AST

Audit de Sécurité Technique

Chapter 2.2
Enumeration, Reconnaissance and Scanning

Abraham Rubinstein

abraham.rubinstein@heig-vd.ch

heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Penetration testing

- **Penetration testing** - process of finding and exploiting vulnerabilities in information security systems that an actual black-hat attacker can exploit and break the information system leading to loss of information
  - Searching for vulnerabilities and exploiting them in a controlled circumstances
  - In a professional, safe manner according to carefully designed scope and rules of engagement
  - To determine the potential impact and business risk
  - A subset of ethical hacking activities

The why of pentest ?

- To allow the organisation to better understand a given risk
- Find vulnerabilities before bad guys do
- Exploiting flaws allows a better estimation of the probability that a given vulnerability might be exploited
  - Skills of the ethical hacker and time available
- A certain estimation of the impact on the systems and on business

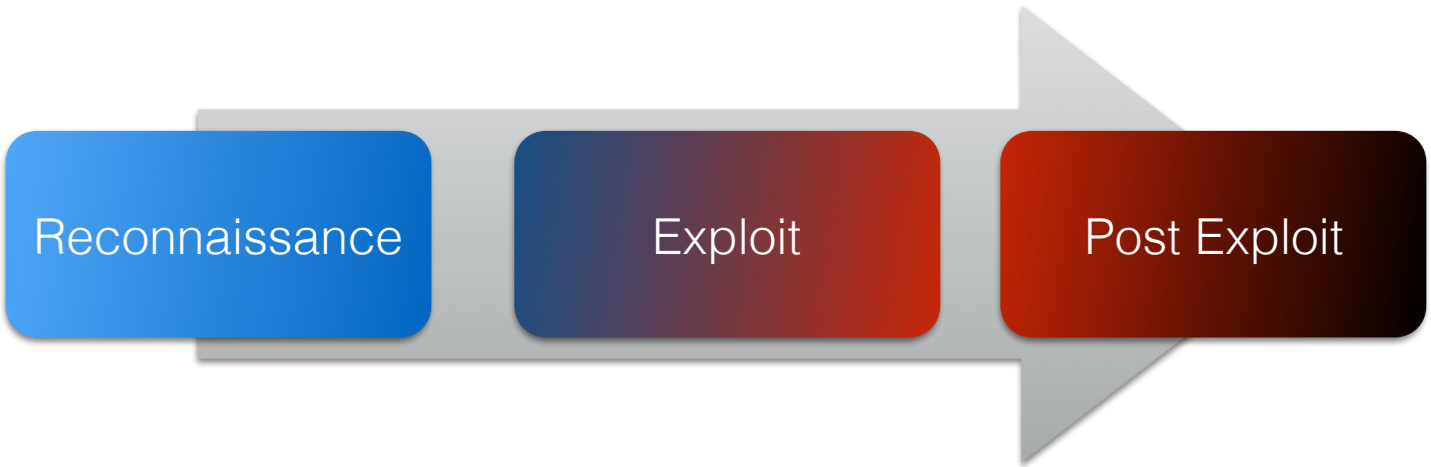
Risk = P(Threat Vulnerability) x Impact

Types of penetration tests

- **Network services** - looking for vulnerabilities on the target systems on the network and exploiting them. Systems can be publicly facing or located within the target's premises (internal network).
- **Client-side** - finding and exploiting vulnerabilities in the client-side software (browsers, media players, etc..)
- **Web application** - looking and exploiting vulnerabilities in web-bases applications
- **Mobile application** - looking and exploiting vulnerabilities in mobile applications on iOS/Android platforms
- **Wireless security** - looking for unauthorised wireless AP or AP with security weaknesses
- **Social engineering** - forcing user to reveal sensitive information
- **Stolen equipment** - involves obtaining a piece of equipment from the target (e.g. corporate laptop computer) and trying to extract sensitive information from it
- **Cryptanalysis attack** - bypassing or breaking the encryption on a local system or across the network. Can also involve evaluation of digital rights management (DRM) solution.
- **Product security** - looking for security flaws in software products (exploitable buffer overflows, privilege escalation, exposure of unencrypted sensitive data)

Attack Kill Chain

- Malicious and ethical hacker rely on same phases in their attacks
  - **Reconnaissance** - gathering information about target
    - Scanning - finding openings in the perimeter
  - **Exploitation** - exploit target systems to compromise them, possibly getting control of them or causing a denial of service
  - **Keeping control** and covering tracks (mostly black-hat and red teams)



Limitations of Pentest

- Penetration testing cannot find all vulnerabilities in a target environment
- Constraints and limitations of a test
  - Project-oriented
    - Scope limit
    - Time limit
    - Access limit
    - Method limit
      - E.g. no Denial of Service to perform distraction
  - Other factors
    - Skills
    - Imagination
    - Known exploits
      - Majority don't write their own exploits or do not have enough time to write an exploit for a specific flaw found in a specific environment

Security project high-level view

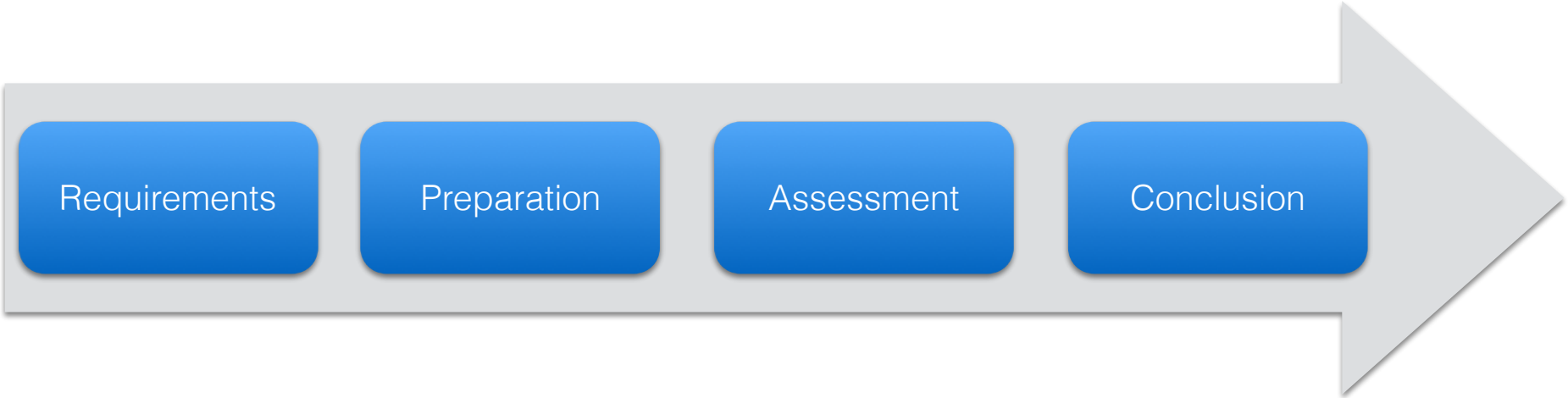


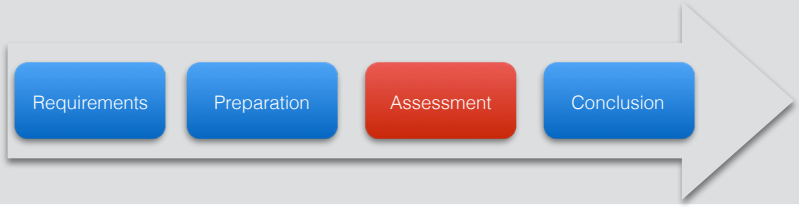
Table of Contents

- Reconnaissance
- Scanning

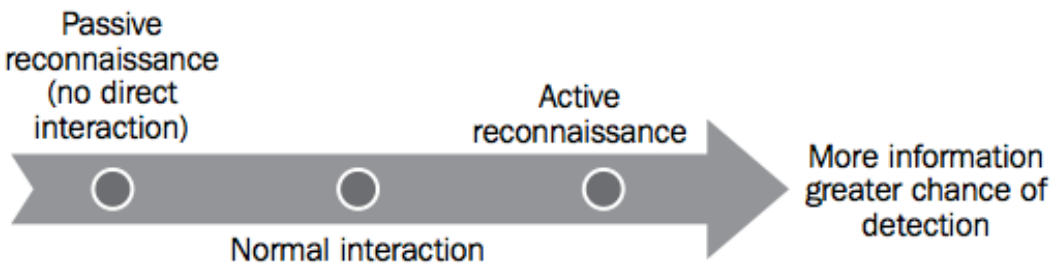
Table of Contents

- **Reconnaissance**
- Scanning

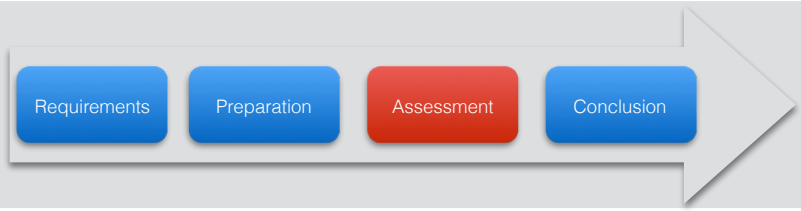
Reconnaissance



- Reconnaissance - the phase where the attacker gathers information from public sources
  - People
  - Business terminology
  - Technical infrastructure
- If budget/time allows, insist on allocating at least one day for the recon



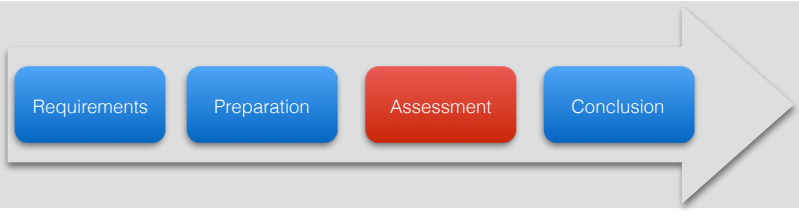
Reconnaissance



- The most obvious way:

… and good imagination !

Inventory

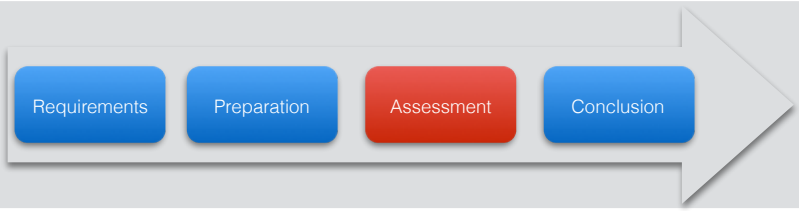


- Throughout your project keep an inventory of what you have discovered or have been provided with

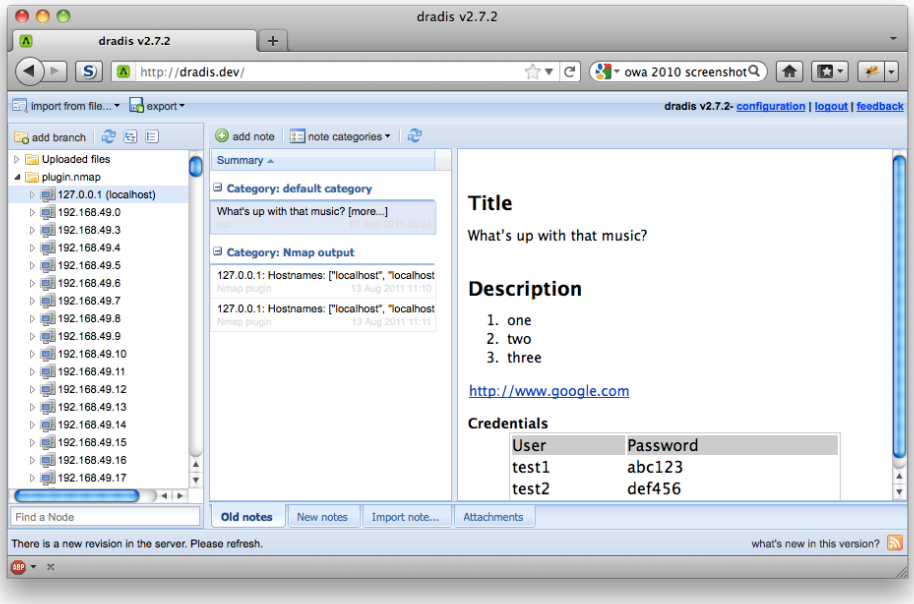
IP address	Name	OS	How Discovered	Open ports	Vulnerabilities	Notes

- The how discovered column is important. Possible methods
  - Provided by the customer
  - Discovered in DNS zone file
  - Discovered during network discovery/network sweep
  - Discovered after pivoting
  - …

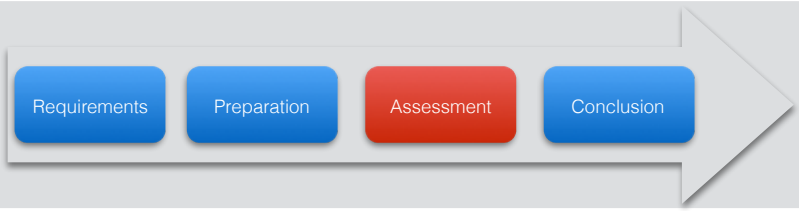
Inventory, Recording and Collaboration



- Some pentesters store their results in a wiki or on git
- Dradis is designed as a collaboration platform for recording and sharing information in a team during security assessment projects
  - http://dradisframework.org/
  - Command-line, GUI and web clients
  - Organised as tree hierarchy
  - Supports importing from Nmap, Nessus, Qualys, Burp
- KeepNote is another option
  - More of a standalone solution



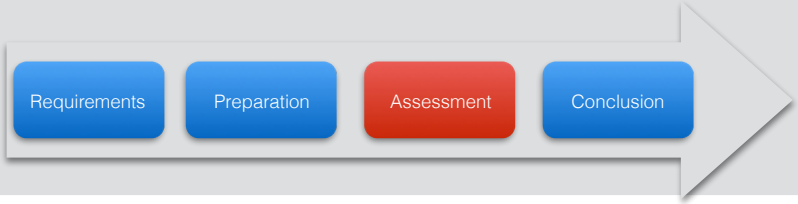
Whois searches



- As an external attacker, you can identify addresses assigned to target site.
- Can provide names, physical addresses, phone numbers and e-mail addresses
  - Useful for social engineering attacks

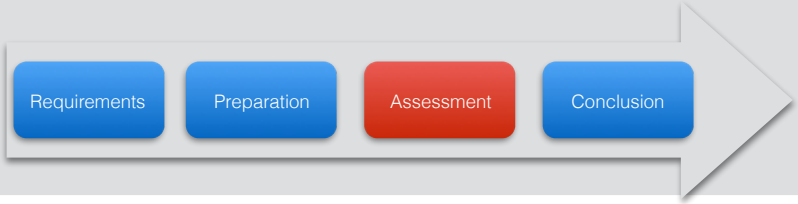
```
root@kali:~# whois heig-vd.ch
whois: This information is subject to an Acceptable Use Policy.
See http://www.nic.ch/terms/aup.html


Domain name:
heig-vd.ch

Holder of domain name:
Haute Ecole d'Ingéniérie et de Gestion du Canton de Vaud
Flückiger Alfred
Informatique
Route de Cheseaux 1
CH-1400 Yverdon-les-Bains
Switzerland
Contractual Language: French

Technical contact:
HEIG-VD
Schlumberger Jérôme
Route de Cheseaux 1
CH-1400 Yverdon-les-Bains
Switzerland

DNSSEC:N

Name servers:
ns01.heig-vd.ch [193.134.218.75]
ns02.heig-vd.ch [193.134.216.115]
scsnms.switch.ch        [130.59.1.30]
scsnms.switch.ch        [130.59.10.30]
scsnms.switch.ch        [2001:620::1]
```

DNS Recon



- Using brute-force attacks, allows attackers to identify new domain names associated with the target.
- If DNS server permits zone transfers to any requester, it will provide you hostnames of internet facing systems.
  - It might even disclose internal IP information if no internal/external segregation is in place
- Finding services that may be vulnerable (for example, FTP) or are otherwise interesting
- Finding misconfigured and/or unpatched servers (dbase.test.target.com)
- Service records (SRV), provide information on service, transport, port, and order of importance for services.

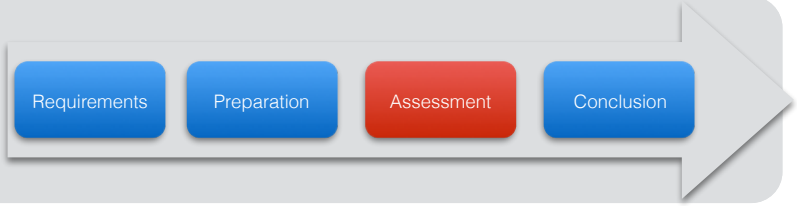
DNS Tools



- `bluto`
  - new tool for domain scan and subdomain enumeration, zone transfers - https://github.com/RandomStorm/Bluto
- `dnsenum`, `dnsmap` and `dnsrecon`
  - DNS scanners, subdomain bruteforce attacks, zone transfers. dnsrecon data can be directly imported into Metasploit
- `dnstracer` - follows the DNS chain back to the server which knows the data
- `fierce` - locates IP space and hostnames from a specified domain by attempting zone transfer and then attempting to brute-force the DNS

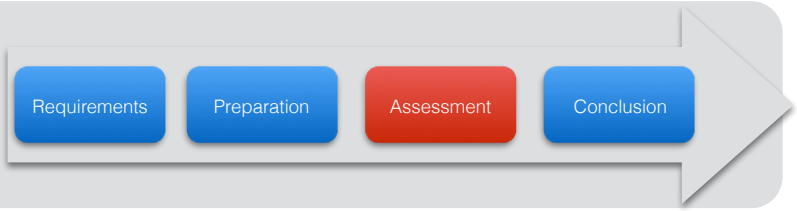
```
root@kali:~# dnsrecon -t std -d heig-vd.ch
[*] Performing General Enumeration of Domain:
[-] DNSSEC is not configured for heig-vd.ch
[*]      SOA ns01.heig-vd.ch 193.134.218.75
[*]      NS ns01.heig-vd.ch 193.134.218.75
[*]      NS scsnms.switch.ch 130.59.1.30
[*]      Bind Version for 130.59.1.30 contact dns-operation@switch.ch
[*]      NS scsnms.switch.ch 130.59.10.30
[*]      Bind Version for 130.59.10.30 contact dns-operation@switch.ch
[*]      NS scsnms.switch.ch 2001:620::1
[*]      NS ns02.heig-vd.ch 193.134.216.115
[*]      MX mailcl1.heig-vd.ch 193.134.216.182
[*]      MX mailcl2.heig-vd.ch 193.134.216.183
[*]      MX mailcl0.heig-vd.ch 193.134.216.181
[*]      TXT heig-vd.ch v=spf1 ip4:193.134.216.180/30 mx ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for heig-vd.ch
[*] 0 Records Found
```

Route to the target



- Route mapping was originally used as a diagnostic tool that allows you to view the route that an IP packet follows from one host to the next. Using the time to live (**TTL**) field in an IP packet, each hop from one point to the next elicits an **ICMP TIME_EXCEEDED** message
- From an attacker's, or penetration tester's perspective, the `traceroute` data yields the following important info:
  - The exact path between the attacker and the target
  - Hints pertaining to the network's external topology
  - Identification of accessing control devices (firewalls and packet-filtering routers) that may be filtering attack traffic

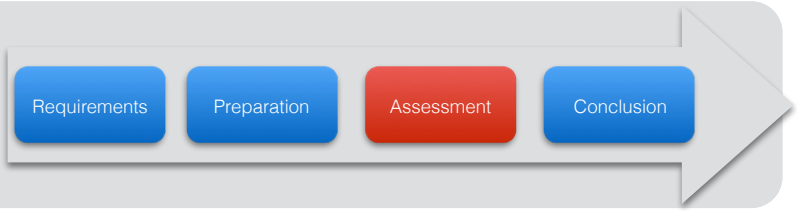
Route to the target



- traceroute uses ICMP packets to map the route
  - in Windows, the program is tracert
- It is likely that you will see most hops filtered (data is shown as * * *)
  - by default, `traceroute` uses UDP
  - traceroute -T uses TCP SYN

```
root@kali:~# traceroute www.google.com
traceroute to www.google.com (24.226.16.35), 30 hops max, 60 byte packets
 1  192.168.117.2 (192.168.117.2)  0.179 ms  0.107 ms  0.099 ms
 2  * * *
 3  * * *
 4  * * *
```

Reconnaissance

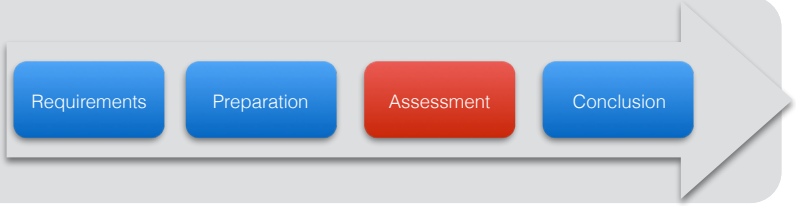


- Those are the most obvious reconnaissance tools
- There are many many more depending on your project, the scope and rules of engagement
- Google for a particular tool
  - In Kali Linux go to
    Applications -> Kali Linux -> Information Gathering
- But always remember to use the tools with due care
  - Don't use the tool unless you know what it does
  - Run a `tcpdump` or `wireshark` to observe the behaviour

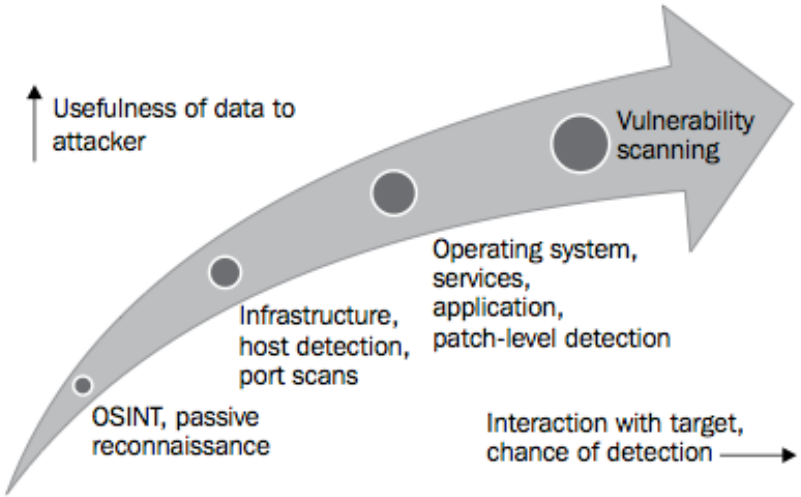
Table of Contents

- Reconnaissance
- **Scanning**

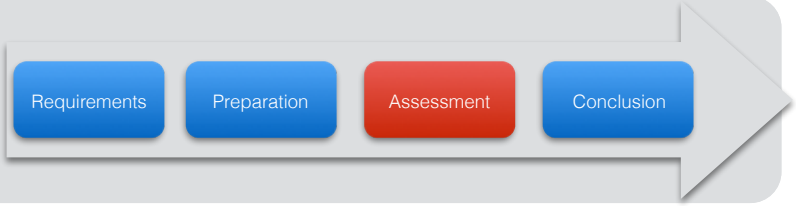
Active Recon



- Previous simple techniques to gather information are almost undetectable
  - Also called Passive Reconnaissance
- Active Reconnaissance - goal is to learn more information about targets and find flaws by interacting with the target environment



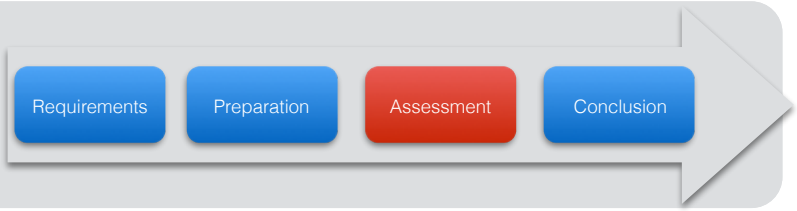
Active Recon



- Most Internet applications communicate using either TCP or UDP protocols
- Most applications have default ports that are used the vast majority of time.
- Example (/etc/services)

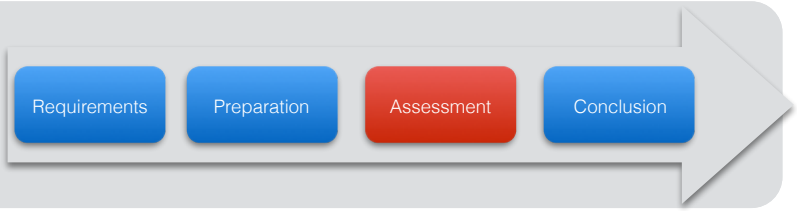
```
ftp-data        20/udp    # File Transfer [Default Data]
ftp-data        20/tcp    # File Transfer [Default Data]
ftp             21/udp    # File Transfer [Control]
ftp             21/tcp    # File Transfer [Control]
ssh             22/udp    # SSH Remote Login Protocol
ssh             22/tcp    # SSH Remote Login Protocol
telnet          23/udp    # Telnet
telnet          23/tcp    # Telnet
smtp            25/udp    # Simple Mail Transfer
smtp            25/tcp    # Simple Mail Transfer
domain          53/udp    # Domain Name Server
domain          53/tcp    # Domain Name Server
tftp            69/udp    # Trivial File Transfer
tftp            69/tcp    # Trivial File Transfer
http            80/udp    www www-http # World Wide Web HTTP
http            80/tcp    www www-http # World Wide Web HTTP
kerberos        88/udp    # Kerberos
kerberos        88/tcp    # Kerberos
pop3           110/udp    # Post Office Protocol - Version 3
pop3           110/tcp    # Post Office Protocol - Version 3
ntp            123/udp    # Network Time Protocol
ntp            123/tcp    # Network Time Protocol
imap           143/udp    # Internet Message Access Protocol
imap           143/tcp    # Internet Message Access Protocol
snmp           161/udp    # SNMP
snmp           161/tcp    # SNMP
```

Scanning



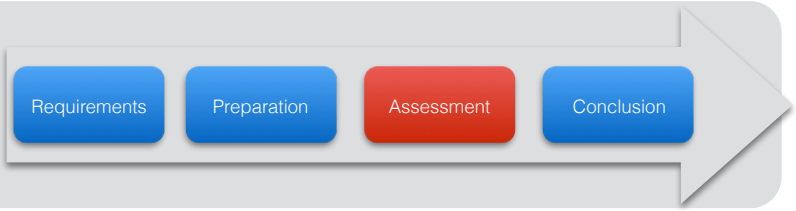
- TCP scanning
  - Send a SYN
    - Receive a SYN/ACK: port open
    - Receive a RST: port closed
    - Receive nothing: port filtered or host down
- UDP scanning
  - More tricky (UDP applications can just discard packets
  - UDP packet sent to a port without an application bound to it — the IP stack should return an ICMP « port unreachable » packet.
    - Get an ICMP packet: port closed
    - Get nothing: either open or filtered
    - Generally takes more time than a TCP scan

Scan Types



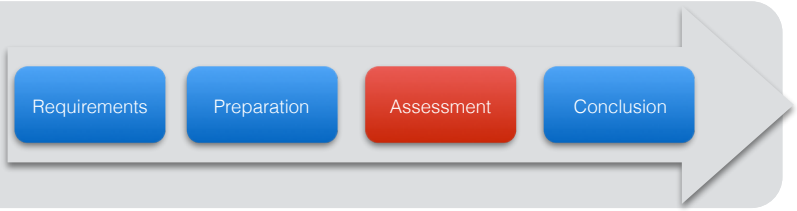
- Network discovery/sweeping - probe the network to identify which hosts are alive
- Port scanning - determine listening TCP and UDP ports on target systems
- OS fingerprinting - determine target device/operating system
- Version scanning - determine the version of services and protocols running on the given TCP and UDP ports
- Vulnerability scanning - determine a list of potential vulnerabilities (misconfigurations, unlatched services, etc.) on target hosts

Scanning IP addresses



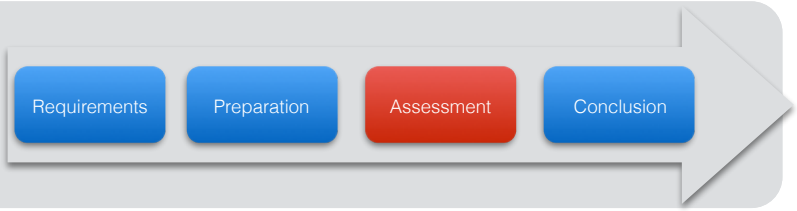
- When scanning and exploiting systems, always use the IP address of the target, not hostnames
  - If you perform you activities based on name, load balancers may alter the target system and corrupt you results
    - Different machines may respond
- For large and very large IP ranges
  - sample a representative subset of hosts
  - sample target ports
    - based on firewall ruleset
  - perform a discovery first

Scan monitoring



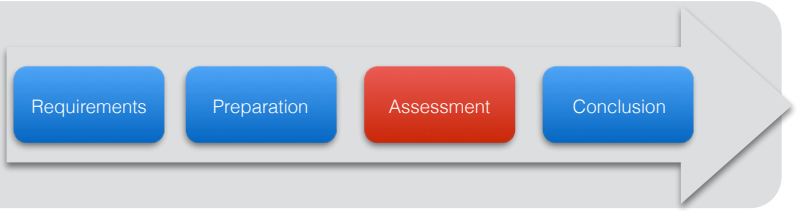
- Whenever you run a scan, run a sniffer so that you can monitor network activity
  - You don't have to capture all the packets into a file
  - Just display them on the screen
  - `tcpdump` is an ideal tool for this purpose
  - run as superuser (`sudo tcpdump`)
  - For a given range, run with the corresponding `net` or `host` argument
    - For example if you scan a `/24` network, run:
      `tcpdump net 192.168.1.0/24`
    - Replace the 192.168.1.0 range with you target range and the mask accordingly

Port Scanning



- Port scanning is the process of connecting to TCP and UDP ports to determine what services and applications are running on the target device.
- There are 65,535 ports each for both TCP and UDP on each system.
- Some ports are known to be associated with particular services (TCP 20 and 21 are the usual ports for the file transfer protocol service (FTP))
- The first 1,024 are the well-known ports, and most defined services run over ports in this range

Nmap



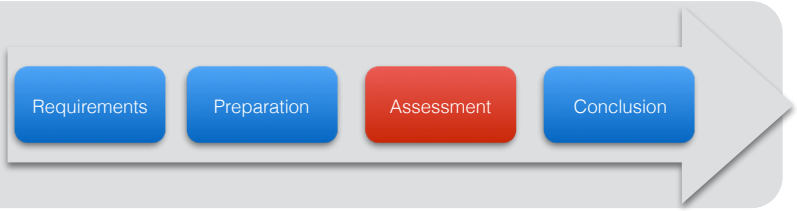
- Nmap is the most popular port scanning tool
  - www.nmap.org
- Not just a port scanner
- Using nmap for port discovery is very noisy—it will be detected and logged by network security devices. Some points to remember are as follows
  - Attackers and penetration testers focused on stealth will test only the ports that impact the kill chain they are following to their specific target. If they are launching an attack that exploits vulnerabilities in a web server, they will search for targets with port 80 or port 8080 accessible
  - Most port scanners have default lists of ports that are scanned—ensure that you know what is on that list and what has been omitted. Consider both TCP and UDP ports
  - Successful scanning requires a deep knowledge of TCP/IP and related protocols, networking, and how particular tools work
  - Port scanning, even when done slowly, can impact a network

Nmap

- The `nmap` tool injects packets into the target network and analyses the response that it receives.
- The `-O` flag commands `nmap` to determine the operating system

```
root@kali:~# nmap -sS -O 127.0.0.1

Starting Nmap 6.47 ( http://nmap.org ) at 2014-10-06 23:46 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.15
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
```

Nmap

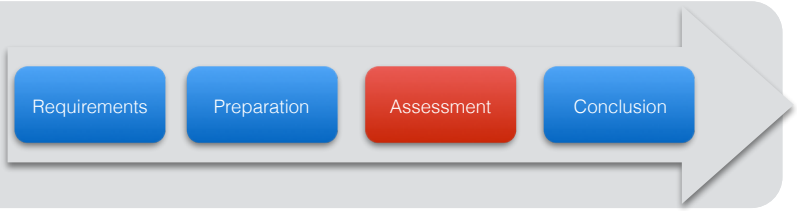


- To perform a ping scan (also called network sweep):
  - `nmap -sn w.x.y.z/nn`
  - Example: `nmap -sn 192.168.1.0/24` will sweep scan the full class C 192.168.1.0 network
  - Example: `nmap -sn 192.168.1.1-10` will sweep scan only first 10 hosts
  - BUT: Only hosts replying to ping will show up !!

Nmap

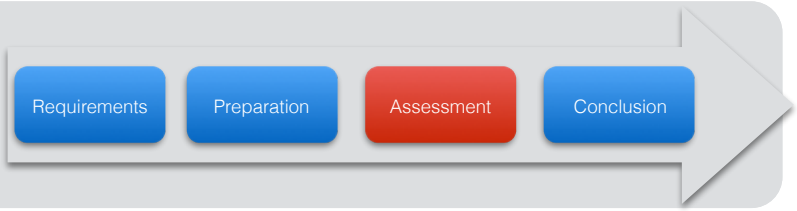
- TCP Scan Types:
  - `-sS` (default): SYN scanning
  - `-sT`: connection scan, which terminates the handshake
  - `-sN` (NULL), `-sF` (FIN), `-sX` (Xmas) and `-sM` (Maimon) scans
  - Packets sent to a closed TCP port without the RST flag set have a RST packet sent in return
  - Packets sent to an open TCP port without one of SYN, RST, or ACK flags set are silently discarded by the IP stack
  - NULL = all flags disabled, FIN = FIN flag set, Xmas = FIN, PSH and URG flags set and Maimon have the FIN and ACK flags set
  - Used especially with stateless firewalls

Nmap



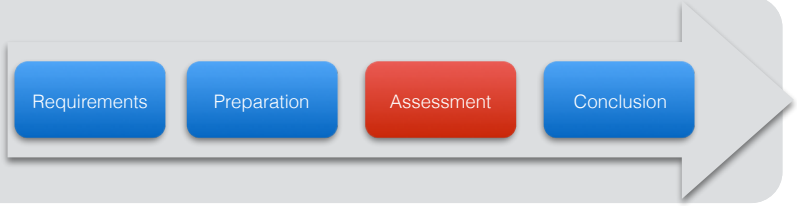
- UDP Scans
  - Empty packet scans
  - `-sU` option. Must be run as root.
  - `-sU -sV` options — send valid application data in UDP packets to ports to see whether an application answers
  - Remember that UDP scans tend to be slow

Nmap



- Scan speed
  - `-T0` (paranoid): send one packet every 5 minutes
  - `-T1` (sneaky): send one packet every 15 seconds
  - `-T2` (polite): send one packet every 0.4 second
  - `-T3` (normal): default behaviour
  - `-T4` (aggressive): lowers host and ports timeouts
  - `-T5` (insane): lowers host and port timeouts even further

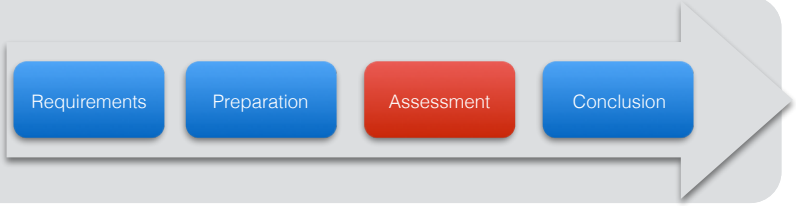
Service fingerprinting



- The final goal of the enumeration portion of reconnaissance is to identify the services and applications that are operational on the target system
- The following are some of the several techniques used to determine active services:
  - **Identify default ports and services**: If the remote system is identified as having a Microsoft operating system with port 80 open (the WWW service), an attacker may assume that a default installation of Microsoft IIS is installed. Additional testing will be used to verify this assumption (nmap).
  - **Banner grabbing**: This is done using tools such as amap, netcat, nmap, and Telnet
  - **Review default web pages**: Some applications install with default administration, error, or other pages. If attackers access these, they will provide guidance on installed applications that may be vulnerable to attack. In the following screenshot, the attacker can easily identify the version of Apache Tomcat that has been installed on the target system.
  - **Review source code**: Poorly configured web-based applications may respond to certain HTTP requests such as HEAD or OPTIONS with a response that includes the web server software version, and possibly, the base operating system or the scripting environment in use.

```
root@kali:~# nc www.heig-vd.ch 80
HEAD /blah.html HTTP/1.0

HTTP/1.1 302 Found
Cache-Control: private
Content-Length: 149
Content-Type: text/html; charset=utf-8
Location: http://www.heig-vd.ch/erreur/404
Server: Microsoft-IIS/7.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 06 Oct 2014 21:55:25 GMT
Connection: close
```

Vulnerability scan



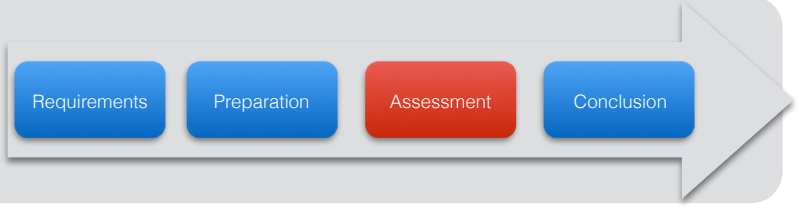
- Vulnerability scanning employs automated processes and applications to identify vulnerabilities in a network, system, operating system, or application that may be exploitable
- When performed correctly, a vulnerability scan delivers an inventory of devices (both authorized and rogue devices), known vulnerabilities that have been actively scanned for, and usually a confirmation of how compliant the devices are with various policies and regulations
- If you thought that port scanning was loud, vulnerability scans are very loud.
  - Stealth is impossible to achieve on mass vulnerability scans

Nmap

vs

Nessus

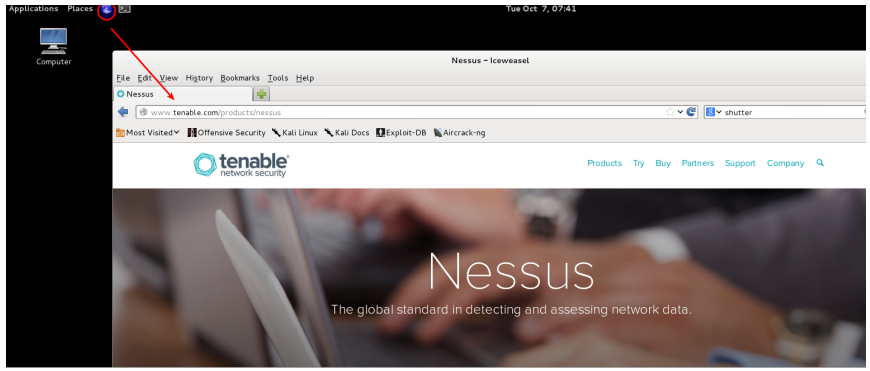
Vulnerability scan



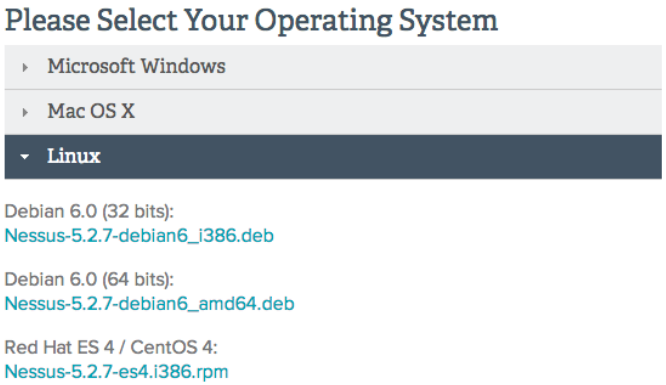
- Even though vulnerability scanners are very powerful tools, they suffer from following limitations:
  - For the most part, vulnerability scanners are signature based—they can only detect known vulnerabilities, and only if there is an existing recognition signature that the scanner can apply to the target
  - Scanners produce large volumes of output, frequently containing false-positive results that can lead a tester astray; in particular, networks with different operating systems can produce false-positives with a rate as high as seventy percent
  - Scanners may have a negative impact on the network—they can create network latency or cause the failure of some devices
    - Running a tcpdump and pinging targets within the scan range is mandatory when scanning IP ranges, especially when you are scanning internal networks

Installing Nessus

- Nessus is one of the most powerful vulnerability scanners
- Unfortunately it is not free - subscription costs $1'500/year
  - Fortunately a free « Home version » exists
- Go to http://www.tenable.com/products/nessus/select-your-operating-system



  - Select Download under Nessus home
- Select your OS (for Kali, choose debian)
- You would need to register in order to receive your activation code http://www.tenable.com/products/nessus-home



Installing Nessus on Kali

- Run
  `sudo dpkg -i Nessus-5.2.7-debian6_amd64.deb`

```
noroot@kali:~$ sudo dpkg -i Nessus-5.2.7-debian6_amd64.deb
[sudo] password for noroot:
Selecting previously unselected package nessus.
(Reading database ... 345878 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.7-debian6_amd64.deb) ...
Setting up nessus (5.2.7) ...
nessusd (Nessus) 5.2.7 [build N25122] for Linux
Copyright (C) 1998 - 2014 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - You can start nessusd by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

noroot@kali:~$
```

- And then `sudo /etc/init.d/nessusd start`
- Open browser and navigate to https://localhost:8834/

Nessus Docker Image

- Unofficial image available on docker hub:

  https://hub.docker.com/r/stevemcgrath/nessus_scanner

- Obtain licence from:

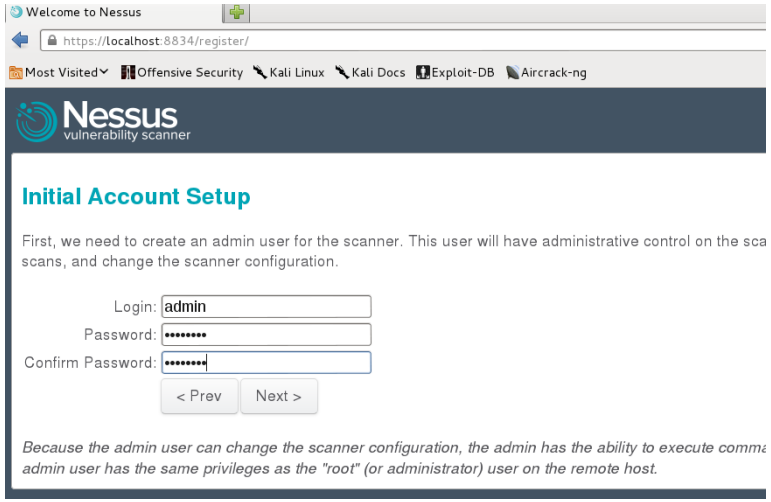
  https://www.tenable.com/products/nessus/nessus-essentials

- Running example:

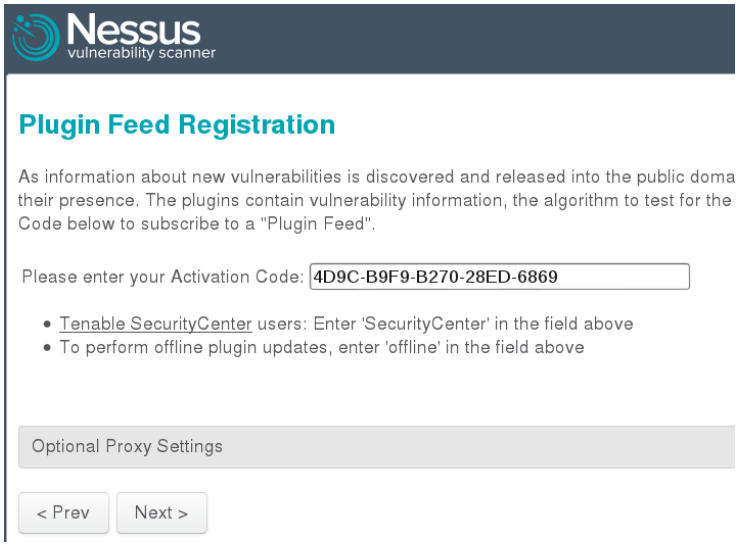
```
docker run -dt -p8834:8834 \
    -e ADMIN_USER="admin" \
    -e ADMIN_PASS="admin" \
    -e LICENSE={XXXX-XXXX-XXXX-XXXX-XXXX}\
    --name nessus_scanner stevemcgrath/nessus_scanner:latest
```

Initialise Nessus

- When first connecting to Nessus Web GUI, you need to create an admin account

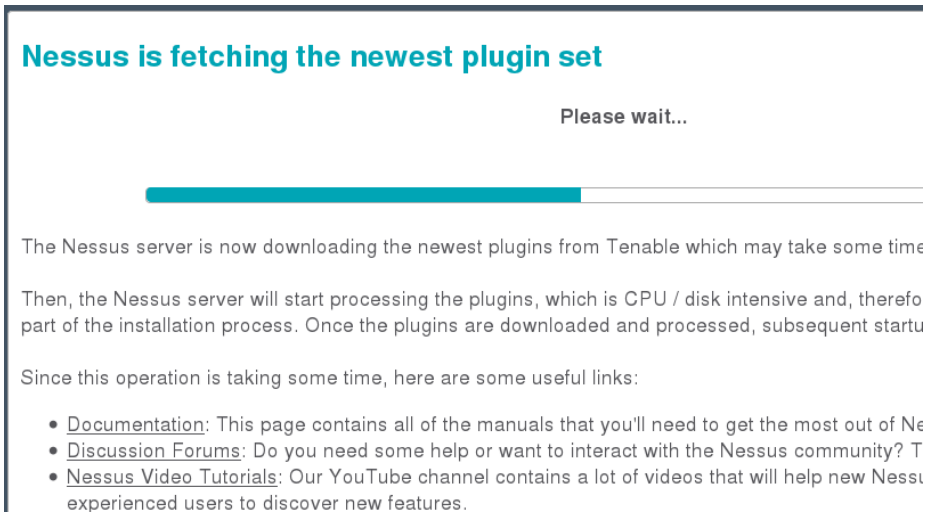


- Enter activation code you have received by email on the next screen



Initialise Nessus

- First time Nessus will take some time fetch all the plugins and set them up



- When the initialisation is finished you will be presented with a login window