z; Creation

81:139 2610:150:8007:0:198:148:81:136 198.148.81.137; 198.148.81.139; 198.148.81.136; 198.148.81.138 198.148.81.135	Date: 2003-08-10T15:01:25Z; Registry Expiry Date: 2017-08-10T15:01:25Z Registrar: eNom, Inc.; Registrar IANA ID: 48; Registrar Abuse Contact Email: Registrar Abuse
Registrant Information	Administrator Information
Registry Registrant ID: db3bfd3345eda734 Registrant Name: Whois Agent Registrant Organization: Whois Privacy Protection Service, Inc. Registrant Street: PO Box 639 Registrant Street: C/O hackthissite.org Registrant City: Kirkland Registrant State/Province: WA Registrant Postal Code: 98083 Registrant Country: US Registrant Phone: +1.4252740657 Registrant Fax: +1.4259744730 Registrant Email: spywvvvq@whoisprivacyprotect.com	Admin Name: Whois Agent Admin Organization: Whois Privacy Protection Service, Inc. Admin Street: PO Box 639 Admin Street: C/O hackthissite.org Admin City: Kirkland Admin State/Province: WA Admin Postal Code: 98083 Admin Country: US Admin Phone: +1.4252740657 Admin Phone Ext: Admin Fax: +1.4259744730 Admin Fax Ext: Admin Email: spywvvvq@whoisprivacyprotect.com
Technical Contact Information	
Registry Tech ID: db3bfd3345eda734; Tech Name: Whois Agent; Tech Organization: Whois Privacy Protection Service, Inc.; Tech Street: PO Box 639 Tech Street: C/O hackthissite.org; Tech City: Kirkland; Tech State/Province: WA; Tech Postal Code: 98083; Tech Country: US; Tech Phone: +1.4252740657 ; Tech Phone Ext:; Tech Fax: +1.4259744730; Tech Fax Ext:; Tech Email: spywvvvq@whoisprivacyprotect.com	

7.1.3 Dnsstuff.com

The dnsstuff.com is also open and powerful tool to gather information. Following are the segments of the information that we gathered Registration, Registrant, Admin / Tech, Network, Technical Information.

Table 8: Registration Information from Dnsstuff.com

Registration Information
Domain Name: HACKTHISSITE.ORG; Registry Domain ID: D99641092-LROR; Registrar WHOIS Server: Registrar URL: http://www.enom.com Updated Date: 2017-01-19T00:22:27Z Creation Date: 2003-08-10T15:01:25Z Registry Expiry Date: 2017-08-10T15:01:25Z Registrar: eNom, Inc. Registrar IANA ID: 48 Registrar Abuse Contact Email: Registrar Abuse Contact Phone:

Table 9: Registrant Information from Dnsstuff.com

Registrant Information
Registry Registrant ID: db3bfd3345eda734 Registrant Name: Whois Agent Registrant Organization: Whois Privacy Protection Service, Inc. Registrant Street: PO Box 639 Registrant Street: C/O hackthissite.org Registrant City: Kirkland Registrant State/Province: WA Registrant Postal Code: 98083 Registrant Country: US Registrant Phone: +1.4252740657 Registrant Phone Ext:

Table 10: Network Information from Dnsstuff.com

Network
Name Server: C.NS.BUDDYNS.COM; Name Server: F.NS.BUDDYNS.COM Name Server: G.NS.BUDDYNS.COM; Name Server: H.NS.BUDDYNS.COM Name Server: J.NS.BUDDYNS.COM

Table 11: Admin /Tech Information from Dnsstuff.com

Admin/Tech/
Admin Street: C/O hackthissite.org Admin City: Kirkland Admin State/Province: WA Admin Postal Code: 98083 Admin Country: US Admin Phone: +1.4252740657 Admin Fax: +1.4259744730
Technical Information
Tech Name: Whois Agent; Tech Organization: Whois Privacy Protection Service, Inc. Tech Street: PO Box 639 ; Tech Street: C/O hackthissite.org; Tech City: Kirkland; Tech State/Province: WA ;Tech Postal Code: 98083 Tech Country: US; Tech Phone: +1.4252740657; Tech Phone Ext: Tech Fax: +1.4259744730 Tech Tech Email: spywvvvq@whoisprivacyprotect.com

7.1.4 Whois Information from Who.is

Who.is also an open tool which can be used to gather information. Only 3 segments was gathered Registrant, Administrative and Technical.

Table 12: Whois information from who.is

Registrant Contact Information
Name Whois Agent Organization Whois Privacy Protection Service Address PO Box 639 Address C/O hackthissite.org City Kirkland State / Province WA Postal Code 98083 Country US Phone +1.4252740657 Fax +1.4259744730 Email spywvvvq@whoisprivacyprotect.com
Administrative Contact
Name Whois Agent Organization Whois Privacy Protection Service, Inc.; Address PO Box 639 Address C/O hackthissite.org City Kirkland State / Province WA Postal Code 98083 Country US Phone +1.4252740657 Fax +1.4259744730 Email spywvvvq@whoisprivacyprotect.com
Technical Information
Name Whois Agent Organization Whois Privacy Protection Service, Inc. Address PO Box 639 Address C/O hackthissite.org City Kirkland State / Province WA Postal Code 98083 Country US Phone +1.4252740657 Fax +1.4259744730 Email spywvvvq@whoisprivacyprotect.com
Network Information
C.NS.BUDDYNS.COM 88.198.106.11, F.NS.BUDDYNS.COM 103.6.87.125 G.NS.BUDDYNS.COM 199.167.17.21, H.NS.BUDDYNS.COM 119.252.20.56 J.NS.BUDDYNS.COM 185.34.136.178

7.1.5 Mxtoolbox.com Information from Mxtoolbox

From this tool we gather the information which is given below in Table 13.

Table 13: Information from Mxtoolbox

Registrant Contact Information
Registrant Name: Whois Agent Registrant Organization: Whois Privacy Protection Service, Inc. Registrant Street: PO Box 639 Registrant Street: C/O hackthissite.org Registrant City: Kirkland Registrant State/Province: WA Registrant Postal Code: 98083 Registrant Country: US Registrant Phone: +1.4252740657 Registrant Fax: +1.4259744730 Registrant Email: spywvvvq@whoisprivacyprotect.com Registry Admin ID: db3bfd3345eda734
Administrative Contact
Admin Name: Whois Agent Admin Organization: Whois Privacy Protection Service Admin Street: PO Box 639 Admin Street: C/O hackthissite.org Admin City: Kirkland

Admin State/Province: WA Admin Postal Code: 98083 Admin Country: US Admin Phone: +1.4252740657 Admin Phone Ext: Admin Fax: +1.4259744730 Admin Email: spywvvvq@whoisprivacyprotect.com
Technical Information
Tech Name: Whois Agent Tech Organization: Whois Privacy Protection Service Tech Street: PO Box 639 Tech Street: C/O hackthissite.org Tech City: Kirkland Tech State/Province: WA Tech Postal Code: 98083 Tech Country: US Tech Phone: +1.4252740657 Tech Fax: +1.4259744730 Tech Email: spywvvvq@whoisprivacyprotect.com
Registrar Information
Domain Name: HACKTHISSITE.ORG; Registry Domain ID: D99641092-LROR Registrar WHOIS Server: Registrar, Updated Date: 2017-01-19T00:22:27Z ;Creation Date: 2003-08-10T15:01:25Z; Registry Expiry Date: 2017-08-10T15:01:25Z Registrar: eNom, Inc. ; Registrar IANA ID: 48 ;Registrar Abuse Contact Email: Registrar Abuse
Technical Information
Tech Name: Whois Agent ; Tech Organization: Whois Privacy Protection Service, Inc. Tech Street: PO Box 639 ; Tech Street: C/O hackthissite.org; Tech City: Kirkland; Tech State/Province: WA ;Tech Postal Code: 98083 Tech Country: US; Tech Phone: +1.4252740657; Tech Phone Ext: Tech Fax: +1.4259744730 Tech Fax Ext: Tech Email: spywvvvq@whoisprivacyprotect.com

7.2. DNS INFORMATION

Following are the tools which are used to gather DNS information

7.2.1. Centralops.net DNS Information

Table 14 below is the information output from Centraops.net. It is an open tool and can be used for gathering information

Table 14: DNS Information from Centralops.net

```
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2018-11-14T06:29:14Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2019-08-
10T15:01:25Z
Registrar Registration Expiration
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email:
abuse@enom.com
Registrar Abuse Contact Phone:
+1.4252982646
Reseller:
Domain Status:
clientTransferProhibited
https://icann.org/epp#clientTransferPr
ohibited
Registrant Organization: Whois Privacy
Protection Service, Inc.
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
```

7.2.2. DNS information from Dnsstuff.com

Table 15 below is with the output information from dnsstuff.com.

Table 15: Dns Information from Dnsstuff.com

Domain	Class	Type	Answer	Response Time
Hackthissite .org	IN	A	198.148.81.135	87ms
Hackthissite .org	IN	A	198.148.81.139	87ms
Hackthissite .org	IN	A	192.148.81.137	87ms
Hackthissite	IN	A	198.148.8	87ms

.org			1.136	
Hackthissite.org	IN	A	198.148.81.138	87ms
c.ns.buddyns.com	IN	A	88.198.106.11	87ms
f.ns.buddyns.com	IN	A	103.6.87.125	87ms
g.ns.buddyns.com	IN	A	199.167.17.21	87ms
h.ns.buddyns.com	IN	A	119.252.20.56	87ms
j.ns.buddyns.com	IN	A	185.34.136.178	87ms
Hackthissite.org	IN	AAAA	2610:150:8007:0:198:148:81:139	87ms

7.2.3. Dns Records from who.is

Table 16 below is with the output information from who.is.

Table 16: Dns Records from Who.is

Name	Class	Type	Data	TTL
Hackthissite.org	IN	SOA	c.ns.buddyns.com admin@hackthissite.org 2017011905 3600 900 604800 86400	3599s
Hackthissite.org	IN	NS	c.ns.buddyns.com	3599s
Hackthissite.org	IN	NS	f.ns.buddyns.com	3599s
Hackthissite.org	IN	NS	g.ns.buddyns.com	3599s
Hackthissite.org	IN	NS	h.ns.buddyns.com	3599s
Hackthissite.org	IN	NS	g.ns.buddyns.com	3599s
Hackthissite.org	IN	A	198.148.81.135	3599s
Hackthissite.org	IN	A	198.148.81.139	3599s
Hackthissite.org	IN	A	192.148.81.137	3599s
Hackthissite.org	IN	A	198.148.81.136	3599s
Hackthissite.org	IN	A	198.148.81.138	3599s

7.2.4 Dns Records from Mxtoolbox.com

Following is the dns records obtained from Mxtoolbox open tool.

Table 17: Dns Records from Mxtoolbox

Type	Domain	IP	TTL
A	Hackthissite.org	137.74.187.100 OVH SAS (AS16276)	60 min
A	Hackthissite.org	137.74.187.100	60 min
A	Hackthissite.org	OVH SAS (AS16276	60 min
A	Hackthissite.org	137.74.187.100	60 min
A	Hackthissite.org	OVH SAS (AS16276	60 min

7.2.5 Web-Archiving

This tool archive the web time to time with concerning to updates. This tool can update you with information about the target's past, present and its status. As we can see in Figure '5' for Web Archiving Results from Waybackmachine.org that, this target activated in 2003. All the black markings indicate the changes done in that year, month, and day, whereas the blue markings in the calendar represent the change done on that month's day. To review any year we simply click on that year box and whole calendar for that year appears below with monthly changes marked in blue circle. We can also

browse any specific date when the change made to the target website and can review the time as well as cached copy of that webpage taken before and after the update. We can also compare the old to new and review the difference between them. We can search and review the target information from past to present and refine it from years to months to weeks till day. We can even get the information about how many times the target updated the information. Every time the information is updated, they take a snapshot of the current and updated contents.

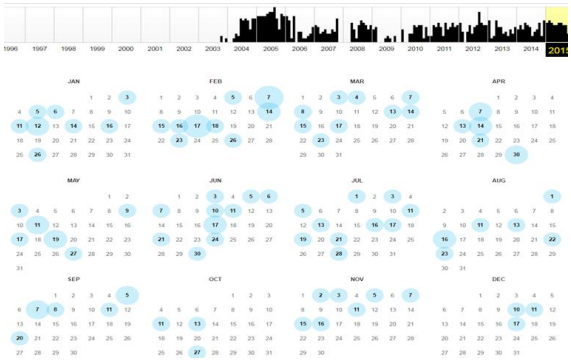

Fig. 5. Web-Archiving from web.archive.org

8 Active Information Gathering

Before the reconnaissance is started, kali Linux virtual machine was built configured for information gathering.

8.1. Nmap & Zenmap

Nmap ("Network Mapper") is a free and open source (license) utility 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 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 official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping)[11].

Fig. 6. Nmap & Zenmap results

8.1.2 Dnsrecon

DNS recon is a comprehensive tool which can do a number of tasks with different operators for example enumeration with "-d" can be used. We can see that with standard domain, the search found the similar information. With "–g" which can do google enumeration and all the records from google search engine. There are many other operators which can be used to find and refine the information for target or save them in any file format. Figure Results from Dnsrecon (Kali).

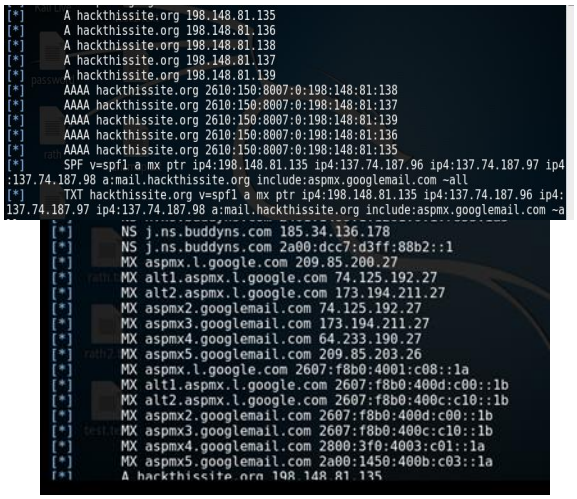

Fig. 7. Dnsrecon from kali

8.1.3. Dnsenum

Table 18: Information from Dnsenum

Name	Class	Type	Data	TTL
Host Addresses:				
Hackthissite.org	IN	A	198.148.81.135	976
Hackthissite.org	IN	A	198.148.81.139	976
Hackthissite.org	IN	A	192.148.81.137	976
Hackthissite.org	IN	A	198.148.81.136	976
Hackthissite.org	IN	A	198.148.81.138	976
Name Servers				
c.ns.buddyns.com	IN	A	88.198.106.11	188s
f.ns.buddyns.com	IN	A	103.6.87.125	188s
g.ns.buddyns.com	IN	A	199.167.17.21	188s
h.ns.buddyns.com	IN	A	119.252.20.56	188s
j.ns.buddyns.com	IN	A	185.34.136.178	188s
Mail (MX) Records				
alt1.aspmx.l.google.com	IN	MX	173.194.219.27	188s
alt2.aspmx.l.google.com	IN	MX	74.125.192.27	188s
aspmx2.googlemail.com	IN	MX	173.194.219.27	188s
aspmx3.googlemail.com	IN	MX	74.125.192.27	188s
aspmx4.googlemail.com	IN	MX	173.194.212.26	188s
aspmx5.googlemail.com	IN	MX	64.233.186.26	188s
aspmx.l.google.com	IN	MX	74.125.70.26	188s

9 TOOL COMPARISON & FEATURE SET

Attack graphs help to determine the security weaknesses that lie in the network. System administrators use it to analyze the network for its weaknesses, that may allow an attacket to expolit it and gain control over the network [12]. The comparison table 1 below will give us a brief review of different tools and feathers to gather different information from regiseration to contact information, location, emails and technical information of network. It also ncludes AS path IPv4 and IPv6 with CIDR, operating system detail information details and its type, server records, dns records which include SOA, MX, NS, SPF, TXT, A records, PTR, DMARC, AXFR, Active host types, Zone type. Beside this information who.is tool which will provide the traceroute, path similar domains and service inforamtion; Moreover, web-archiving along with HTTP & SSL information with certificate with detail information about http header, server,methods being used, the type of SSL certificiate and whereabouts, public keys, signature and its encryption. The table below will also help us to deteremin which tool or set of toos can be pair together gather the specific information. Not one or two tools will be enough to gather information multiple source of infomration is required to understand and attack building a attack methodolog for target. For example who.is open tool and dnsrecon can give us all the basic to comprehensive reports of DNS and network with other related information; however, dnsmap and whois tool will be able to provide same and other related information, along with traceroute and tracepath; on-the-otherhand, Web-archiving can give us a brief history of target listing and updates bundled with search operators, which can be very efficient to find the related information for the target, which eventually gives attacker / hacker an edge to corelate.

Table 17: Comparision of Tool & Feature Set

Information	Tools										
Target Inf	Passive							Active			
	Centeeralops.net	Dnsstuff.com	Who.is	Mxtoolbox.com	Web-archive	Waybackarchive	Search Operator	Nmap	Zenmap	Dnsrecon	Dnsenum
Contact Information											
Registeration	Detail	Detail	Some	Detail	No	No	No	No	No	No	No
Registrant	Detail	Detail	Detail	Detail	No	No	No	No	No	No	No
Admin Info	Detail	Detail	Detail	Detail	No	No	No	No	No	No	No
Tech Info	Detail	Detail	Detail	Detail	No	No	No	No	No	No	No
Network Information											
Network Range	Detail	Detail	No	Some	No	No	No	No	No	Yes	Yes
CIDR	Detail	Detail	No	No	No	No	No	No	No	Yes	Yes
Net Name	Detail	Detail	No	No	No	No	No	No	No	Yes	Yes
Type	Detail	Detail	No	No	No	No	No	No	No	Yes	Yes
Origin AS	Detail	NO	No	No	No	No	No	No	No	Yes	Yes
Contact Info	Detail	YES	Some	Yes	No	No	No	No	No	No	No
DNS Information											
SOA	Yes	Detail	Yes	Yes	No	No	No	No	No	Yes	Yes
NS	Yes	Detail	Yes	Yes	No	No	No	No	No	Yes	Yes
MX	Yes	Detail	Yes	Yes	No	No	No	No	No	Yes	Yes
SPF	Yes	Detail	Yes	Yes	No	No	No	No	No	No	Yes
TXT	Yes	Detail	No	Yes	No	No	No	No	No	No	Yes
A Record	Yes	Detail	No	Yes	No	No	No	No	No	Yes	Yes
AAAA Rec	Yes	Detail	Yes	Yes	No	No	No	No	No	Yes	Yes
PTR	Yes	Detail	Yes	Yes	No	No	No	No	No	No	Yes
DMARC	Yes	Yes	No	Yes	No	No	No	No	No	No	Yes
Active Host	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes
AXFR	Yes	No	No	No	No	No	No	No	No	Yes	Yes
Web-Archiving											
Archiving Years	No	No	09	No	Since Online	Since Online	No	No	No	No	No
Multiple Search Operators	No	No	Yes	No	Yes	Yes	No	No	No	No	No
Service Level	No	No	Paid Services	No	Free	Free	No	No	No	No	No
Documents / Texts	No	No	No	No	Yes	Yes	No	No	No	No	No
Audio, Video, Images	No	No	No	No	Yes	No	No	No	No	No	No

Information	Tools										
Target Inf	Passive							Active			
	Centeralops.net	Dnsstuff.com	Who.is	Mxtoolbox.com	Web-archive	Waybackarchive	Search Operator	Nmap	Zenmap	Dnsrecon	Dnsenum
Software	NO	NO	NO	NO	YES	NO					
Whois Information											
Operating System	No	No	No	No	No	No	No	No	Yes	Yes	No
Open Ports	No	No	No	No	No	No	No	No	Yes	Yes	No
Up Time	No	No	No	No	No	No	No	No	Yes	Yes	No
Network Distance	No	No	No	No	No	No	No	No	Yes	Yes	No
Service Information	Yes	No	No	No	No	No	No	Yes	Yes	No	No
Traceroute	Yes	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No
Similar Domains	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes
HTTP & SSL Information											
Http Header	No	Yes	No	No	No	No	No	Yes	Yes	No	No
Http Server Header	No	Yes	No	No	No	No	No	Yes	Yes	No	No
Http Method	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No
SSL Cert Type	Yes	Detail	No	Yes	No	No	No	Yes	Yes	No	No
SSL Cert Issuer	Yes	Detail	No	Yes	No	No	No	Yes	Yes	No	No
Cert public key	Yes	Detail	No	No	No	No	No	Yes	Yes	No	No
Cert Signature	Yes	Detail	No	YES	No	No	No	Yes	Yes	No	No
Cert Encryption	Yes	Detail	No	YES	No	No	No	Yes	Yes	No	No

10 CONCLUSION

This paper outline the existing correlation of reconnaissance life cycle and investigates active and passive reconnaissance method and techniques with practical implementation of various tools for a successful cyber reconnaissance attack. This paper further shows that a single reconnaissance methodology, technique or tool may not give us all the required information for a successful cyber reconnaissance attack. Therefore, a combination of tools with methodologies and techniques required to be incorporated together to get all the required information. The research concludes that, for active reconnaissance DNSENUM is the first tool for collecting information regarding DNS, while NMAP and ZENMAP tools are best for gathering HTTP and SSL information. For passive reconnaissance DNSSTUFF.com provides a very

detailed information regarding network, DNS, contact, HTTP and SSL. CENTERALOPS.net is also as much effective as DNSSTUFF.com MXTOOLBOX.com provides the least information. The study concludes that combination of NMAP/ ZENMAP (active) and DNSSTUFF.com (passive) will give an attacker enough information for a successful attack.

9 REFERENCES

[1] Reconnaissance: https://en.wikipedia.org/wiki/Reconnaissance

[2] H.P Sanghvi Cyber Reconnaissance in IJCA (0975-8887) Volume 63-No.6, February 2013

[3] H.P Sanghvi Cyber Reconnaissance in IJCA (0975-8887) Volume 63-No.6, February 2013

[4] Engelbert Peter van Loon Offensive Cyber by Collin 2012 https://cyberwar.nl/d/MSc-thesis_Offensive-Cyber_Collin-van-Loon_June-2012. pdf

[5] Siraj A. Shaikh, Howard Chivers, Philip Nobles, John A. Clark, Hao Chen http://www.sciencedirect.com/science/article/pii/S1353485808701296

[6] Jian Ren, Tongtong Li, Yun Li, November 16, 2008, INSPEC Accession Number: 10466154, 10.1109/MILCOM.2008.4753343 http://ieeexplore.ieee.org/document/4753343/?reload=true

[7] Cedric Pernet APT Kill Chain- Part 3: Reconnaissanceblog.airbuscybersecurity.com/post/2014/05/APT-Kill-chain-Part-3-%3A-Reconnaissance

[8] Ms. Gurline Kaur & Navjot Kaur, Penetration Testing – Reconnaissance with NMAP-Tool-www.ijarcs.info/index.php /Ijarcs/article /download/3111/3094

[9] Sandeep Kumar Yadav, Daya Shankar, Shrikant Lade: A Network Based Approach to Discover Security Vulnerability on Host System-www.ijarcsse.com/docs/papers/ Volume_4/12_December2014/V4I12-0294.pdf

[10] S Manjit Kaur, Gurpreet Kaur, Er. Gurjot Singh: A Descriptive study of Active Scanning & Reconnaissance tools http://www.iarjset.com/upload/2016/april-16/IARJSET%2038.pdfdf

[11] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones: AN OVERVIEW OF PENETRATION TESTING http://airccse.org/journal/nsa/1111nsa02.pdf

[12] Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani: VULNERABILITY SCANNERS: A PROACTIVE APPROACH TO ASSESS WEB APPLICATION SECURITY http://wireilla.com/papers/ijcsa/V4N1/4114ijcsa11.pdf