IT3789 Cyber Security Attack & Defence

L7 – Vulnerability Identification (1)

NANYANG POLYTECHNIC

WITH KNOWLEDGE COMES RESPONSIBILITY

Vulnerability Identification

Scanning

War Dialling

Network Mapping

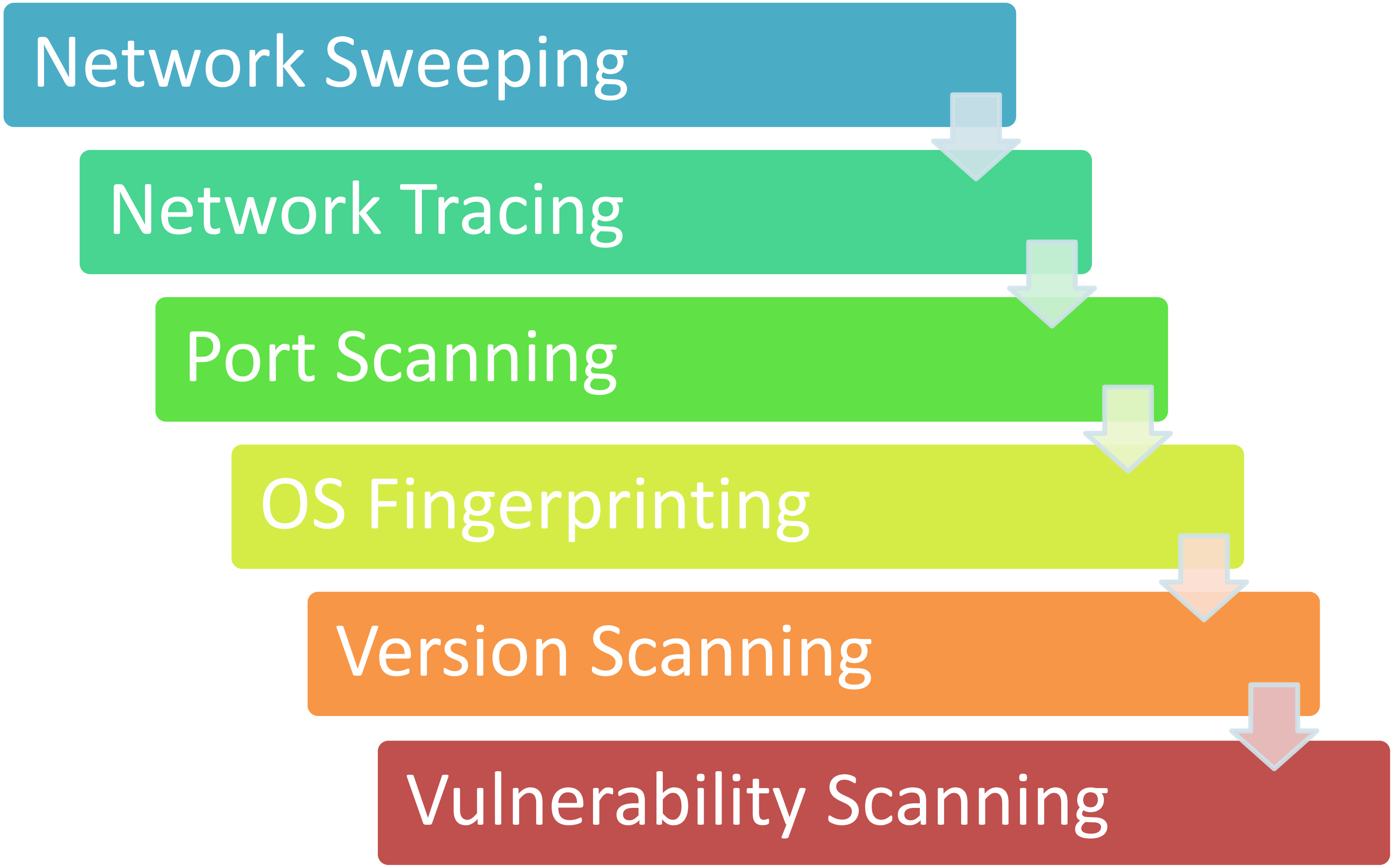
Port Scanning

Vulnerability Scanning

Scanning

- Learn more about targets and find openings by interacting with the target.
- Hacker continues to gather information regarding the target network and its individual hosts.
- Information gathered in this phase help hacker to determine which exploit to use.

Workflow of Scanning Phase



Network Sweeping

Network Tracing

Port Scanning

OS Fingerprinting

Version Scanning

Vulnerability Scanning

Type of Scanning

Network Sweeping

- Send probe packets to all addresses in target range.
- Identify live hosts in the target network.

Network Tracing

- Determine the topology of target network.
- Draw a network map using results from network sweeping.

Port Scanning

- Find openings by looking for listening TCP & UDP ports.
- Specific port numbers gives hints to what services are running in machines.

Type of Scanning

OS fingerprinting

- Determine the operating system based on their network behaviours.
  - Using specially crafted test packets designed to measure the operating system behaviours.
  - Sniffing traffic from the target to determine the kind of operating system.

Version Scanning

- Determine the version of services and protocols by interacting with open TCP and UDP ports.
- Note that administrator may put services on alternative ports.

Vulnerability Scanning

- Determine a list of potential vulnerabilities in the target environment based on findings.
- e.g. Misconfigurations or unpatched services.

Scanning Tips for Penetration Testing

- Scan target using IP address not domain name.
  - Many networks use DNS to perform load balancing and traffic distribution.
  - Results might not be accurate.
    - Unknowingly, multiple hosts are scanned simultaneously.
    - Results merged as if they are from one machine.
    - Expected service derived from results may not exist on target machine.

Scanning Tips for Penetration Testing

- Dealing with large scans
  1. Sample a subset of machines.
     - Choose sample targets with typical configurations that is similar to the other systems.
     - Downside: These sample targets may not accurately represent the other systems.
  2. Sample a subset of target ports.
     - Only scan the most interesting ports.
       - e.g. 21 (FTP), 22 (SSH), 25 (SMTP), 80 (HTTP), etc.
       - http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml
     - Downside: Other ports are not tested and may be vulnerable.

Scanning Tips for Penetration Testing

- Dealing with large scans (cont'd)

  3. Review network firewall ruleset and scan only those ports that is not protected by firewall.

     - Overcomes the downside of sampling targets and specific ports.
     - Downside: Does not measure potential bugs in the firewall.
       - Effort required by target organisation personnel.
       - No longer black box testing.

Scanning Tips for Penetration Testing

- Dealing with large scans (cont'd)
  4. Use hyper-fast port scanning methods.
     - Use multiple machines to scan.
     - Lower timeouts of each scan.
     - Increase number of scan (Eg. # of scan sockets per scan, parallel scans etc.)
     - Use fast scanning tools such as masscan and ScanRand.
       - https://www.sans.org/security-resources/idfaq/what-is-scanrand/3/20
     - Downside: Denial of service attack may occur.
- Run sniffer while scanning.
  - Verify scanning tool is functioning properly by monitoring network activity.
  - tcpdump is ideal as it is small, flexible and fast.

Scanning Tools Recap

- War Diallers
  - Spots badly secured external connection using THC-Scan, PhoneSweep and TeleSweep etc.
- War Driving
  - Scan for wireless access points using Kismet etc.
- Network mappers
  - Ping sweeps, traceroute, Cheops-ng (an automated tool), Maltego etc.
- Port Scanners
  - Scanning for open ports at targeted systems using nmap, zenmap etc.
- Vulnerability Scanners
  - Scan for known vulnerabilities using tools such as Nessus.
    - Misconfigurations
    - Unpatched systems with known vulnerabilities
    - Other weaknesses

Vulnerability Identification

Scanning

War Dialling

Network Mapping

Port Scanning

Vulnerability Scanning

War Dialing

- A technique of dialing telephone numbers to find an open modem connection that provide remote access to a network
  - Remote access to a system or internal network allows attacks to be launched against target.
- Dial up modem connection usually have weaker security than the main Internet connection.
  - Many remote-access systems use the Password Authentication Protocol (PAP) which sends passwords in clear.
  - Many companies do not control dial-in ports as strictly as the firewall.
  - Machines with modem attached can be anywhere even if these modems are no longer required.
  - Many servers still have modem with phone lines connected as backup in case the primary Internet connection fails.

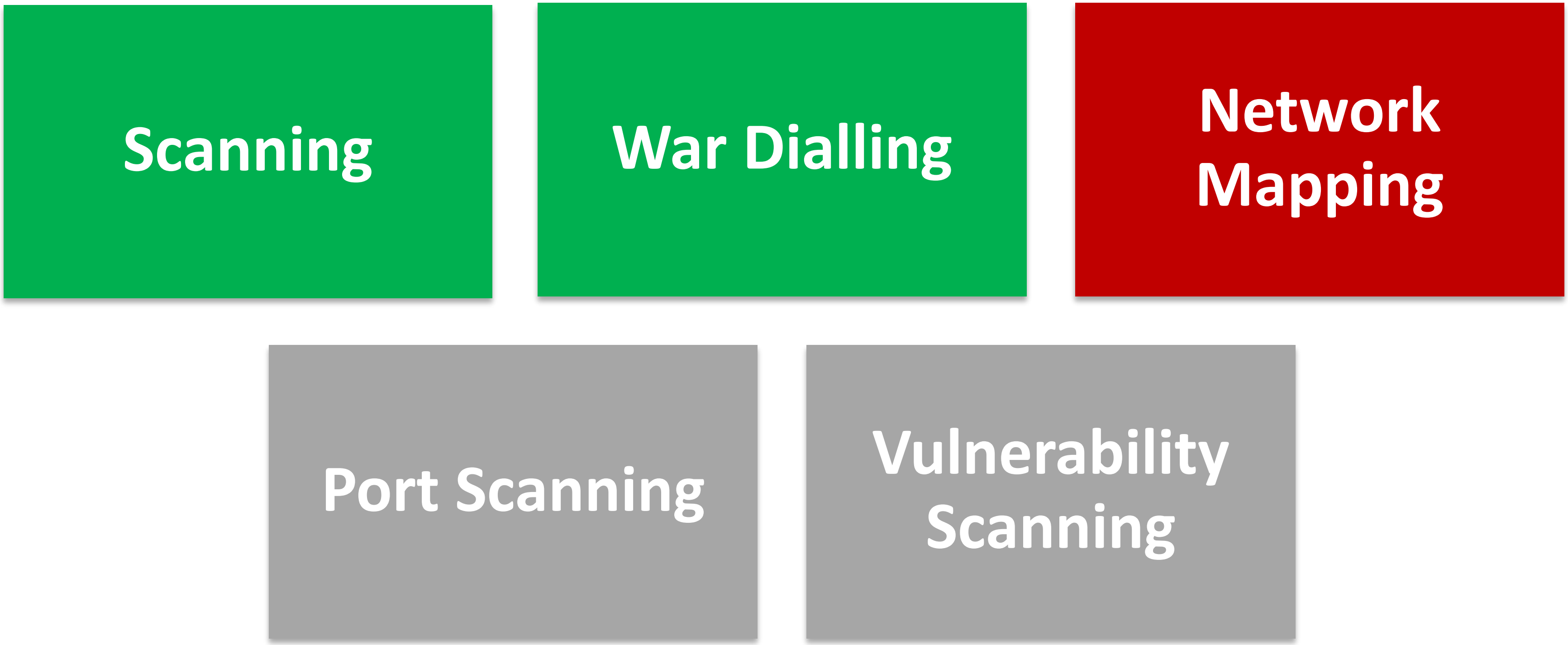
**“One million dollars
in firewalls and security can be
defeated by one cheap modem”**

Sandstorm.net

War Dialing

- War dialer programs
  - THC-Scan, PhoneSweep and TeleSweep.
- After locating modems, tools can:
  - Determine the type of line discovered including carriers, tones, voice mail boxes (VMB).
  - Send nudging sequences to determine the known remote admin tools running on target machine like pcAnywhere and then use client application to log in.
  - Look for systems that don’t require a password.
  - Pass-guess systems that need password using tools like THC-LoginHacker.

Vulnerability Identification



Scanning

War Dialling

Network Mapping

Port Scanning

Vulnerability Scanning

Network Mapping

- IP-based attack rather than phoneline-based attack.
- Scan Internet and organisation’s internal network.
- Determine target network topology.
  - Determine which addresses have live machines.
  - Develop a map of the target network.
- Manual tools like ping or traceroute.
- Automated tools like Cheop-ng on Unix-based machines.

Ping Sweep Technique

- Determine systems are alive by performing a ping sweep of the IP address range.
  - Systems that respond with a ping reply are considered alive.
- Ping sweep is also know as Internet Control Message Protocol (ICMP) scanning.
  - Broadcast ICMP requests to all hosts on a network.
  - The machine with the specified IP address will send an ICMP ECHO reply.

Ping Sweep Technique

- Simple but not necessary accurate.
  - No reply from system does not mean system is not alive.
    - e.g. Systems can be alive but behind firewall.
- Benefit of using ping sweep.
  - It can be run in parallel.
  - All systems can be scanned at the same time.

Simple Ping Sweep Script

```
root@bt:~# ping -c 1 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.051 ms

--- 192.168.1.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.051/0.051/0.051/0.000 ms
```

- Ping command to obtain just the IP address of host that is live.

```
ping -c 1 192.168.1.100 | grep "bytes from" |cut -d" " -f4 |cut -d":" -f1
```

Simple Ping Sweep Script

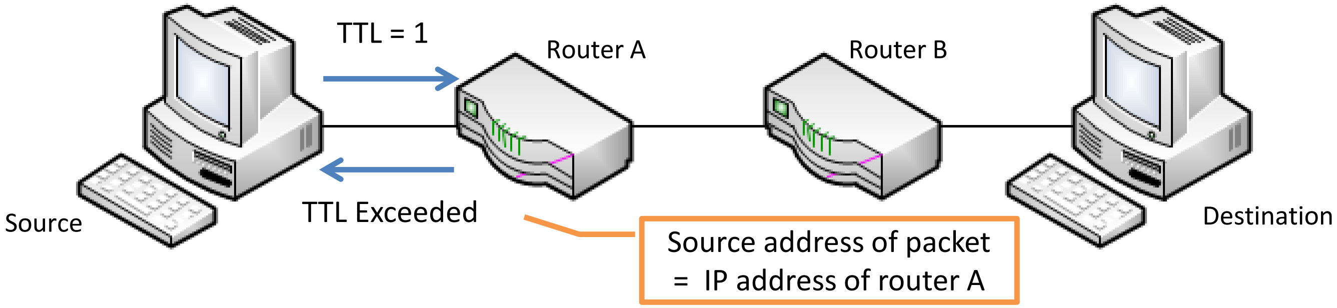
```
#!/bin/bash

if [ -z "$1" ];then
echo "[*] Simple Ping Sweep Script"
echo "[*] Usage     : $0 <Net Range>"
echo "[*] Example   : $0 192.168.10"
exit 0
fi

for ip in $(seq 1 254); do
   ping -c 1 $1.$ip |grep "bytes from" |cut -d" " -f4 |cut -d":" -f1 &
done
```

If 1st argument is null, return true.

To run command concurrently.

Traceroute

- Traceroute sends a sequence of packets addressed to a destination host.
- Packets are sent to target with incremental time-to-live (TTLs).
  - The TTL field is reduced by every host on the route to its destination.
  - If the TTL field reaches zero before the datagram arrives at its destination, it will be dropped.



Source address of packet = IP address of router A

Traceroute

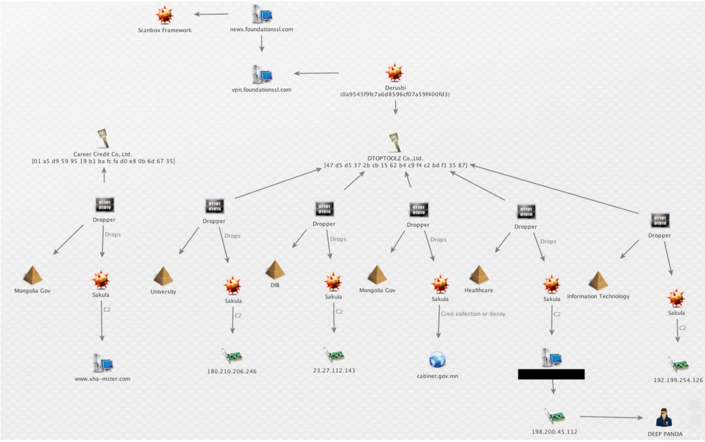
- Discovers the route packets take between two systems.
  - Uses TTL behaviour of routers to determine the addresses of router between attacker and target machine.
- Can be used to draw a map of the target network.
- Found in most operating systems.
  - Linux/Unix : traceroute
  - Windows : tracert

Other Network Sweep Tools

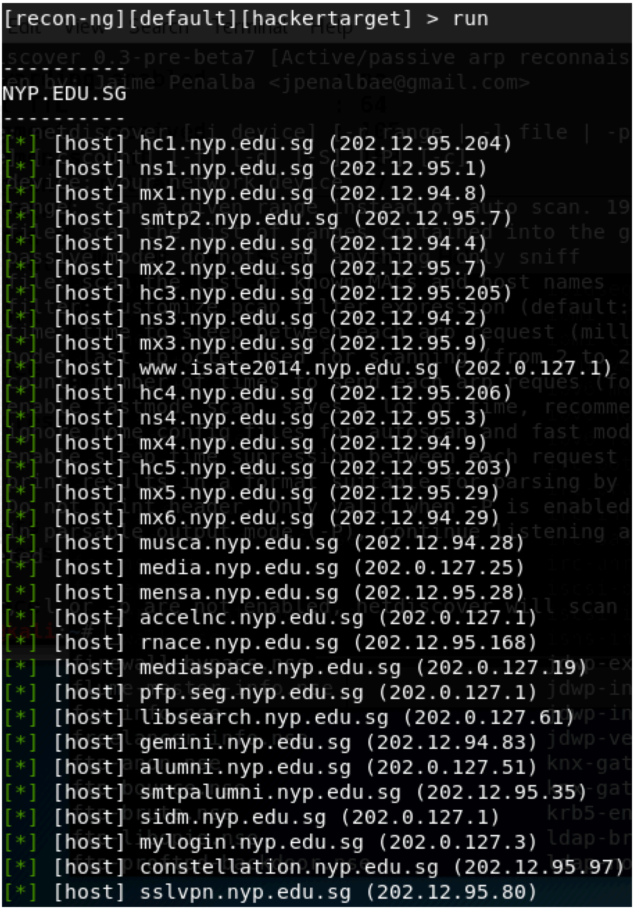
- Angry IP (http://www.angryip.org)
  - GUI-based tool
- ICMPQuery (www.angio.net/security/icmpquery.c)
  - Command line tool for Linux/UNIX
- Hping (http://www.hping.org/)
  - A packet generator and analyzer for the TCP/IP protocol.
  - One of the de-facto tools for security auditing and testing of firewalls and networks.

Other Network Sweep Tools

- Maltego (https://www.paterva.com/web7/)
  - A powerful footprinting tool.



- Recon-ng ()
  - A web reconnaissance framework.



```
[recon-ng][default][hackertarget] > run

-----------
NYP.EDU.SG
-----------
[*] [host] hc1.nyp.edu.sg (202.12.95.204)
[*] [host] ns1.nyp.edu.sg (202.12.95.1)
[*] [host] mx1.nyp.edu.sg (202.12.94.8)
[*] [host] smtp2.nyp.edu.sg (202.12.95.7)
[*] [host] ns2.nyp.edu.sg (202.12.94.4)
[*] [host] mx2.nyp.edu.sg (202.12.95.7)
[*] [host] hc3.nyp.edu.sg (202.12.95.205)
[*] [host] ns3.nyp.edu.sg (202.12.94.2)
[*] [host] mx3.nyp.edu.sg (202.12.95.9)
[*] [host] www.isate2014.nyp.edu.sg (202.0.127.1)
[*] [host] hc4.nyp.edu.sg (202.12.95.206)
[*] [host] ns4.nyp.edu.sg (202.12.95.3)
[*] [host] mx4.nyp.edu.sg (202.12.94.9)
[*] [host] hc5.nyp.edu.sg (202.12.95.203)
[*] [host] mx5.nyp.edu.sg (202.12.95.29)
[*] [host] mx6.nyp.edu.sg (202.12.94.29)
[*] [host] musca.nyp.edu.sg (202.12.94.28)
[*] [host] media.nyp.edu.sg (202.0.127.25)
[*] [host] mensa.nyp.edu.sg (202.12.95.28)
[*] [host] accelnc.nyp.edu.sg (202.0.127.1)
[*] [host] rnace.nyp.edu.sg (202.12.95.168)
[*] [host] mediaspace.nyp.edu.sg (202.0.127.19)
[*] [host] pfp.seg.nyp.edu.sg (202.0.127.1)
[*] [host] libsearch.nyp.edu.sg (202.0.127.61)
[*] [host] gemini.nyp.edu.sg (202.12.94.83)
[*] [host] alumni.nyp.edu.sg (202.0.127.51)
[*] [host] smtpalumni.nyp.edu.sg (202.12.95.35)
[*] [host] sidm.nyp.edu.sg (202.0.127.1)
[*] [host] mylogin.nyp.edu.sg (202.0.127.3)
[*] [host] constellation.nyp.edu.sg (202.12.95.97)
[*] [host] sslvpn.nyp.edu.sg (202.12.95.80)
```

Vulnerability Identification (1)

Scanning

- Type of Scanning
- Workflow of Scanning Phase
- Scanning Tips
- Scanning Tools Recap

War Dialing

Network Mapping

- Ping Sweep Technique
- Traceroute
- Other Network Sweep Tools