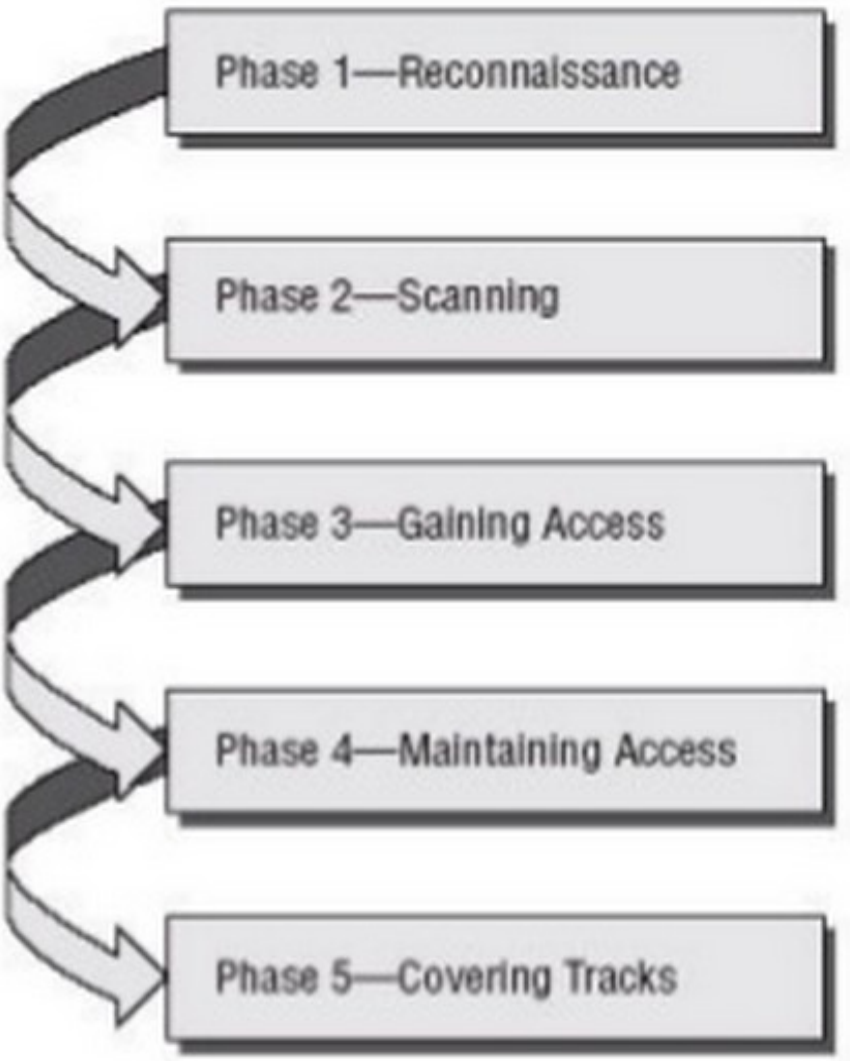
Nmap

Port scanner to Vulnerability analysis

What is Nmap?

- Nmap, short for "network mapper", is an open source utility which can quickly scan broad ranges of devices and provide valuable information about the devices on your network. It can be used for IT auditing and asset discovery as well as for security profiling of the network.

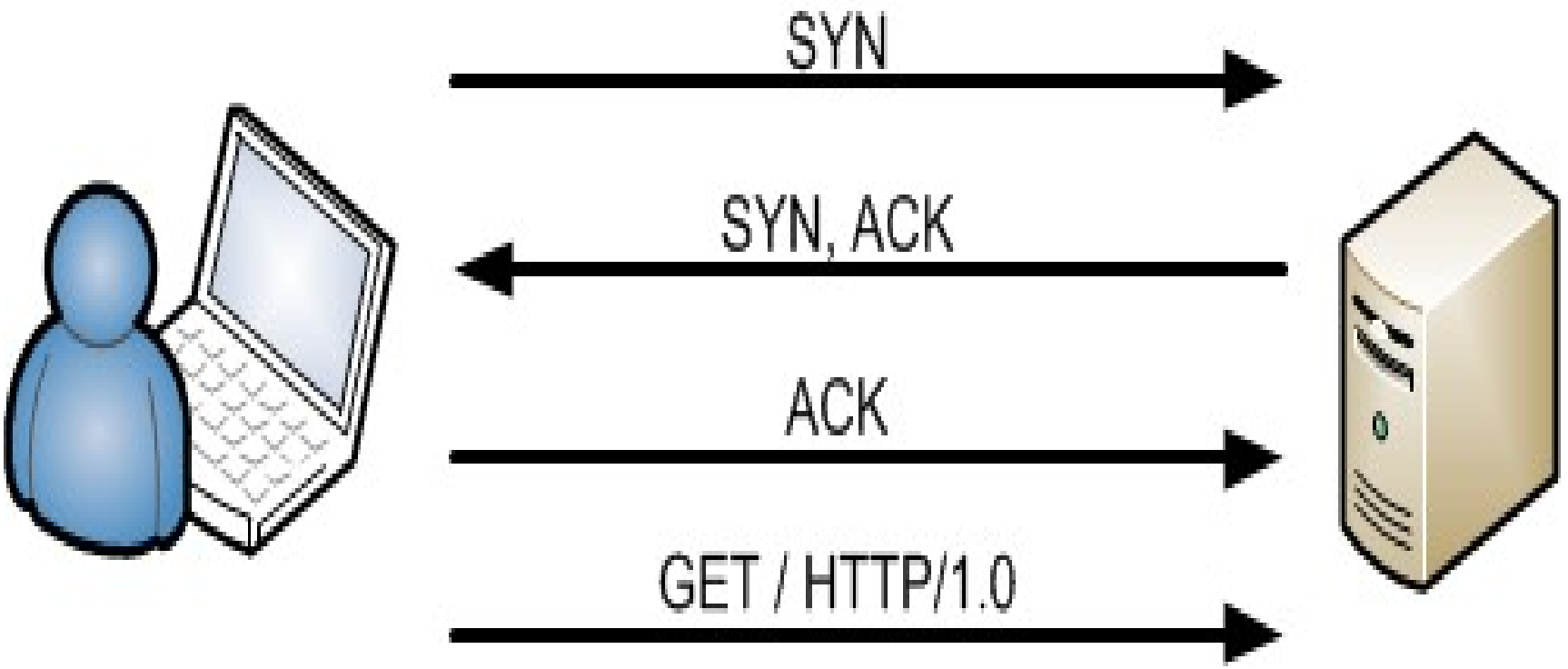
The attack process



Before we proceed?

- Do we know what happens in the TCP handshake

This is it...



Back to nmap, nmap basics...

- Nmap uses raw IP packets to determine what hosts are available on the network, the services that are enabled, the operating system and version of the host, what sort of firewall or packet filters are in place and many other aspects of the network. The information can be used both proactively to identify and correct security holes and by attackers to perform reconnaissance about the types and quantities of targets available and what weaknesses exist.

Nmap basics

- Nmap is available for a wide range of operating system platforms including Linux, Solaris, Free/Net/OpenBSD, Mac OS X and Windows using Zenmap GUI.

Scan techniques

- TCP scanning The simplest port scanners use the operating system's network functions and is generally the next option to go to when SYN is not a feasible option
- SYN scanning SYN scan is another form of TCP scanning. Rather than use the operating system's network functions, the port scanner generates raw IP packets itself, and monitors for responses. This scan type is also known as "half-open scanning", because it never actually opens a full TCP connection.

Scan techniques

- UDP scanning UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message. if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open.
- ACK scanning This kind of scan does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This kind of scan can be good when attempting to probe for the existence of a firewall and its rule sets.

Scan techniques

- Other functions we can get our of nmap
  - OS discovery
  - System Version Information
  - Network Discovery
  - Vulnerability Discovery

Lets get our hands dirty

- apt-get install nmap
- nmap 10.10.0.x #single host
- nmap 10.10.0.0/24 #whole subnet
- nmap 10.10.0.1-5 #few hosts, 1 – 5

- OS detection
  - nmap -A 10.10.0.x
  - nmap -v -A 10.10.0.x

Getting hands dirty

- Nmap ping scan
  - Nmap -sP 10.10.0.0/24
- Activating script-engine
  - -sC flag or - - script to specify script
  - nmap --script smb-check-vulns.nse -p445 10.10.0.146
    - Or nmap --script smb-check-vulns.nse --script-args=unsafe=1 -p445 10.10.0.146