Footprinting and Reconnaissance

Footprinting and Reconnaissance

Footprinting is the process of using various tools and techniques to understand and learn the targets infrastructure and vulnerabilities.

In the initial phase we wan to find out as much as possible from gathering information that is publicly available without actually interacting with the scanned target. This kind of attack can be passive or pseudonymous.

Here are some of the of information you can gathered about a target during footprinting.

- Websites
- Alternative Websites
- Domain names
- Network blocks
- Specific IP addresses
- Network services and applications
- System architecture

- Authentication mechanisms
- Access control mechanisms
- Employee email & Phone numbers
- Contact addresses

In this lab we will use tools like ping, tracert and search engines to obtain information about a our target.

lets start with the basic ping command. In this lab series i will use www.hackthissite.org to try out my attacks.

“Hack This Site is a free training ground for users to test and expand their hacking skills. Our community is dedicated to facilitating an open learning environment by providing a series of hacking challenges, articles, resources, and discussion of the latest happenings in hacker culture. We are an online movement of artists, activists, hackers and anarchists who are organizing to create new worlds.”

Open CMD and ping a your favorite site, i am pinging www.hackthissite.org

```
C:\>ping www.hackthissite.org

Pinging www.hackthissite.org [137.74.187.102] with 32 bytes of data:
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45

Ping statistics for 137.74.187.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 40ms, Average = 40ms

C:\>
```

We can see that the site replied with its IP address which is 137.74.187.102.

Now when we have the IP address we can use tracert to see the path the trafic is taking from your client to www.hackthissite.org

```
C:\>tracert 137.74.187.102

Tracing route to hackthissite.org [137.74.187.102]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.10.1
  2     1 ms     1 ms     1 ms  h85-209-118-1.cust.a3fiber.se [85.209.118.1]
  3     1 ms     1 ms     1 ms  gsl-bbr-1-be102.net.comhem.se [213.200.167.80]
  4     4 ms     9 ms     6 ms  gbg1.dr2.a3network.se [88.129.174.24]
  5     1 ms     1 ms     1 ms  gbg1.a3network.se [88.129.128.62]
  6     1 ms     1 ms     1 ms  gbg1.cr1.a3network.se [85.8.9.16]
  7     7 ms     7 ms     7 ms  sto2.cr1.a3network.se [85.8.10.20]
  8    29 ms    18 ms    18 ms  s-b10-link.telia.net [213.248.93.188]
  9    18 ms    17 ms    19 ms  s-bb4-link.telia.net [62.115.119.80]
 10    33 ms    33 ms    33 ms  ffm-bb4-link.telia.net [62.115.138.105]
 11    34 ms    51 ms    30 ms  ffm-b1-link.telia.net [62.115.137.169]
 12    39 ms    39 ms    39 ms  be100-163.fra-5-a9.de.eu [178.33.100.250]
 13   222 ms    44 ms    45 ms  be103.rbx-g2-nc5.fr.eu [94.23.122.240]
 14     *        *        *     Request timed out.
 15     *       40 ms     *     vl7.vss-10b-6k.fr.eu [178.33.100.218]
 16    40 ms    40 ms    40 ms  hackthissite.org [137.74.187.102]

Trace complete.

C:\>
```

With the tracert command we can fallow the trafic trough all routers and firewalls until we arrive to the website.

Use www.netcraft.com To Obtain More Data

Open www.netcraft.com in your web browser, In the right menu under “What’s that site running?” enter www.hackthissite.org the result page will open. Here we can see all the subdomains the site have.

Results for hackthissite.org

Found 4 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.hackthissite.org		october 2003	sharktech	freebsd
2.	hackthissite.org		september 2007	sharktech	unknown
3.	radio.hackthissite.org		august 2011	sharktech	freebsd
4.	mirror.hackthissite.org		august 2011	ovh static ip	freebsd

On the result page click on the site report next to the domain name, a new page will load with information like email address, physical addresses, OS versions, Web Server version and a lot more.

Use WHOIS to obtain domain name information

WHOIS is a database that have information about domains and information about the people that own them. Using this tool give you the potential to gather personal information about the people that you can later use when doing social engineering. As well as collecting information as:

- Information about the owner
- Contact information
- Location
- Domain name servers
- The IP address
- The date of created

There several ways to use “WHOIS” like online services, applications and from command line, use the method that you are that you are comfortable with. If you are using a windows client then you need to download WHOIS, there is no need to install anything if you are using Kali Linux.

In this example we will show you how to use WHOIS from windows command line. Download WHOIS from Microsoft from https://docs.microsoft.com/en-us/sysinternals/downloads/whois and extract the files to the C:\ drive root.

Open CMD and type in whois [-v] domainname [whois.server]

```
C:\>whois -v hackthissite.org

Whois v1.20 - Domain information lookup
Copyright (C) 2005-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to ORG.whois-servers.net...
Server ORG.whois-servers.net returned the following for HACKTHISSITE.ORG

Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2019-01-14T03:31:05Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2019-08-10T15:01:25Z
Registrar Registration Expiration Date:
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#clientTransferProhibited
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
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-02-09T22:32:34Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Use internet archives to get old versions of websites

“The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, the print disabled, and the general

public”

Use internet archives like the wayback machine to get old versions of sites and check if you can find vulnerabilities or if you can extract other useful information from old versions of the site.

Use Google Hacking

Google hacking is an information gathering technique that uses Google search queries to identify vulnerabilities in web applications, gather information of individual targets, discover errors, disclosing sensitive data, discover credentials and other sensitive information.For more information on google hacking scripts please search https://www.exploit-db.com

The cache operator finds the recent cache value of a website.

```
cache:www.hackthissite.org
```

The link operator lists pages linking to a specific domain or URL.

```
link:www.hackthissite.org
```

The info operator displays information about a page.

```
info:www.hackthissite.org
```

The site operator restricts the search to a specific site.

```
site:www.hackthissite.org
```

The allinurl operator only returns specified keyword in URL.

```
allinurl:network camera
```

The allintitle operator returns specified keyword in title.

```
allintitle:online-it.nu
```

Website gathering tools

There are many tools one can use to extract and gather information from the targets websites. Below are some examples of browsers plugins and applications that you can use.

- Web Data Extractor 8.3 Link
- Firebug plugin for Chrome
- HTTrack Website Copier For Windows Link

Gathering information from DNS

If the target have some kind of public facing server then they will have some kind of a DNS servers, we can use DNS to gather information about email servers and other servers that the target is utilizing by analyzing the record types of the DNS server. List of DNS records typs.

There are many tools online and offline you can use to gather information about DNS, in this example we are using nslookup, to use nslookup open command line in windows or

shell in linux and type in nslookup and the FQDN or the IP address of the target.

Below are some examples of DNS query’s.

```
# Check DNS A record
C:\>nslookup
Default Server:  8.8.8.8
Address:  8.8.8.8

> set type=a
> www.google.se
Server:  8.8.8.8
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.se
Address:  216.58.207.227
```

```
# Check DNS mx record
C:\>nslookup
Default Server:  8.8.8.8
Address:  8.8.8.8

> set type=mx
> live.se
Server:  8.8.8.8
Address:  8.8.8.8

Non-authoritative answer:
live.se MX preference = 10, mail exchanger = eur.olc.protection.outlook.com

eur.olc.protection.outlook.com  internet address = 104.47.126.33
eur.olc.protection.outlook.com  internet address = 104.47.124.33
```

We have looked at the basic tools you can utility’s when footprinting a target, we have looked on how to find information of a target without interacting whit the target.

The are allot of tools you can use under the footprinting phase, as always google is your best friend, there is tons of information out there.

Check out the Ethical Hacking notes for more Kali Linux quick guides.