Information Gathering

Module 2

Footprinting

- Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.
- Footprinting could be both **passive** and **active**.
- Reviewing a company's website is an example of passive footprinting,
- Whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

What’s Information Gathering ?

- Information gathering is the first phase of penetration testing in which we collect publicly available information or internal information about target while performing active information gathering as well as passive information gathering which we can use it our further testing phases.

- One of the key terms often associated with information gathering is **Open Source Intelligence (OSINT).**

- OSINT is information derived from sources that have no security controls preventing their disclosure.

Information Gathering/Footprinting

Information gathered during this phase includes the following:

- IP address
- Domain Name
- Namespaces
- Employee Information
- Phone Numbers
- Facility information
- Job Information
- Physical Location

Passive Information Gathering

Passive Information Gathering –

- This method can be used before the active information gathering, because is less evasive.

- Only the publicly published information of the target information is used, and it is gathering as much information as possible without establishing contact between the pen-tester and the target.

- For this we can use some opensource tools, for example: *whois* domain, social networks, mail servers, list of applications hosted on the same IP address and other open information.

Active Information Gathering

Active Information Gathering –

- On this type of approach, more preparation is required from the pen-tester because it leaves traces, which can result in the trigger of alerts to the target.
- Using this method, the targeted organization may become aware of the ongoing process since there is an active engaging with the target.
- At this stage, we obtain information about the open ports, services, versions of the applications, version of the operating system, etc.

Scanning

- Scanning focuses on an active engagement of the target with the intention of obtaining more information.
- Scanning target network will ultimately locate active hosts that can be targeted in later phases.
- Basic tools used during this phase :
  - Pings
  - Ping Sweeps
  - Port Scans
  - Tracert

Toolset of the pen-tester for Scanning

Indirect way of retrieving Information:

- The very first tool that everyone should use is Google.
- The Google Hack Database shows you a big list of useful tricks to look for information with the Google Search Engine.
- Maltego is also another tool that help link data with business and email addresses.

The main tool of a pen-tester is a **security-oriented operating system**.

- The major ones are Kali, ParrotSec and BlackArch, Backtrack

Tools for scanning and Information gathering

- **Nmap –** is an open-source network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses, it can also be used to vulnerability scan.
- **OWASP ZAP –** is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.
- **nslookup –** this is an available command-line tool in every computer for querying the Domain Name System to obtain domain names or IP addresses or even other DNS records.

#Many other tools exist but are more specific depending on the results of the ones mentioned above.

Google Hacking:

- The process involves using advanced operators to fine-tune results a user wants.
- It is possible to obtains items such as passwords, certain file types, sensitive folders, logon portals, configuration data and other data.
- Following operators can be used
  - site: <website name> <keywords> - restrict the search to location specific
  - allinurl: <keywords> – return results with specific query in the url.
  - link: <website name> - used to list any web pages that contain links to the page or site specified in query.
  - allintitle: <website> - return page with specified keywords in their title.
  - info:<website name> - presents information about listed pages.
  - cache:<website name> - display version of web page that google contains in its cache.

https://www.exploit-db.com/google-hacking-database

#explore Netcraft: https://www.netcraft.com

Location and Geography

- Google Maps
- Google earth
- Bing maps

Domain Name Information

- You can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

- The Whois database will provide information about the DNS server and the contact information of a domain.
- Whois is a protocol for searching internet registrations, databases for registered domain names, IPs, and autonomous systems. This protocol is specified in RFC 3912 (https://www.ietf.org/rfc/rfc3912.txt).

Domain Name Information

```
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: http://whois.educause.edu

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail.  The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

-----------------------------------------------------------

Domain Name: SOMAIYA.EDU

Registrant:
        K.J. SOMAIYA & SONS
        Somaiya Bhavan, 45/47 Mahatma Gandhi Road
        Fort
        Mumbai, MAHARASHTRA 400001
        India
```

WHOIS Lookup

Search domain name registration records

```
-----------------------------------------------------------

Domain Name: SOMAIYA.EDU

Registrant:
        K.J. SOMAIYA & SONS
        Somaiya Bhavan, 45/47 Mahatma Gandhi Road
        Fort
        Mumbai, MAHARASHTRA 400001
        India

Administrative Contact:
        SAMIR SOMAIYA
        SOMAIYA, SAMIR
        45-47 M. G. Road, Fort
        MUMBAI, 400001
        India
        +91.2222048272
        samir@somaiya.com

Technical Contact:
        Mahaveer Devannavar
        Somaiya Vidyavihar
        K. J. Somaiya Institute of Management Studies and Research,
        Room No: 108, First Floor, Vidyavihar [East]
        Mumbai, 400077
        India
        +91.2267283095
        mahaveer@somaiya.edu

Name Servers:
        NS-1831.AWSDNS-36.CO.UK
        NS-1184.AWSDNS-20.ORG
        NS-307.AWSDNS-38.COM
        NS-893.AWSDNS-47.NET

Domain record activated:    15-Oct-1996
Domain record last updated: 04-Jun-2021
Domain expires:             31-Jul-2024
```

Domain Name Information

- Whois is a protocol for searching internet registrations, databases for registered domain names, IPs, and autonomous systems. This protocol is specified in RFC 3912 (https://www.ietf.org/rfc/rfc3912.txt).

- By default, Kali Linux already comes with a **whois** client. To find out the Whois information for a domain, just type the following command:

```
# whois example.com
```

- The following is the result of the Whois information:

```
Domain Name: EXAMPLE.COM
   Registrar: RESERVED-INTERNET ASSIGNED NUMBERS AUTHORITY
Sponsoring Registrar IANA ID: 376
   Whois Server: whois.iana.org
   Referral URL: http://res-dom.iana.org
   Name Server: A.IANA-SERVERS.NET
   Name Server: B.IANA-SERVERS.NET
   Updated Date: 14-aug-2015
   Creation Date: 14-aug-1995
   Expiration Date: 13-aug-2016
>>> Last update of whois database: Wed, 03 Feb 2016 01:29:37 GMT <<<
```

Analysing the DNS records

- Goal of using the tools in the DNS records category is to collect information about the DNS servers and the corresponding records of a target domain.
- Common Tools:
  - Host
  - Dig
  - DMitry
  - Maltego

The following are several common DNS record types:

No.	Record type	Description
1	SOA	This is the start of authority record.
2	NS	This is the name server record.
3	A	This is the IPv4 address record.
4	MX	This is the mail exchange record.
5	PTR	This is the pointer record.
6	AAAA	This is the IPv6 address record.
7	CNAME	This is the abbreviation for canonical name. It is used as an alias name for another canonical domain name.

Analysing the DNS records: **Host**

- After we get the DNS server information, the next step is to find out the IP address of a hostname.

- Host: command-line tool to look up the IP address of a host from a DNS server.

```
# host hackthissite.org
```

- The host command looks for these records by querying the DNS servers listed in the /etc/resolv.conf file of your Kali Linux system.

Analyzing the DNS records: **dig**

- Besides the host command, you can also use the dig command to do DNS interrogation.

```
# dig hackthissite.org
```

```
# dig hackthissite.org
; <<>> DiG 9.9.5-9+deb8u5-Debian <<>> hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44321
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;hackthissite.org.    IN  A
;; ANSWER SECTION:
hackthissite.org.  5  IN  A  198.148.81.139
hackthissite.org.  5  IN  A  198.148.81.137
hackthissite.org.  5  IN  A  198.148.81.138
hackthissite.org.  5  IN  A  198.148.81.135
hackthissite.org.  5  IN  A  198.148.81.136
;; Query time: 80 msec
;; SERVER: 172.16.43.2#53(172.16.43.2)
;; WHEN: Tue Feb 02 18:16:06 PST 2016
;; MSG SIZE  rcvd: 125
```

Analyzing the DNS records: **dig**

- By default, the **host** command will look for the A, AAAA, and MX records of a domain. To query for any records, just give the -a option to the command:

```
# host –a hackthissite.org
```

```
# host -a hackthissite.org
Trying "hackthissite.org"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32115
;; flags: qr rd ra; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;hackthissite.org.    IN  ANY
;; ANSWER SECTION:
hackthissite.org.  5  IN  A  198.148.81.135
hackthissite.org.  5  IN  A  198.148.81.139
hackthissite.org.  5  IN  A  198.148.81.137
hackthissite.org.  5  IN  A  198.148.81.136
hackthissite.org.  5  IN  A  198.148.81.138
hackthissite.org.  5  IN  NS  ns1.hackthissite.org.
hackthissite.org.  5  IN  NS  c.ns.buddyns.com.
hackthissite.org.  5  IN  NS  f.ns.buddyns.com.
hackthissite.org.  5  IN  NS  e.ns.buddyns.com.
hackthissite.org.  5  IN  NS  ns2.hackthissite.org.
hackthissite.org.  5  IN  NS  b.ns.buddyns.com.
hackthissite.org.  5  IN  NS  d.ns.buddyns.com.
Received 244 bytes from 172.16.43.2#53 in 34 ms
```

Analyzing the DNS records: **dig**

- Deepmagic Information Gathering Tool (DMitry) is an all-in-one information gathering tool. It can be used to gather the following information:
  - The Whois record of a host by using the IP address or domain name
  - Host information from https://www.netcraft.com/
  - Subdomains in the target domain
  - The email address of the target domain
  - Open, filtered, or closed port lists on the target machine by performing a port scan

Analyzing the DNS records: **Maltego**

- Maltego is an open source intelligence and forensics application.
- It allows you to mine and gather information and represent the information in a meaningful way.
- The phrase open source in Maltego means that it gathers information from open source resources.
- After gathering the information, Maltego allows you to identify the key relationship between the information gathered.
- graphically display the links between data

Analyzing the DNS records: **Maltego**

- Maltego allows you to enumerate the following internet infrastructure information:
  - Domain names
  - DNS names
  - Whois information
  - Network blocks
  - IP addresses

Analyzing the DNS records: **Maltego**

It can also be used to gather the following information about people:

- Companies and organizations related to the person
- Email addresses related to the person
- Websites related to the person
- Social networks related to the person
- Phone numbers related to the person
- Social media information

#Kali Linux, by default, comes with Maltego 3.6.1 Kali Linux edition.

DNS Interrogation using dnsenum

- **DNS enumeration** is the technique of probing specific DNS records for a specific organization's domain. In other words, we ask a DNS server about the IP addresses and server names for a target organization.
- Additionally, we attempt to perform a DNS zone transfer.
- A **DNS zone transfer** would allow the ***zone*** file to be copied from a master DNS server to another DNS server, such as a secondary DNS server.

- dnsenum is a very simple and easy-to-use tool for enumerating and resolving DNS information for a given target.
- It has the ability to automatically perform DNS zone transfers using the **nameserver** details

DNS Interrogation using dnsenum

- Use dnsenum zonetransfer.me command to perform DNS enumeration on the zonetransfer.me domain

- dnsenum will attempt to obtain all of the servers and hostnames for the given domain. We are able to obtain the nameservers, mail servers (used for email exchange), and IP addresses for each server and hostname found.

```
root@kali:~# dnsenum zonetransfer.me
Smartmatch is experimental at /usr/bin/dnsenum line 698.
Smartmatch is experimental at /usr/bin/dnsenum line 698.
dnsenum VERSION:1.2.4

-----   zonetransfer.me   -----


Host's addresses:
__________________

zonetransfer.me.                         7199     IN    A        5.196.105.14


Name Servers:
______________

nsztm1.digi.ninja.                       10799    IN    A        81.4.108.41
nsztm2.digi.ninja.                       10799    IN    A        34.225.33.2


Mail (MX) Servers:
___________________

ASPMX.L.GOOGLE.COM.                      292      IN    A        173.194.68.27
ALT1.ASPMX.L.GOOGLE.COM.                 292      IN    A        172.217.192.27
ASPMX2.GOOGLEMAIL.COM.                   292      IN    A        172.217.192.27
ALT2.ASPMX.L.GOOGLE.COM.                 292      IN    A        209.85.202.27
ASPMX3.GOOGLEMAIL.COM.                   292      IN    A        209.85.202.26
ASPMX4.GOOGLEMAIL.COM.                   292      IN    A        173.194.76.26
ASPMX5.GOOGLEMAIL.COM.                   292      IN    A        74.125.128.26
```

DNS Interrogation using dnsenum

- dnsenum will attempt to perform a DNS zone transfer by querying the specific nameservers found during the enumeration process, as shown in the following screenshot:

```
Trying Zone Transfers and getting Bind Versions:
_______________________________________________


Trying Zone Transfer for zonetransfer.me on nsztm1.digi.ninja ...
zonetransfer.me.                         7200     IN    SOA                (
zonetransfer.me.                         300      IN    HINFO        "Casio
zonetransfer.me.                         301      IN    TXT                (
zonetransfer.me.                         7200     IN    MX                 0
zonetransfer.me.                         7200     IN    MX                10
zonetransfer.me.                         7200     IN    MX                10
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    MX                20
zonetransfer.me.                         7200     IN    A        5.196.105.14
zonetransfer.me.                         7200     IN    NS       nsztm1.digi.ninja.
zonetransfer.me.                         7200     IN    NS       nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me.               14000    IN    SRV                0
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me. 7200     IN    PTR      www.zonetransfer.me.
asfdbauthdns.zonetransfer.me.            7900     IN    AFSDB              1
asfdbbox.zonetransfer.me.                7200     IN    A         127.0.0.1
asfdbvolume.zonetransfer.me.             7800     IN    AFSDB              1
canberra-office.zonetransfer.me.         7200     IN    A        202.14.81.230
cmdexec.zonetransfer.me.                 300      IN    TXT               ";
contact.zonetransfer.me.                 2592000  IN    TXT                (
dc-office.zonetransfer.me.               7200     IN    A        143.228.181.132
deadbeef.zonetransfer.me.                7201     IN    AAAA     dead:beaf::
dr.zonetransfer.me.                      300      IN    LOC               53
```

Using the host utility to perform DNS analysis

```
┌──(kali㉿kali)-[~]
└─$ host zonetransfer.me
zonetransfer.me has address 5.196.105.14
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
zonetransfer.me mail is handled by
```

```
┌──(kali㉿kali)-[~]
└─$ host hackthissite.org
hackthissite.org has address 137.74.187.101
hackthissite.org has address 137.74.187.104
hackthissite.org has address 137.74.187.102
hackthissite.org has address 137.74.187.103
hackthissite.org has address 137.74.187.100
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:101
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:104
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:100
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:102
hackthissite.org has IPv6 address 2001:41d0:8:ccd8:137:74:187:103
hackthissite.org mail is handled by 20 alt2.aspmx.l.google.com.
hackthissite.org mail is handled by 30 aspmx5.googlemail.com.
hackthissite.org mail is handled by 20 alt1.aspmx.l.google.com.
hackthissite.org mail is handled by 30 aspmx2.googlemail.com.
hackthissite.org mail is handled by 30 aspmx3.googlemail.com.
hackthissite.org mail is handled by 10 aspmx.l.google.com.
hackthissite.org mail is handled by 30 aspmx4.googlemail.com.
```

Using the host utility to perform DNS analysis

- Use the host -t ns zonetransfer.me command to attempt enumeration by obtaining the nameservers for the domain. The -t operator allows you to specify the DNS record:

```
root@kali:~# host -t ns zonetransfer.me
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
```

Using the host utility to perform DNS analysis

- Now that we have obtained the nameservers for the domain, let's use the information we have gathered so far.
- Let's attempt to perform a DNS zone transfer by querying nameservers for the domain by using the `host -l zonetransfer.me nsztml.digi.ninja` command, as shown in the following screenshot:

```
root@kali:~# host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 5.196.105.14
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
14.105.196.5.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransf
er.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
home.zonetransfer.me has address 127.0.0.1
internal.zonetransfer.me name server intns1.zonetransfer.me.
```

query all nameservers for a given domain—sometimes, one server may be misconfigured even though the others are secured.

DNS Enumeration

SpiderFoot:

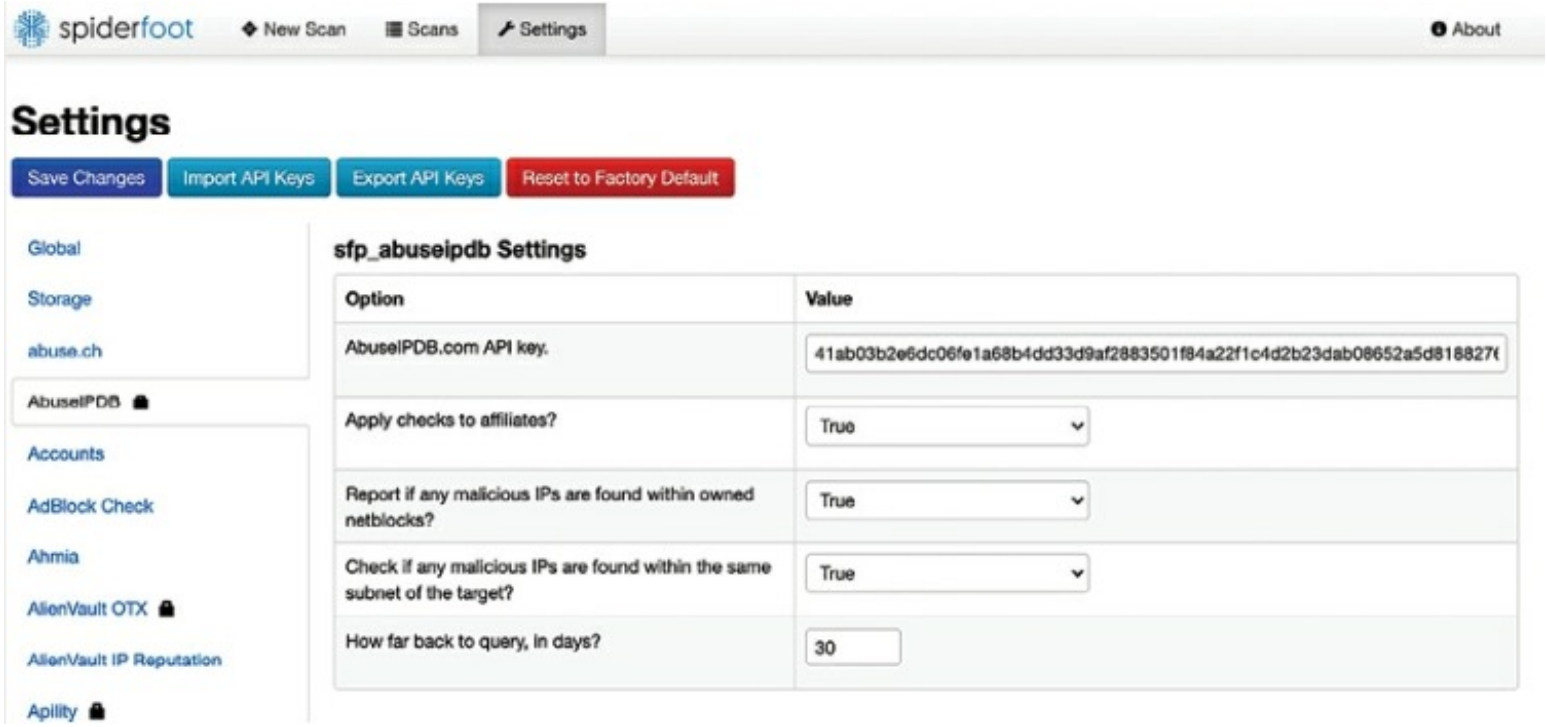
- automates both offensive and defensive passive reconnaissance using OSINT.
- written in Python 3 with the GPL license, and it is preinstalled in the latest version of Kali.
- provides the option to configure a number of APIs to strengthen the outcome.

```
└─# spiderfoot -l 10.0.2.15:8009
Starting web server at http://10.0.2.15:8009 ...


*************************************************************
 Use SpiderFoot by starting your web browser of choice and
 browse to http://10.0.2.15:8009
*************************************************************


[25/Apr/2021:18:18:47] ENGINE Listening for SIGTERM.
[25/Apr/2021:18:18:47] ENGINE Listening for SIGHUP.
[25/Apr/2021:18:18:47] ENGINE Listening for SIGUSR1.
[25/Apr/2021:18:18:47] ENGINE Bus STARTING
[25/Apr/2021:18:18:47] ENGINE Started monitor thread '_TimeoutMonitor'.
[25/Apr/2021:18:18:47] ENGINE Serving on http://10.0.2.15:8009
[25/Apr/2021:18:18:47] ENGINE Bus STARTED
```

DNS Enumeration

SpiderFoot:

- automates both offensive and defensive passive reconnaissance using OSINT.
- written in Python 3 with the GPL license, and it is preinstalled in the latest version of Kali.
- provides the option to configure a number of APIs to strengthen the outcome.



Active Information Gathering

- Active information gathering uses a direct approach to engage with our target; it involves making a connection between our machine and the target network and systems.

- We gather information like, live hosts, running services and application versions, network file shares, and user account information.

- Performing active information gathering does pose a risk of detection.

- Determining live hosts will give us an idea of the number of devices that are online.
- Knowing the operating system and running services on a target helps us to understand the role of that device in the network and the resources it provides to its clients.

Nmap Introduction

- Nmap is the world's leading port scanner, and a popular part of our hosted security tools. Nmap, as an online port scanner, can scan your perimeter network devices and servers from an external perspective ie outside your firewall.

- Nmap, short for Network Mapper, is a network discovery and security auditing tool.

- Nmap is widely used by network administrators to scan for
  - Open ports and services
  - Discover services along with their versions
  - Guess the operating system running on a target machine
  - Get accurate packet routes till the target machine
  - Monitoring hosts

Nmap Introduction

Host Identification:

1. Sending Ping i.e., ICMP Echo Request to all IP addresses in the network. This is often referred to as Ping Sweep.

- Not a very good approach in discovering assets as it is most likely that system on the network will ignore incoming pings due to firewall blocking.

- Better Approach: sending different types of packets to a system to determine if system is alive or not.

2. Nmap will send following packets to the system:

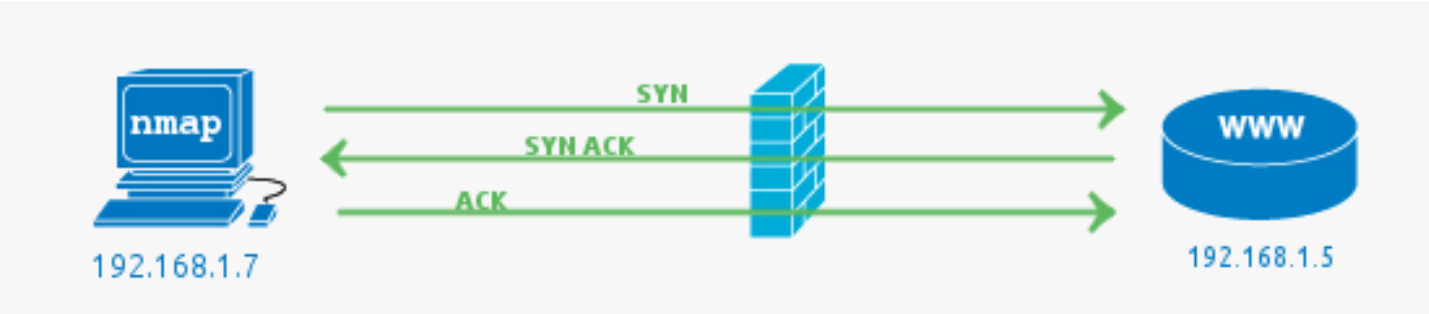
- ICMP Echo request
- TCP SYN packet to port 443
- TCP ACK packet to port 80
- ICMP timestamp request

Understanding Open, Closed and Filtered

The 3-way TCP handshake:

- This involves a SYN sent to an TCP open port that has a service bound to it, typical examples are HTTP (port 80), SMTP (port 25), POP3 (port 110) or SSH (port 22).

- The server side will see the SYN and respond with SYN ACK, with the client answering the SYN ACK with an ACK. This completes the set up and the data of the service protocol can now be communicated.



Understanding Open, Closed and Filtered

<u>An Open Port</u> (service) is found:

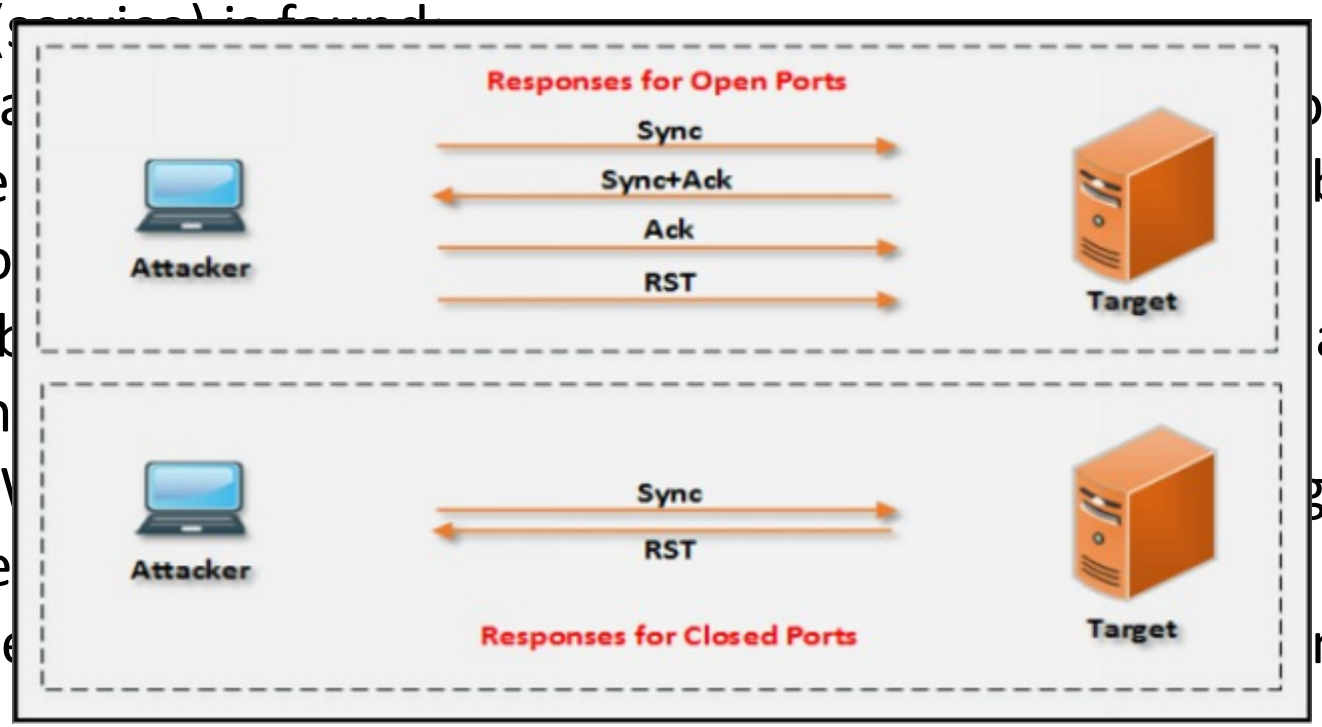
- Open Ports are usually what you are looking for when kicking off Nmap scans.
- The open service could be a publicly accessible service that is, by its nature, supposed to be accessible.
- It may be a back-end service that does not need to be publicly accessible, and therefore should be blocked by a firewall.
- Notice that Wireshark captures RST packet sent after accepting the SYN + ACK from the web server.
- This RST is sent by Nmap as state of the port has been determined by SYN + ACK.

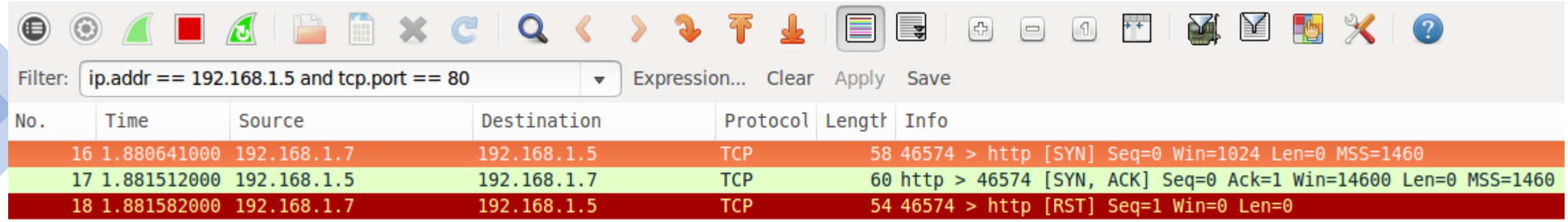
Understanding Open, Closed and Filtered

<u>An Open Port (</u>

- Open Ports a
- The open se
  supposed to
- It may be a b
  therefore sh
- Notice that W
  from the we
- This RST is se

off Nmap scans.
by its nature,
accessible, and
g the SYN + ACK
ned by SYN + ACK.

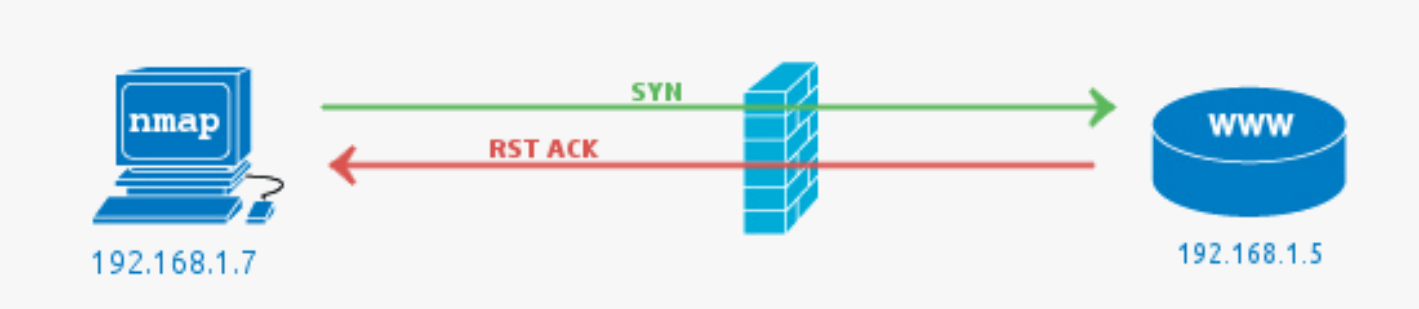




Understanding Open, Closed and Filtered

<u>Closed ports</u> (when the Firewall fails):

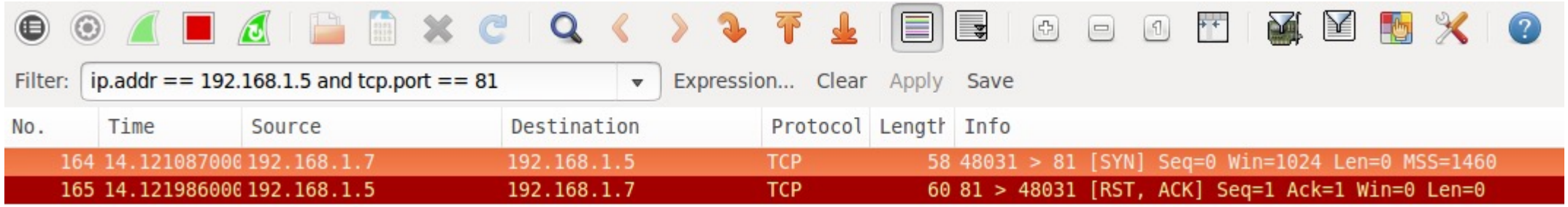
- closed ports most commonly indicate there is no service running on the port, but the firewall has allowed the connection to go through to the server.
- It can also mean no firewall is present at all.
- it is possible to configure a firewall to reject packets rather than drop. This would mean packets hitting the firewall would be seen as closed (the firewall is responding with RST ACK).
- Pictured below is a case where a firewall rule allows the packet on port 81 through even though there is no service listening on the port. This is most likely because the firewall is poorly configured.



Understanding Open, Closed and Filtered

<u>Closed ports</u> (when the Firewall fails):

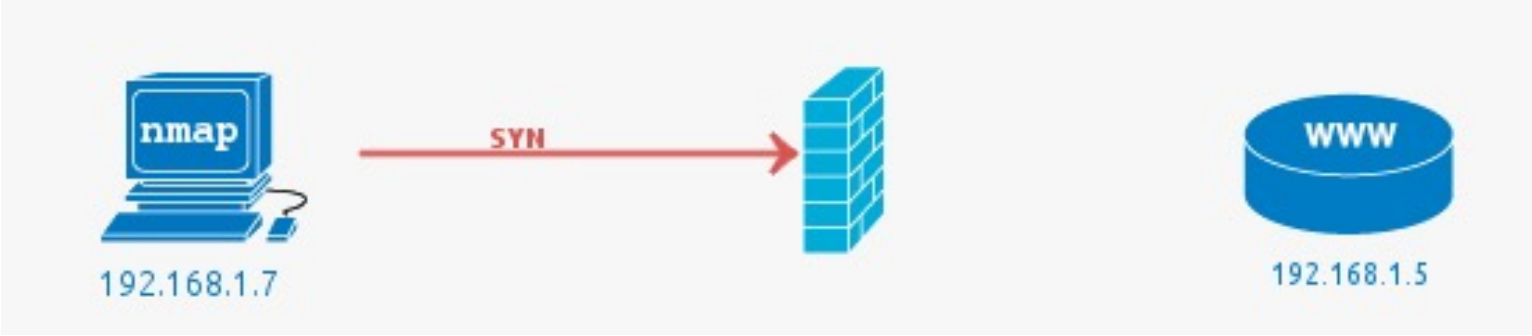
- closed ports most commonly indicate there is no service running on the port, but the firewall has allowed the connection to go through to the server.
- It can also mean no firewall is present at all.
- it is possible to configure a firewall to reject packets rather than drop. This would mean packets hitting the firewall would be seen as closed (the firewall is responding with RST ACK).
- Pictured below is a case where a firewall rule allows the packet on port 81 through even though there is no service listening on the port. This is most likely because the firewall is poorly configured.



Understanding Open, Closed and Filtered

<u>Filtered ports</u> (when the Firewall drops a packet):

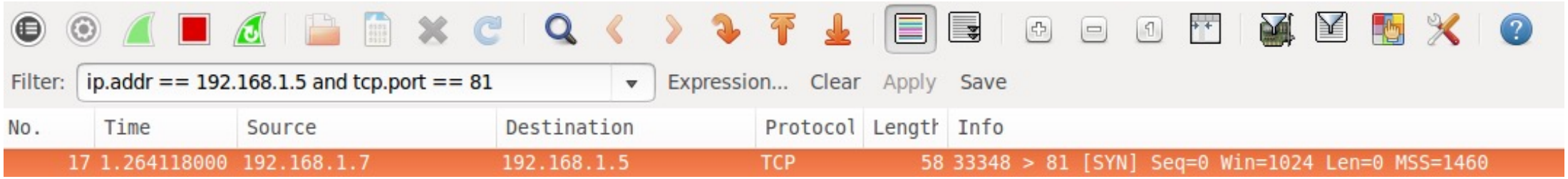
- The job of a firewall is to protect a system from unwanted packets that could harm the system.
- In this simple example, the port scan is conducted against port 81, as there is no service running on this port, using a firewall to block access to it is best practice.



Understanding Open, Closed and Filtered

<u>Filtered ports</u> (when the Firewall drops a packet):

- A filtered port result from Nmap indicates that the port has not responded at all.
- The SYN packet has simply been dropped by the firewall.
- See the following Wireshark packet capture that shows the initial packet with no response.



Nmap Scan Types

TCP SCAN

- A TCP scan is used to check and complete a three-way handshake between you and a chosen target system.
- A TCP scan is generally very noisy and can be detected with almost little to no effort.
  - This is “noisy” because the services can log the sender IP address and might trigger Intrusion Detection Systems.

UDP SCAN

- UDP scans are used to check whether there is any UDP port up and listening for incoming requests on the target machine.
- Unlike TCP, UDP has no mechanism to respond with a positive acknowledgment, so there is always a chance for a false positive in the scan results.
- UDP scans are used to reveal Trojan horses that might be running on UDP ports or even reveal hidden RPC services.
- This type of scan tends to be quite slow because machines tend to slow down their responses to this kind of traffic as a precautionary measure.

Nmap Scan Types

SYN SCAN

- This is another form of TCP scan.
- Difference : unlike a normal TCP scan, **nmap** itself crafts a syn packet, which is the first packet that is sent to establish a TCP connection.
- Here, the connection is never formed, rather the responses to these specially crafted packets are analyzed by Nmap to produce scan results.

ACK SCAN

- ACK scans are used to determine whether a particular port is filtered or not.
- This proves to be extremely helpful when trying to probe for firewalls and their existing set of rules.
- Simple packet filtering will allow established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not.

Nmap Scan Types

Other NMAP Scan Types:

- FIN Scan
- NULL Scan
- XMASS Scan

Nmap Commands

The barebone syntax of Nmap is: **`$ nmap [FLAGS] [IP]`**

Scanning Techniques

Flag	Use	Example
-sS	TCP syn port scan	nmap -sS 192.168.1.1
-sT	TCP connect port scan	nmap -sT 192.168.1.1
–sU	UDP port scan	nmap –sU 192.168.1.1
–sA	TCP ack port scan	nmap –sA 192.168.1.1

Service Version and OS Detection

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Port Specification

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

Host Discovery

Flag	Use	Example
-Pn	only port scan	nmap -Pn192.168.1.1
-sn	only host discover	nmap -sn192.168.1.1
-PR	arp discovery on a local network	nmap -PR192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Operating System Fingerprinting

- Ability to identify Operating system based on network traffic that is end is known as Operating system fingerprinting.
- Typically done using TCP/IP stack fingerprinting techniques.
- Following points provide a guess what OS remote system is running:
  - Differences in how OS responds
  - Differences in versions of an OS responds
  - What TCP options they support
  - Order in which they send packet and lot other details.

NMAP Scripts

- Nmap functionality can be extended using NMAP Scripts
- Nmap scripting engine allows in-depth target enumeration and information gathering.
- Nmap has around 600 scripts serving different purposes.

- In kali Linux, scripts can be found at `/usr/share/nmap/scrpits`

NMAP Scripts

HTTP Enumeration:

- Common service fond on many hosts
- Runs on port 80 by default
- It can be invoked using the command

  namp –script http-enum <target IP address>

- Output:

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -script http-enum 192.168.134.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-06 20:43 EST
Nmap scan report for 192.168.134.129
Host is up (0.00076s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:0C:29:64:7B:14 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.00 seconds
```

NMAP Scripts

HTTP Methods:

- Supports use of various methods such as GET, POST, DELETE and so on.
- Scripts `http-methods` can be used
- Additional NMAP scripts HTTP enumeration
  - http-title
  - http-method-taper
  - http trace
  - http-fetch
  - http-wordpress-enum
  - http-devframework
  - http NSE Library

NMAP Scripts

SMB Enumeration:

NMAP Scripts

DNS Enumeration:

NMAP Scripts

FTP Enumeration:

NMAP Scripts

MySQL Enumeration:

NMAP Scripts

SSH Enumeration:

NMAP Scripts

SMTP Enumeration:

NMAP Scripts

VNC Enumeration: