The golden age of hacking

Whois

DNS

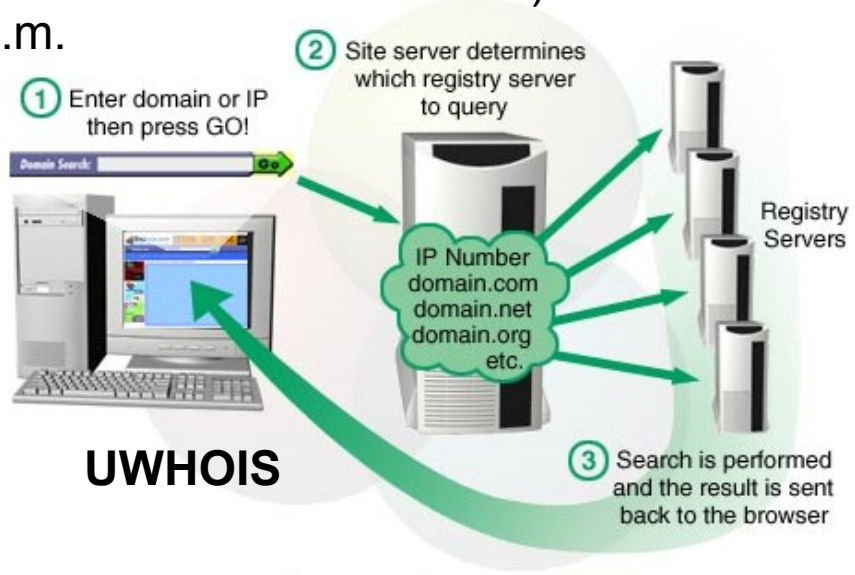
Scanning

IDS and IPS

BT ~ # whois
Usage: whois [OPTION]... OBJECT...

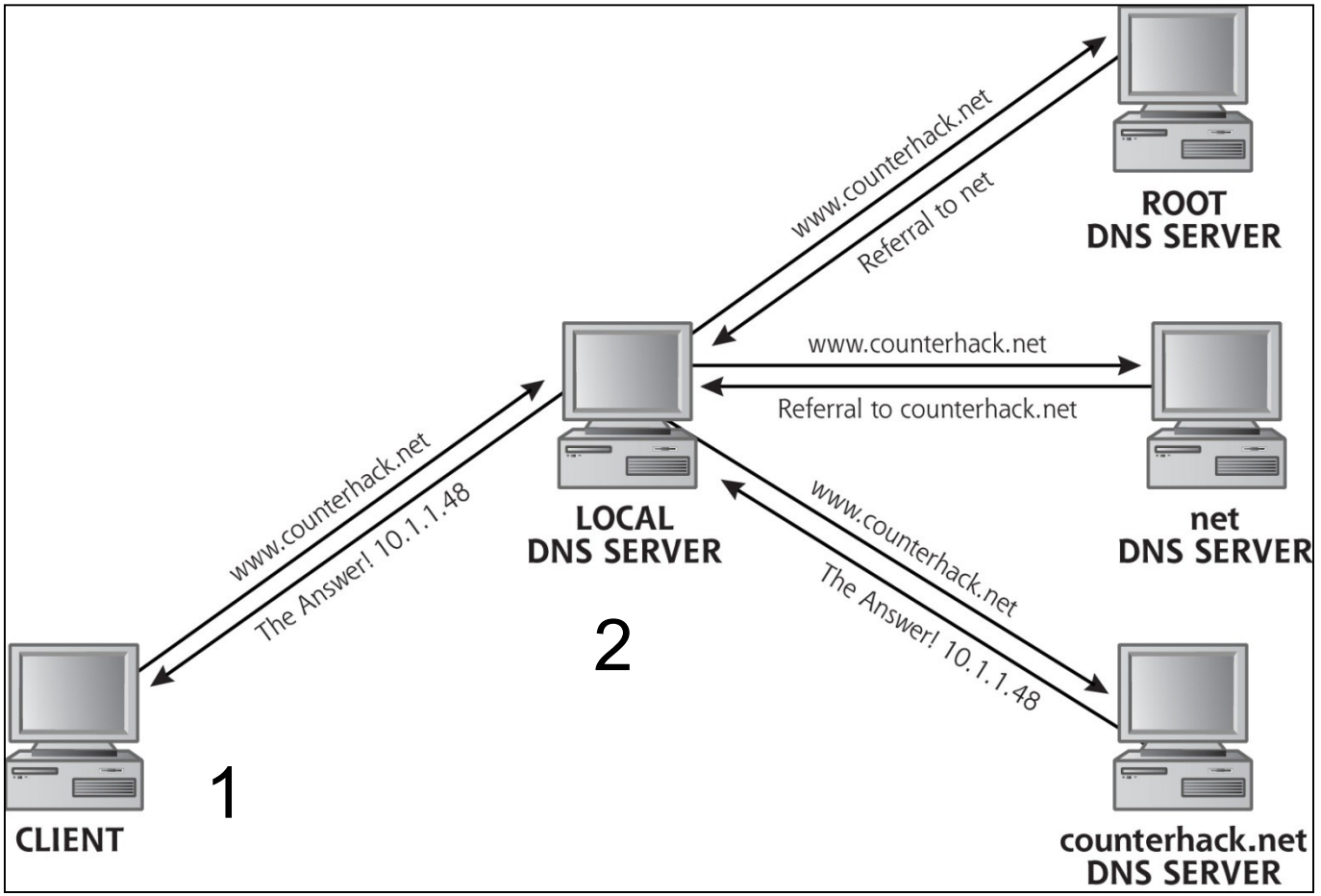
Whois databases

- Registrator for domains - list: www.internic.com
- Who owns a specific domain?
  - www.whois.net, InterNIC or any other WHOIS service
  - www.uwhois.com for country specific .ru .se .uk etc. (universal)
  - Name, phone number, mail, post address, reg. data, name servers
- Who own a specific IP number?
  - Maintains the WHOIS database
    - Maps IP-address to FQDN (Fully Qualified Domain Name) and give info about the FQDN m.m.
    - Often the ISP:s information
  - www.ripe.net (Europe)
  - www.arin.net (USA)
  - www.apnic.net (Asia)
  - www.lacnic.net (South America)
  - www.afrinic.net (Africa)



Forward DNS resolving

- First check the local DNS cache (1) and hosts file
  - ipconfig /displaydns (UNIX cannot easily dump this)
- If not the local DNS server (2) and its cache and so on…

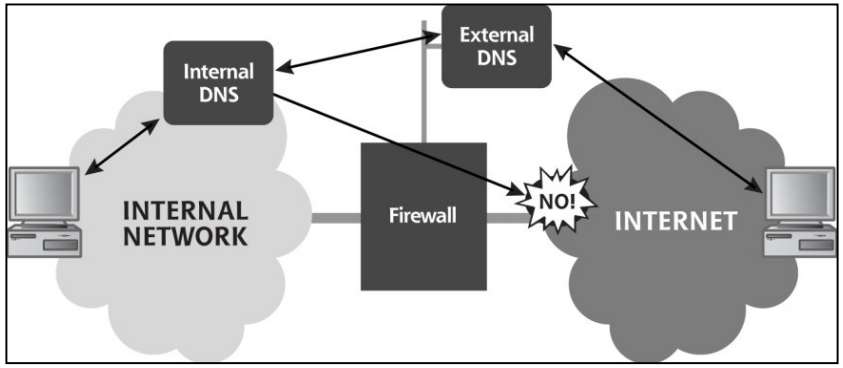


DNS records

- Address (A record)
  - Maps a domain name to a specific IP address
- Alias (CNAME record)
  - Associates an A record with an alias name
- Host information (HINFO record)
  - Associates system information with the domain name
- Mail Exchange (MX record)
  - Identifies the mail servers of the given domain
- Name Server (NS record)
  - Identifies the DNS servers of the given domain
- Text (TXT record)
  - Associates a text with the domain name

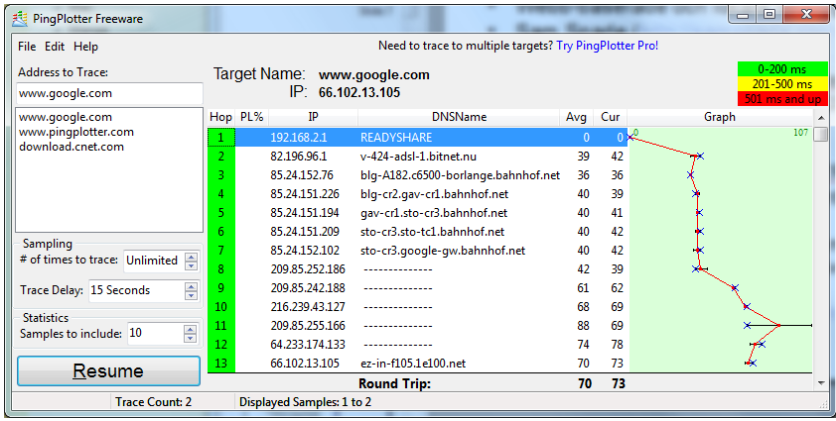
Query DNS servers

- Usually a domain must have at least 2 DNS server in order to be ”qualified” and fault tolerant on Internet
  - Primary and secondary DNS
- DNS services as ZoneEdit.com
  - Static DNS
  - Dynamic DNS
  - Secondary DNS
- Attackers goal
  - Conduct a zone transfer, gets more or less the DNS config file
- Tools
  - host, dig, nslookup (zone transfer not possible in GNU/Linux), etc.
  - Must set tool to use primary or secondary DNS
- Defense
  - Do not use informative names and HINFO or TXT records
  - Restrict zone transfers – only primary to secondary (or tertiary)
  - FW-filter port 53 **TCP** (zone transfers and other large queries) to only allow connections from secondary.UDP 53 is for DNS queries/responses
  - Split DNS – outside can only resolve public DNS names



DNS resolving and GP tools

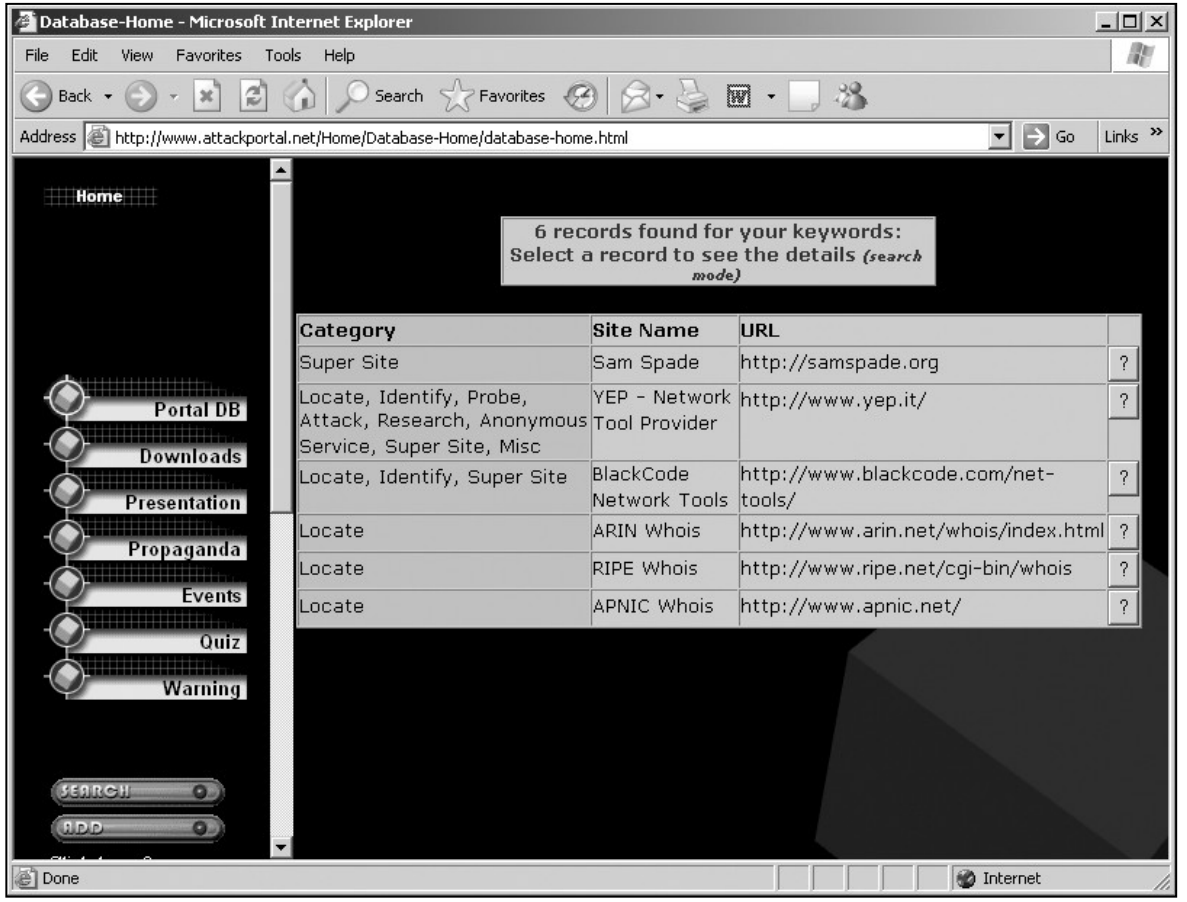
- Does reverse DNS work?
  - Reverse lookup, often point to the ISP (owner of the IP-adresses)
  - Common mistake for split DNS (see earlier slide)
- Web based and local native tools in OS
- Sam Spade (http://samspade.org/d/) spade114.exe
  - Contains many tools
- TRaceRT or Visual Trace Route
  - Show hops between own IP and FQDN
  - Windows -> tracert
  - GNU/Linux, Unix -> traceroute
  - Matts Trace Route MTR - WinMTR
- Get hold of phone number and contact info to personel at FQDN
  - Often errors in whois
  - www.google.com or other search engine
  - Yellow and white pages for respective country
    - Often cost money
- Good resource! http://www.sans.org/reading_room/



PingPlotter

Web attack/reacon portals

- http://www.attackportal.net
- http://www.cotse.com/iptools.html
- http://www.securityspace.com/
- http://network-tools.com/
- http://samspade.org/
- http://dnsstuff.com/
- Doubtful existence …?



What is Fast flux?

- A cyber crime architecture where IP addresses are swapped
- A Fast flux domain hosting involves the use of botnet zombie drones on broadband IPs infected to act as reverse proxies for the spammer's website or nameservers
- The spamvertised domain, or its nameserver, is pointed at a rapidly changing series of zombie IPs (hence the name) with very short "TTL" values -- usually less than five minutes (300s)
- There are typically four or five "A" records to distribute the load and increase the odds of the website staying up. Their proxy service hides the IP location of the spammer's dedicated servers
- As the very action of hijacking computers is illegal in most jurisdictions, such fast flux hosting is only used for further criminal activities such as phishing and child pornography

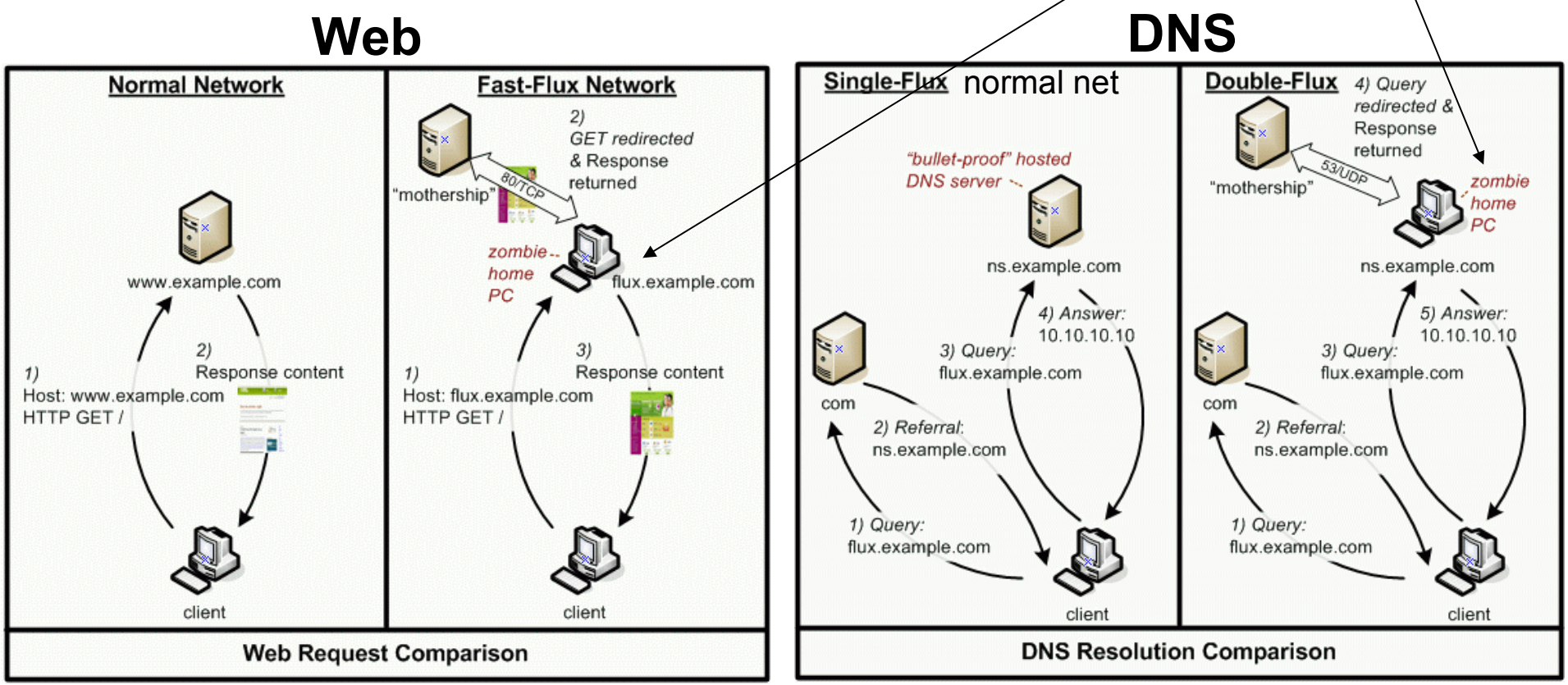
- Double flux have some similarities to split DNS in my opinion

http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#164

http://en.wikipedia.org/wiki/Fast_flux

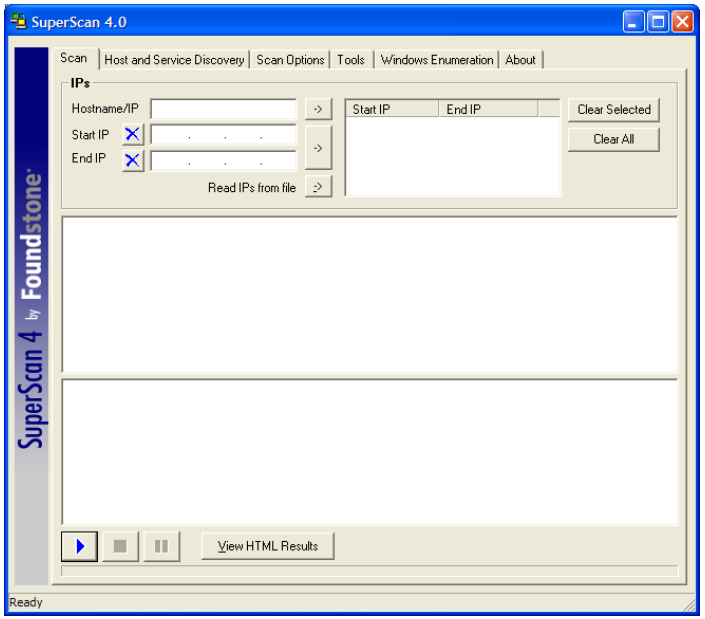
What is ***-flux?

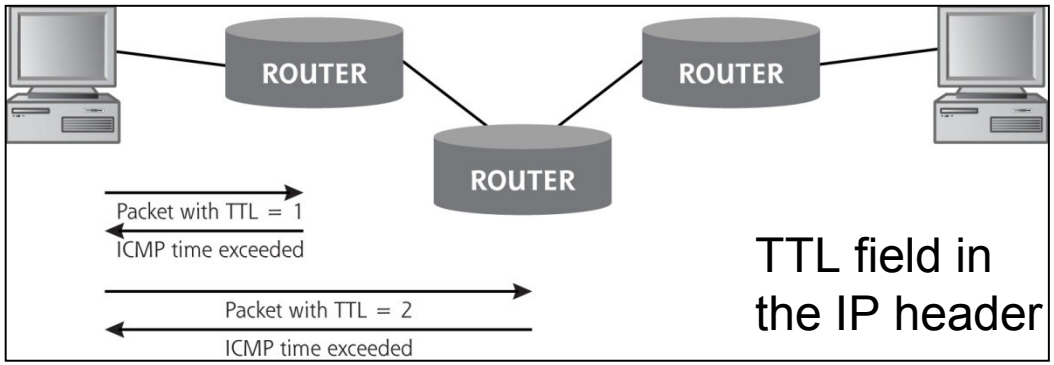
- Know Your Enemy: Fast-Flux Service Networks
  - Animations etc.
  - http://www.honeynet.org/papers/ff/

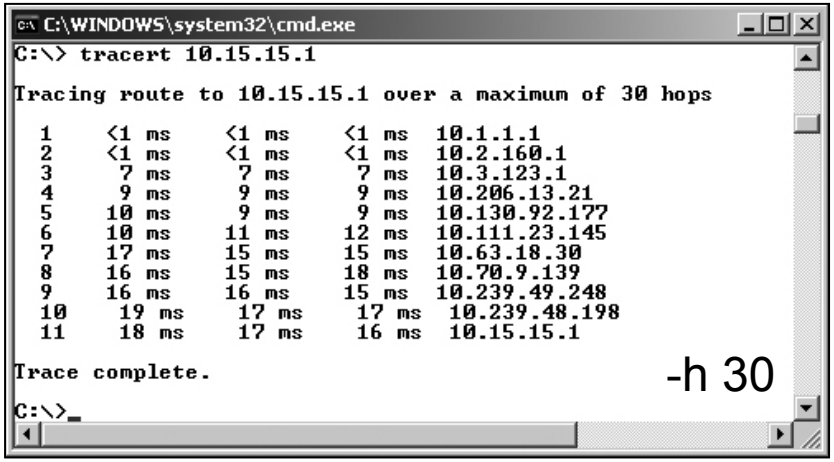


Network mapping

- Gaining an understanding of the victim network architecture
- Sweeping - finding live hosts
  - Ping (ICMP echo request > response)
  - TCP packets to potentially open ports
    - SYN-ACK response
  - UDP packets to likley closed ports
    - ICMP port unreachable message response
- Traceroute – find out the topology
  - TTL (Time To Live) hops – roundtrip time
  - Unix sends UDP and
    Windows sends ICMP packets



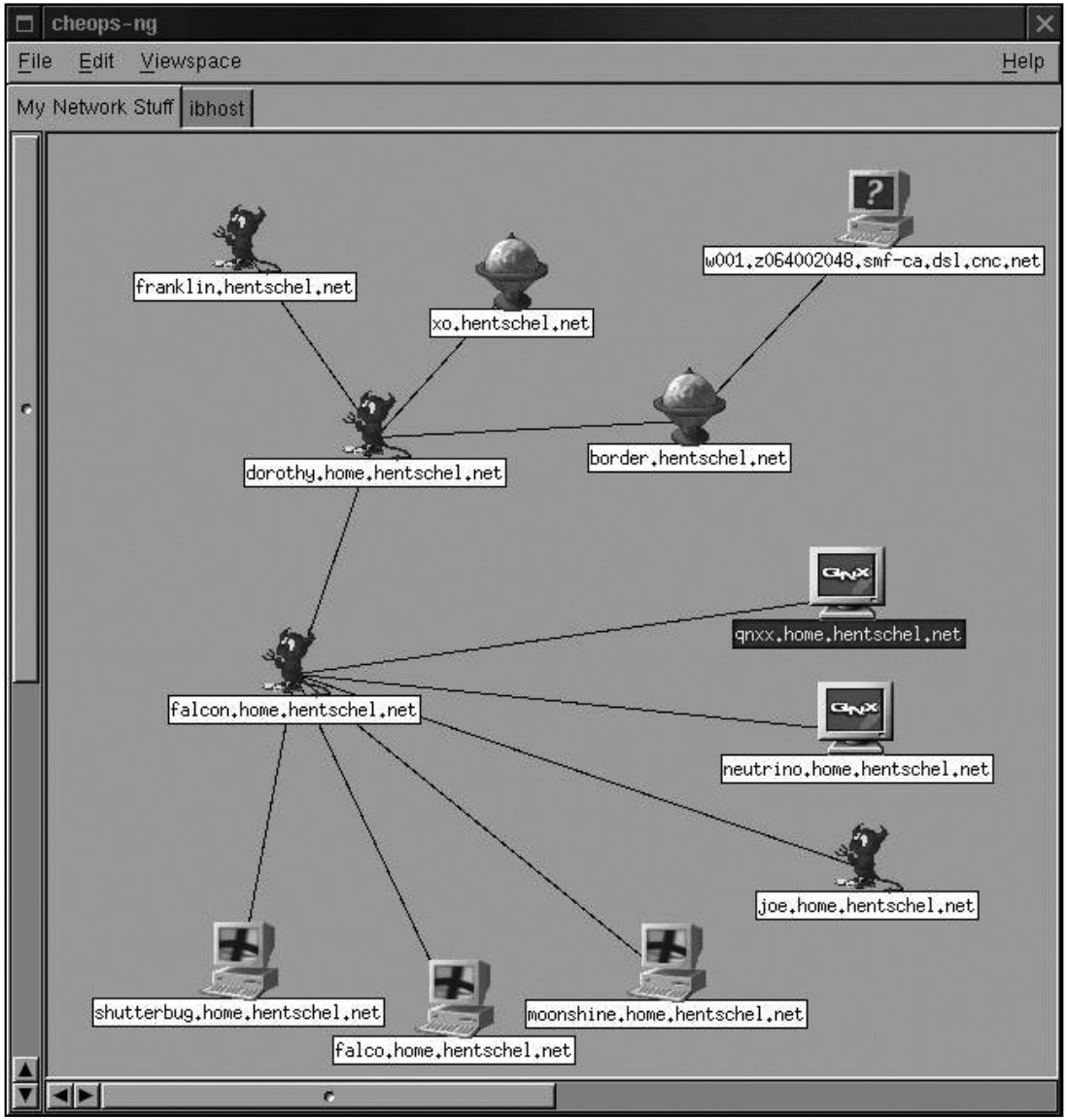




Automated network mapping

- Backtrack menu >
  - Cheops etc.
- There are many pro-tools available
  - Solarwinds Engineer toolset
- Defense
  - Block ICMP (ping) for all private hosts
  - Filter out ICMP time exceeded messages leaving your network

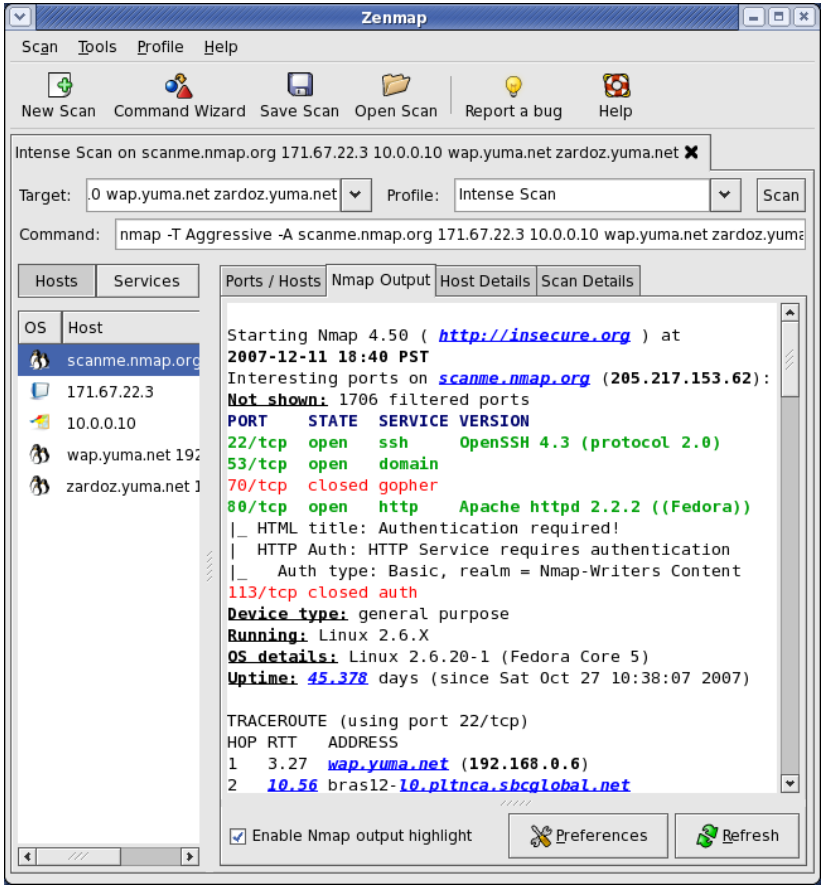
Result is the (***) answer



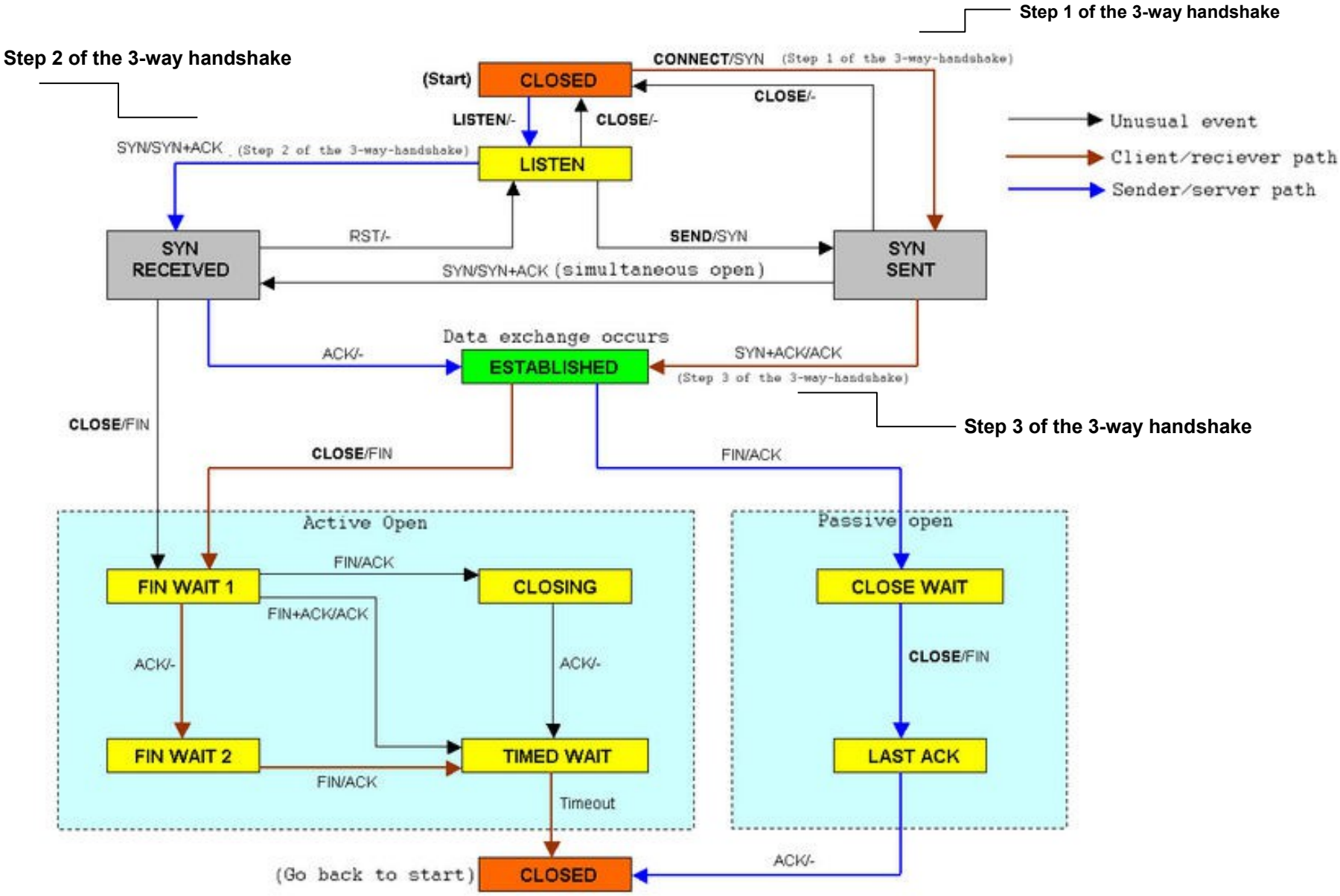
Nmap Port Scanning Tool

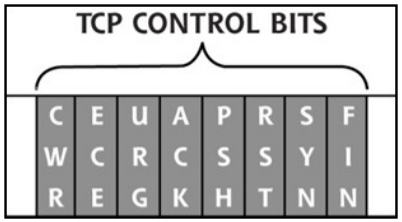
http://nmap.org <---> http://insecure.org

- 65536 TCP and UDP ports
  - http://www.iana.org/assignments/port-numbers
- Author: Fyodor
- Console and graphic
- Unix tool - Windows have some limitations
- Very many options
- When scanning, remember
  - Illegal in many countries
  - Host may be flooded



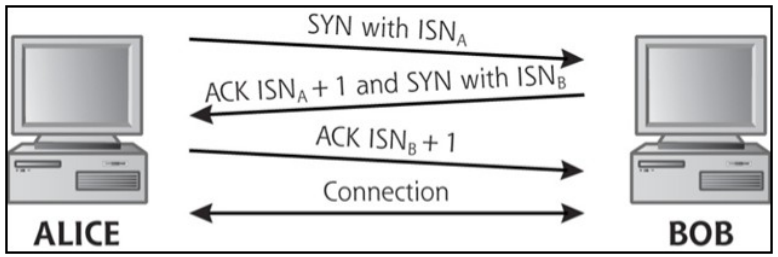
TCP/IP state chart

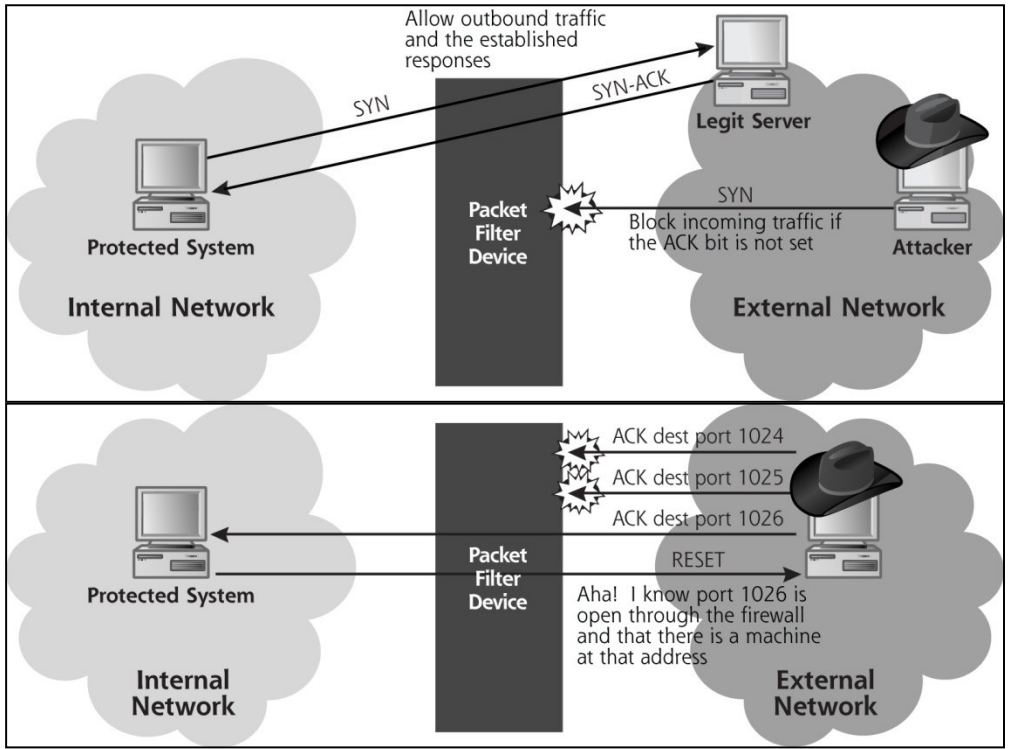




Types of Nmap scans 1

- TCP connect scan (-sT)
  - Complete the three-way handshake, not stealthy
  - RST (RESET) is sent if closed
- TCP SYN scan (-sS)
  - Only send initial SYN and wait for ACK then stop
- TCP FIN (-sF), Xmas Tree (-sX) and null scan (-sN)
  - Sends packets that are not expected to start a connection
  - A closed port sends RST, a listening port sends nothing (Windows does not correspond) maybe…
- TCP ACK scan (-sA)
  - Always set after handshake
  - RST = packet got thru FW and system may exist
  - No response or ICMP port unreachable = filtered by FW
  - Different OS react different on ACK packets on open and closed ports
    - Some send RST back when open
    - Some send RST back when closed

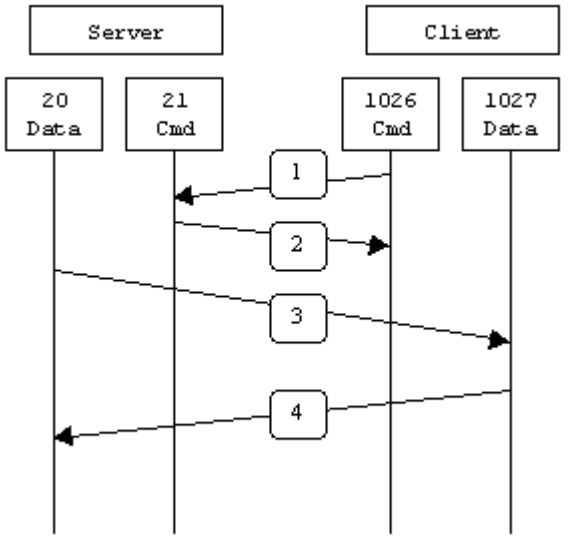




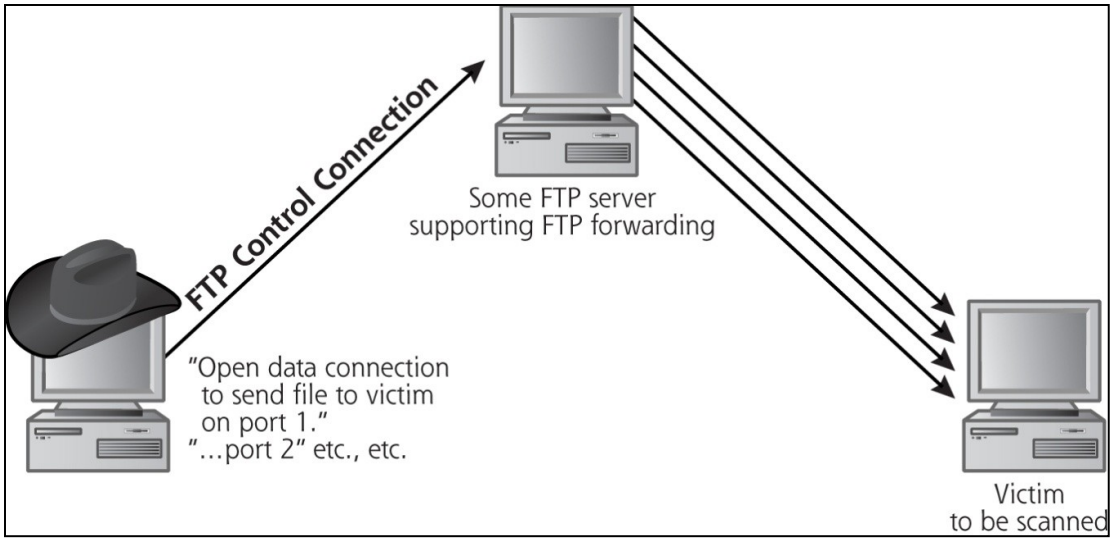
Types of Nmap scans 2

http://slacksite.com/other/ftp.html

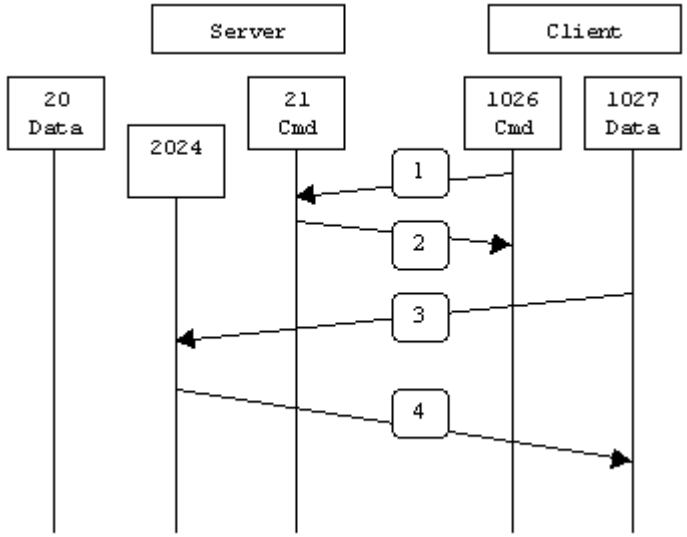
Stealty FTP bounce scans (-b)



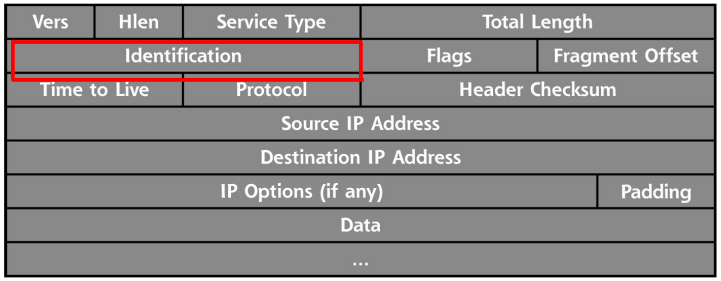
- Active and passive FTP
  - Command (21) and Data (20)
- Attack builds on FXP (File eXchange Protocol)
  - Usually used for warez
- Attacker request that a file is FXP:ed to victim
  - Port status will be given



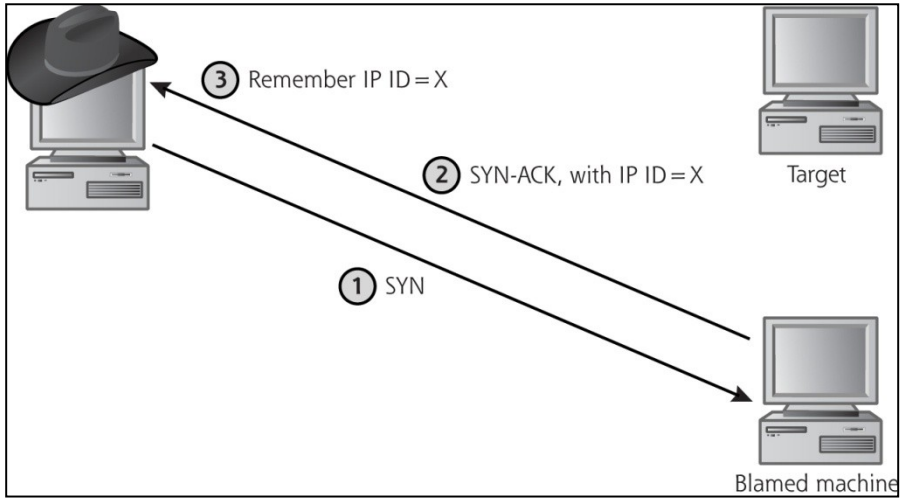
Passive FTP

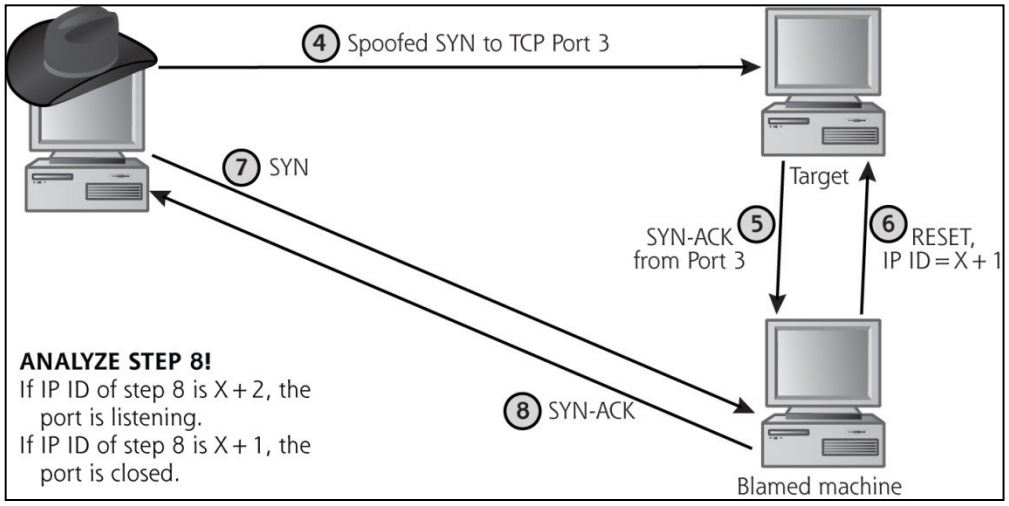


Types of Nmap scans 3 Stealty idle scan (-sI)



- IP header got Identification field (IP ID)
  - Used to put fragmented packets together into one
  - Every packet got an unique number which is incremented x+1 for next
- Attacker finds an idle computer (Windows) to blame
- If target is listening in step 5, blamed will answer otherwise nothing will happen
- Attacker analyze response in step 8



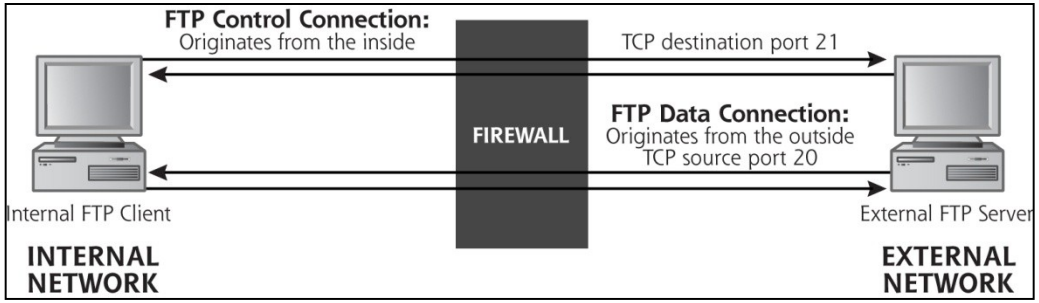


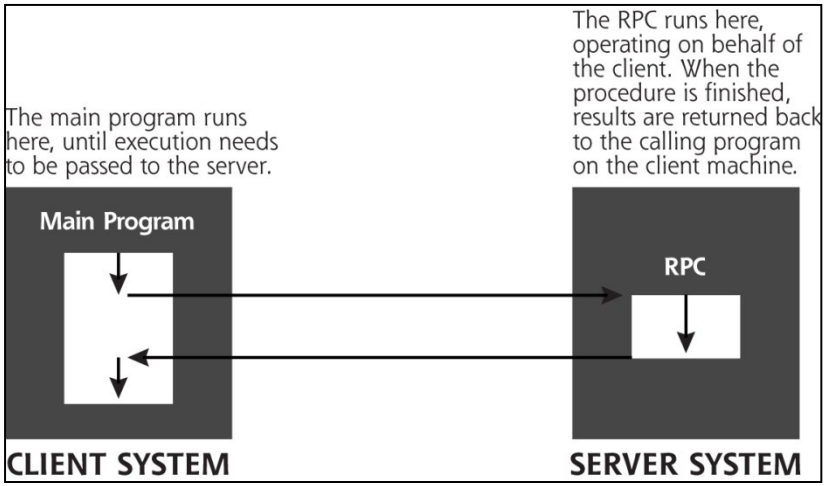
Types of Nmap scans 4, UDP (-sU), version scans (-sV) and ping sweeps (-sP)

- UDP is unreliable by nature
  - UDP packet response
    - ICMP unreachable = port closed
    - UDP packet = port open
    - Sometimes UDP packet needs payload
      - Nmap interpret it as open or filtered, e.g. Nmap does not really know for sure…
- Version scans analyze the service banner (grabbing)
  - Hiding services on obscure ports are futile
  - Simple with NetCat: nc -v <hostname> <port>
- Ping sweeps with either ICMP or TCP
  - Scans the whole network (as described earlier)

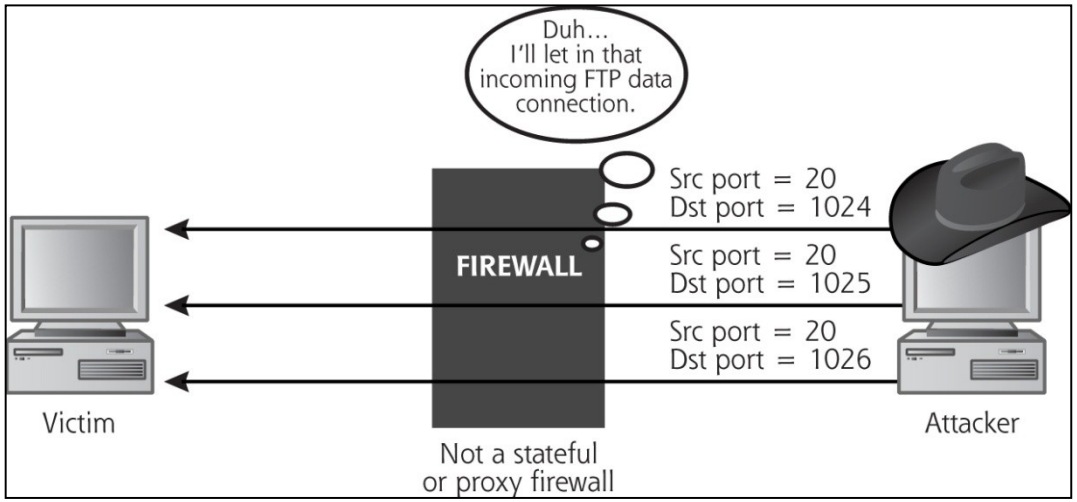
Types of Nmap scans 5, RPC scans (-sR) and source port manipulation

- Remote Procedure Call
  - Find vulnerabilities
- Manipulating the source port to increase pass-thru chances





  - TCP on port 25 or 80 + ACK
  - UDP on port 53
- FTP-server data
  - Active mode



Decoys and OS fingerprinting (-O) etc.

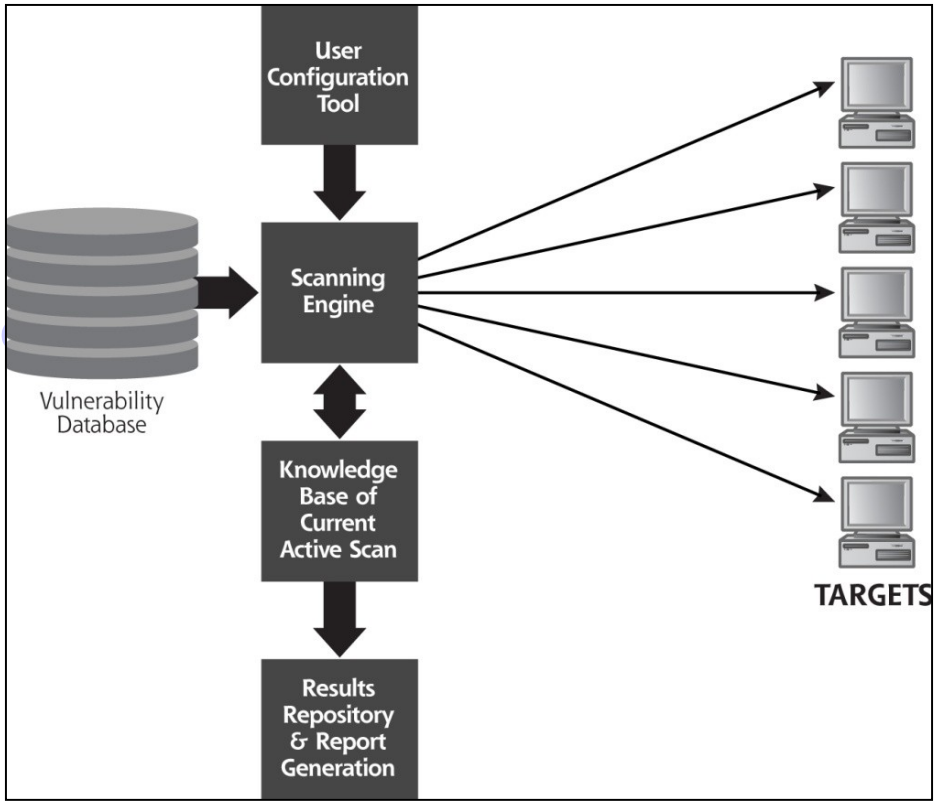
- Decoys
  - Insert spoofed source IP adresses
    - Number of decoy adresses + 1 (attackers IP)
- Active OS fingerprinting
  - Different OS TCP stacks responds different to unexpected control bits or flags in header
  - Measures predictability of initial sequence number in SYN-ACK response
  - Xprobe2 – tool that focus on active OS fingerprinting
- Timing options
  - 6 different scans from very slow to insane fast
- IP fragmentation
  - Slice the packets in smaller chunks to foil IDS/IPS

Nmap scan examples

- Scan for one port (139) identifying all computers running Netbios / SMB putting result in a grep able text file
  - # nmap -p 139 192.168.0.* -oG 139.txt
- Launches a stealth SYN scan against each machine that is up out of the 256 IPs on the class C sized network where scanme resides. It also tries to determine what operating system is running on each host that is up and running. This requires root privileges because of the SYN scan and OS detection.
  - # nmap -sS -O scanme.nmap.org/24
- Scans 4096 IPs for any web servers (without pinging them) and saves the output in both grep able and XML formats
  - # nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
- Nmap Reference Guide
  - http://nmap.org/book/man.html

Vulnerability scanners

- Automating the checks for vulnerabilities
  - Configuration errors and weaknesses
  - Well known system vulnerabilities
- Nessus – popular and free
  - Around 20k plugins of vulnerabilites
  - Report
  - Write own scripts
  - Check demos on http://www.tenablesecurity.c
- Other
  - Rapid7 NeXpose, w3af
  - OpenVAS
  - Harris STAT scanner
  - ISS, GFI LANguard
  - E-eye Retina etc.



Defense against port scanning & vulnerabilities

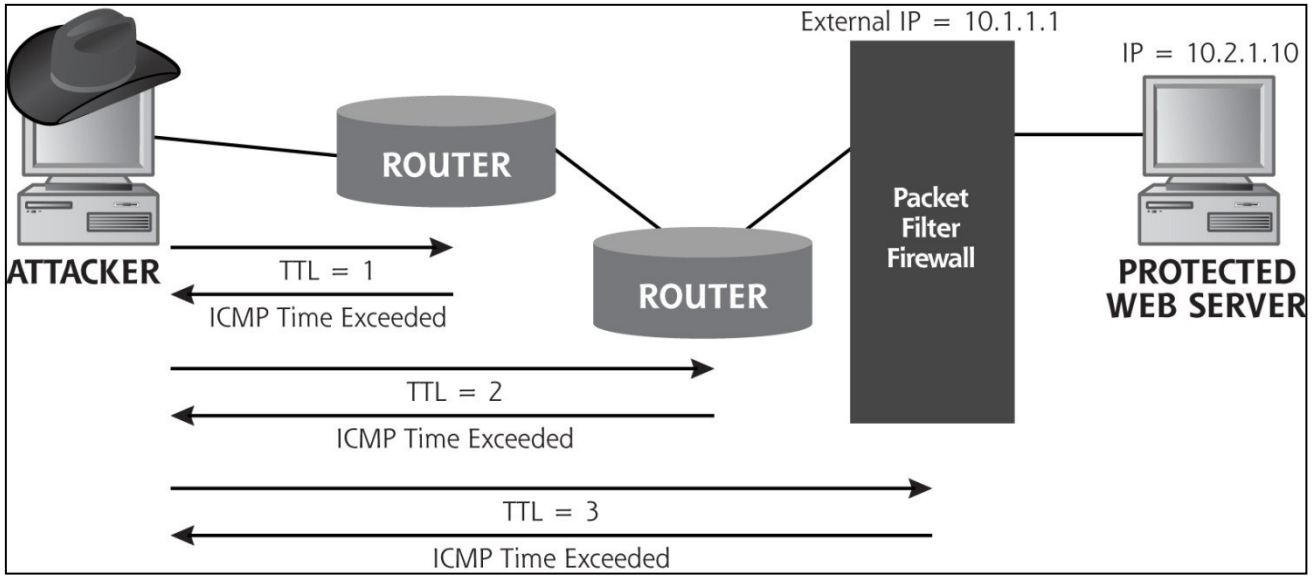
- Harden the system
  - Remove everything unnecessary!
    - Open ports, network services/daemons, software
  - Patch everything to newest version and use a personal firewall
  - Tight configuration and strong passwords on networked applications
- Verify/check with tools as:
  - Nmap, netstat, TCPView, lsof, Nessus, etc…
  - Services.msc, /etc/inetd.conf, /etc/init.d/
- Add intelligent (stateful) packet filtering
  - Minimize open firewall ports

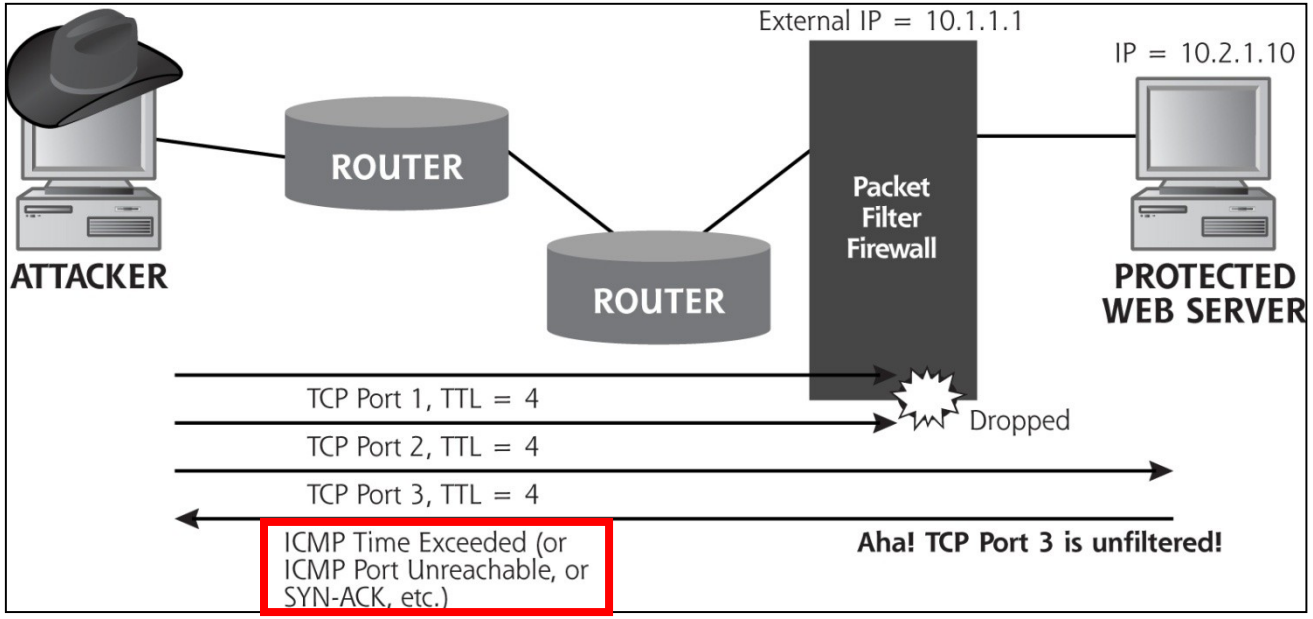
- Firewalk (walks thru the firewall)
  - Determines the firewall (FW) ACL rule set
    - As Nmap ACK scan (established connections)
  - Tells the attacker where FW allows new connections (SYN)
  - Works as traceroute with TTL IP field
  - Attacker must know two IP-addresses, one before and one after FW

Firewalk – determine FW rules

http://articles.techrepublic.com.com/5100-10878_11-5055357.html
http://www.vulnerabilityassessment.co.uk/firewalk.htm

- Discovery phase
- Scanning Phase
  - TCP packets TTL=FW+1
  - Any response means unfiltered
- Does not work against proxy-FW





IDS (Intrusion Detection Systems)

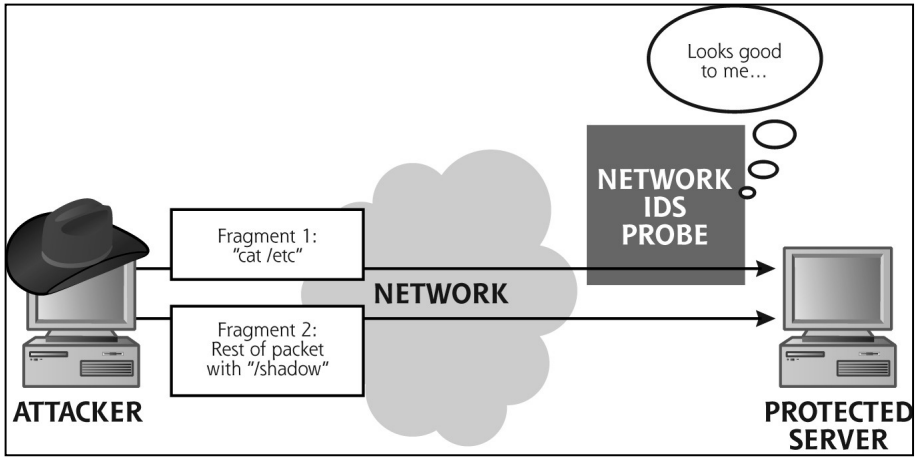
- Used to detect if an intrusion has occurred, proceeds or attempts have been made - using network "signatures"
- Network based
  - A system with software which ”sniffs” (capture network traffic) the network in real-time thrugh a promiscuous network card
  - Analyzes the type of packet, frequency, deviation, pattern, etc.
- Server/client based
  - Uses intelligent agent software wich monitors all processes in real-time
  - Analyzes system calls, logs, file systems, etc. (as an AV agent)
- Or both technologies together
- The console is admin interface to control IDS
  - Policy, configuration
  - Process alarms
  - Download and view data from sensors
- Snort is a popular IDS Tool

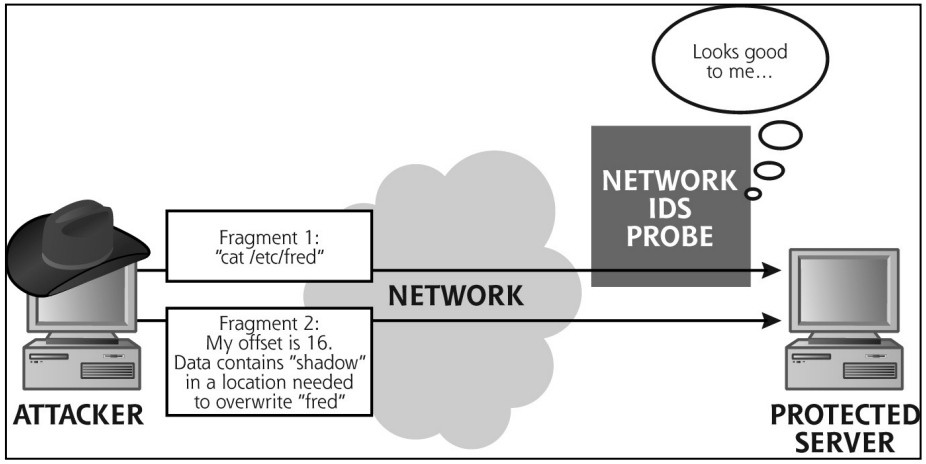
IPS (Intrusion Prevention System)

- Used to filter/block certain traffic for a specific event based on the IDS config, eg
  - Blocking a specific network segment from attacks
  - Filter out a specific IP address
  - Notify administrators that something is going on by email for example
  - Notify the ISP (Internet Service Provider)
- Implementing an IDS/IPS require as usually some form of analysis, in this case the division of the detection zones, attack signatures, etc.
- Internal (host-based) IDS/IPS
  - Monitors and protects internal information (your own computer)
  - Tripwire - http://www.tripwire.com/
- For IDS and IPS to work you must have an updated signature database (like AV agent)

How attackers can evade IDS and IPS

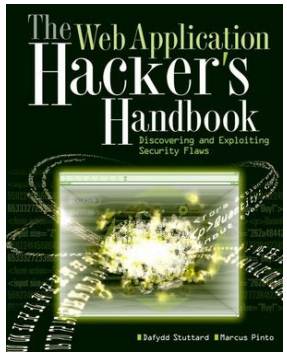
- Technique at the network level
  - Mess with the appearance of traffic so signature will not match
  - Mess with context so it's difficult to interpret
- IDS/IPS may have difficulties/limitations to "remember" and analyze everything correct
  - Use fragmented packets
  - Flood of fragmented packets
  - Fragment the packets in unexpected ways
  - Ex. Tiny fragment attack and Fragment overlap attack

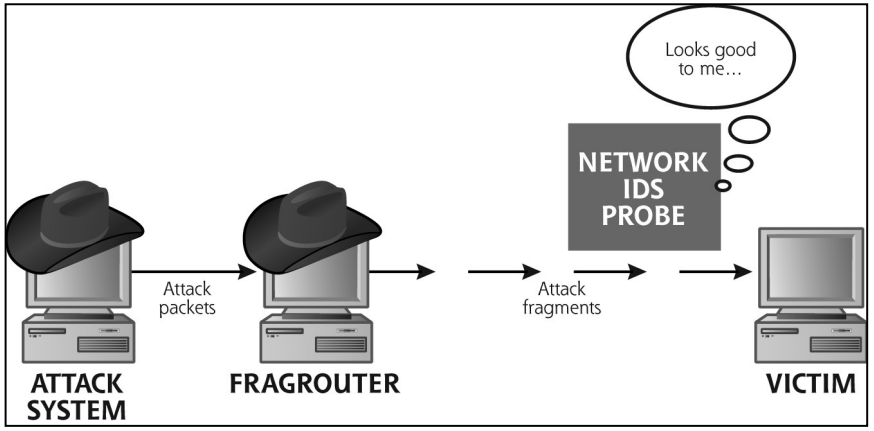




How attackers can evade IDS and IPS

- Application level – Nikto2 (CGI, ASP, JSP, PHP)
  - Mainly a web vulnerability scanner
  - Have at least 10 different tactics to evade IDS/IPS in the web requests
  - Variants on a simple HTTP request: GET /cgi-bin/broken.cgi HTTP/1.0
    - URL encoding - *GET /%63%67…….%7e/cgi-bin/broken.cgi HTTP/1.0*
    - /./ directory insertion - *GET /./cgi-bin/./broken.cgi HTTP/1.0*
    - Premature URL ending - *GET /HTTP/1.0\r\n HEADER: ../../cgi-bin/*
    - Long URL – *GET /thisisaverylongurl…blablabal/../cgi-bin/broken.cgi HTTP/1.0*
    - Fake parameter
    - Tab separation instead of space
    - Case sensitivity
    - Windows delimiter e.g. "\"
    - NULL method e.g. %00
    - Session splicing (fragm. packets)





- Network level - FragRouter and FragRoute
  - A software router that slice and dice packets so IDS/IPS will not understand them, have at least 35 "recipes"