Computer Security

Secure the Computer

Secure the Network

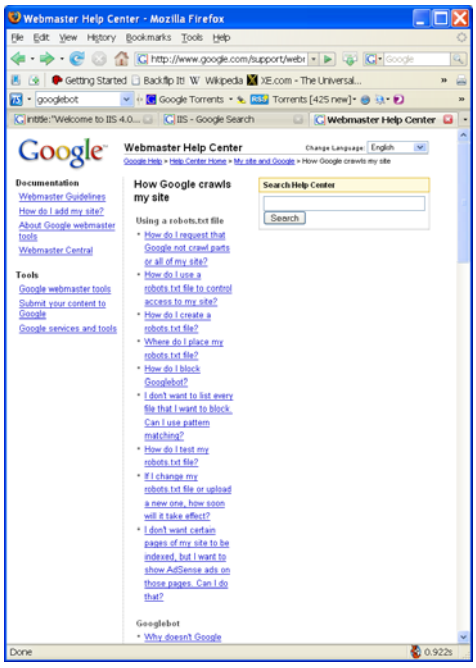
Secure the Software

Insecurity

- Virus, Trojans & Worms
- Case the place
  - Footprinting
  - Scanning
  - Enumeration
- Defences
  - Tools
  - Configuration
- Finding Vulnerabilities
  - Wireshark & Port Scans
- Hacking
  - Hack Windows
  - Hack Unix
  - Hack the Network
  - Hack Software

Google Bad ?

- Google knows about *everything* these days, deadly efficient.
- Google Bots search for and find links relentlessly.
- Lots of people leave information about their own vulnerabilities on their web sites.



Google: The hackers friend

- Google can give you targets of opportunity.
- Run the search…
  - **`Inline: “Welcome to IIS 4.0”`**
- 32 sites running IIS with huge number of security vulnerabilities. Better than last year – 64 then!

Vulnerabilities with Google I

- Try…
  - "VNC Desktop" inurl:5800
    - Gave me 149 hits, allows remote users to login & control machines, sometimes without a password
  - filetype: pwd service
    - Gave me about 195,000 hits, some of these will have usernames and passwords. Many others warn against using Front Page.
    - Hacker may use **`John the Ripper`** SW to crack any passwords revealed

Vulnerabilities with Google II

- filetype inurl:"htaccess|passwd|shadow|htusers"
  - Gave me 1,250 hits some may have unshadowed Unix password files
- filetype:properties inurl:db intext:password
  - Gave me 43 hits (fewer than before, 800+), may give me a database password, even in clear text
  - Actually gave me a plain text password for a top UK University research site !!!
- "not for distribution" confidential site:edu
  - This gave me about 347 hits, **.gov** gave me 129 hits

Go for the Jugular Trudi!

- "This file was generated by Nessus"
  - Results **1 - 10** of about **242** for **"This file was generated by Nessus"**. (**0.37** seconds)
  - Results **1 - 10** of about **788** for **"This file was generated by Nessus"**. (**0.36** seconds)
  - Well, Nessus is a vulnerability scanner used by many sys-admins, but they leave the reports up on the Internet – how foolish is that?
  - These Sys-Admins did the work for me and then tell the whole world how their systems are vulnerable… ooh!

Footprinting

WHOIS [Domain & IP Relates Searches]

DNS Interrogation

Network Reconnaissance

Footprinting

- Footprint is a profile, often unique, of intended target's Internet, remote access, and intranet\extranet profile.
- *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."* Sun Tzu, On the Art of war.
- Attacker will endeavor to discover the security posture of any victim. Requires expertise, tools and techniques and a good dollop of patience.

Internet Footprinting I

- **Domain related searches** can be done using a `whois` server
  - `http://www.whois.sc/`
  - Lots of others, like `SamSpade.org`, `foundstone.com`, NetScan Tools Pro `nwpsw.com`
  - You can check out dcu.ie and get lots of info about the site

Internet Footprinting II

- IP-Related searches will give us information about who owns an IP address, who administers it and possibly servers on that network.
- Some information may be bogus, a tripwire to catch potential threats, phone numbers, email addresses etc.

DNS Interrogation

- May be configured insecurely!
- Best done on Linux, more tools available.
- Zone transfer: Allows secondary master server to update its zone database from primary master.
- May be improperly configured to supply copy of zone to anyone.
- Problem: non separation of public\private segregation of external DNS info (public) from internal (private) info provide disclosure of organisation’s internal Network.
- This transference should be restricted in the DNS configuration. Only externally connected machines should be reported by a DNS

Network Reconnaissance

- ***traceroute*** is another tool in the hackers arsenal (***tracert*** on Windows).
- Used to learn the network topology.
- Many systems sift out ***tracert*** packets.
- They can send ICMP echo request packets (default in Windows), which of course are blocked in many systems.

Scanning

nmap

Available on the Web & my Directory

Malware

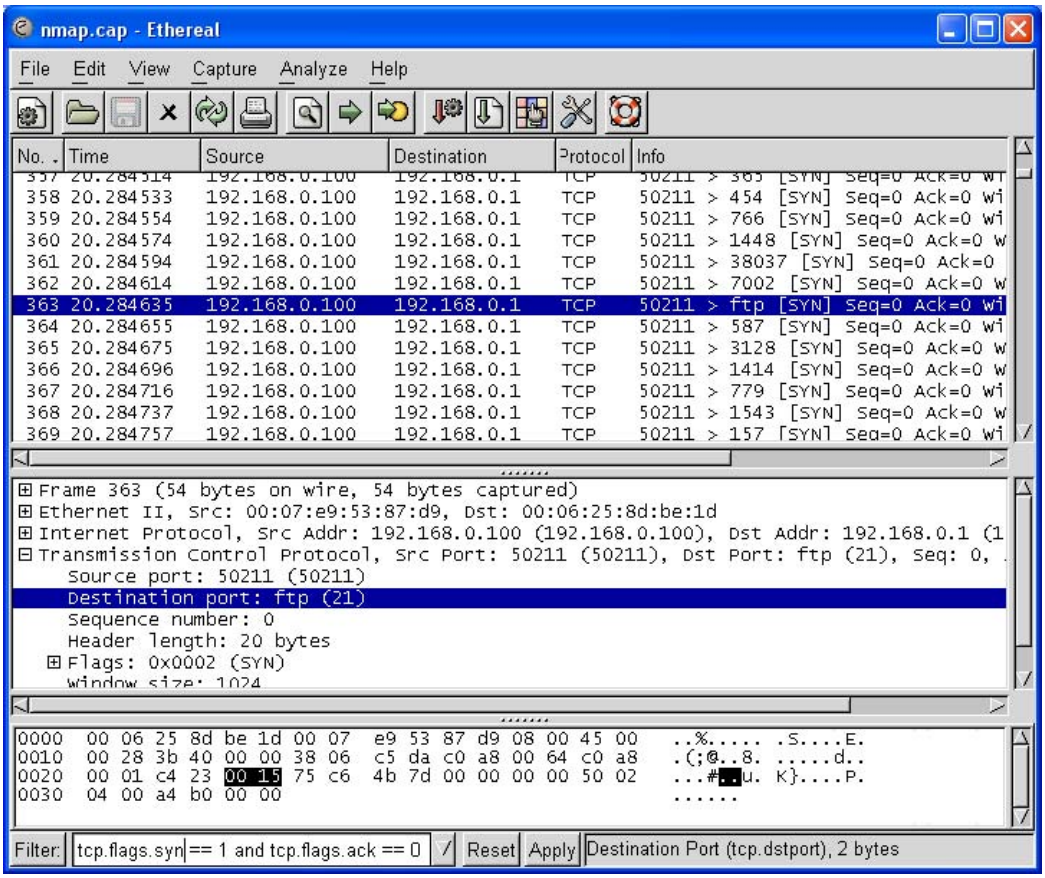
- Bugs in server side SW is often exploited.
- Send carefully crafted packets to a port on remote system may cause error, allowing attacker through back-door.
- Buffer overflow attacks overflow buffers for holding parameters, writing into address space of server, overwriting location of next instruction pointer.
- Attacker inserts location of their own code.
- Once attacker knows that certain SW is running, may target particular addresses.
- Tools for finding open ports used here to survey systems for vulnerable back doors, called port scanners.
- Scanning is always regarded as an attack on a system

nmap

- ***nmap*** is a port scanning tool, very versatile and freely available across many OS.
- Sends SYN messages, server responds with SYNACK on open ports.
- ***nmap*** can disguise its operation with decoy scans, spoofing IP addresses, targeting multiple IP addresses etc.

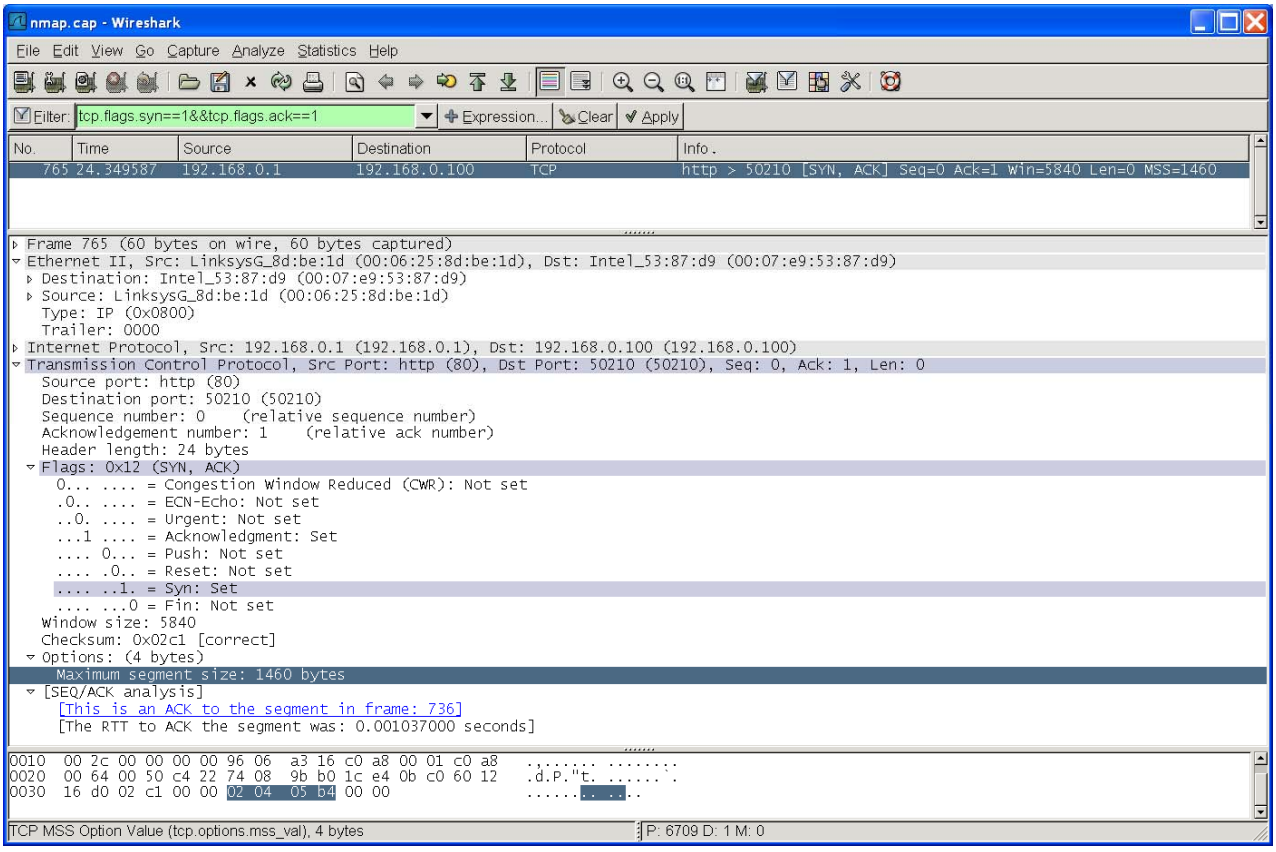
Wireshark & nmap

- In file *nmap.cap*, used filter
  - `tcp.flags.syn ==1 && tcp.flags.ack == 0`
- This isolates probe packets sent by nmap
- Sent 6693 packets, between 3 and 4 SYN messages for each of the 1658 ports scanned
- To obfuscate scan, does not proceed from low to high port numbers, nor all probes for a single port together.
- Wireshark names some well-known port numbers: 80 – web servers; 25 – email
- Known ports allow users to locate services on remote machines more easily.

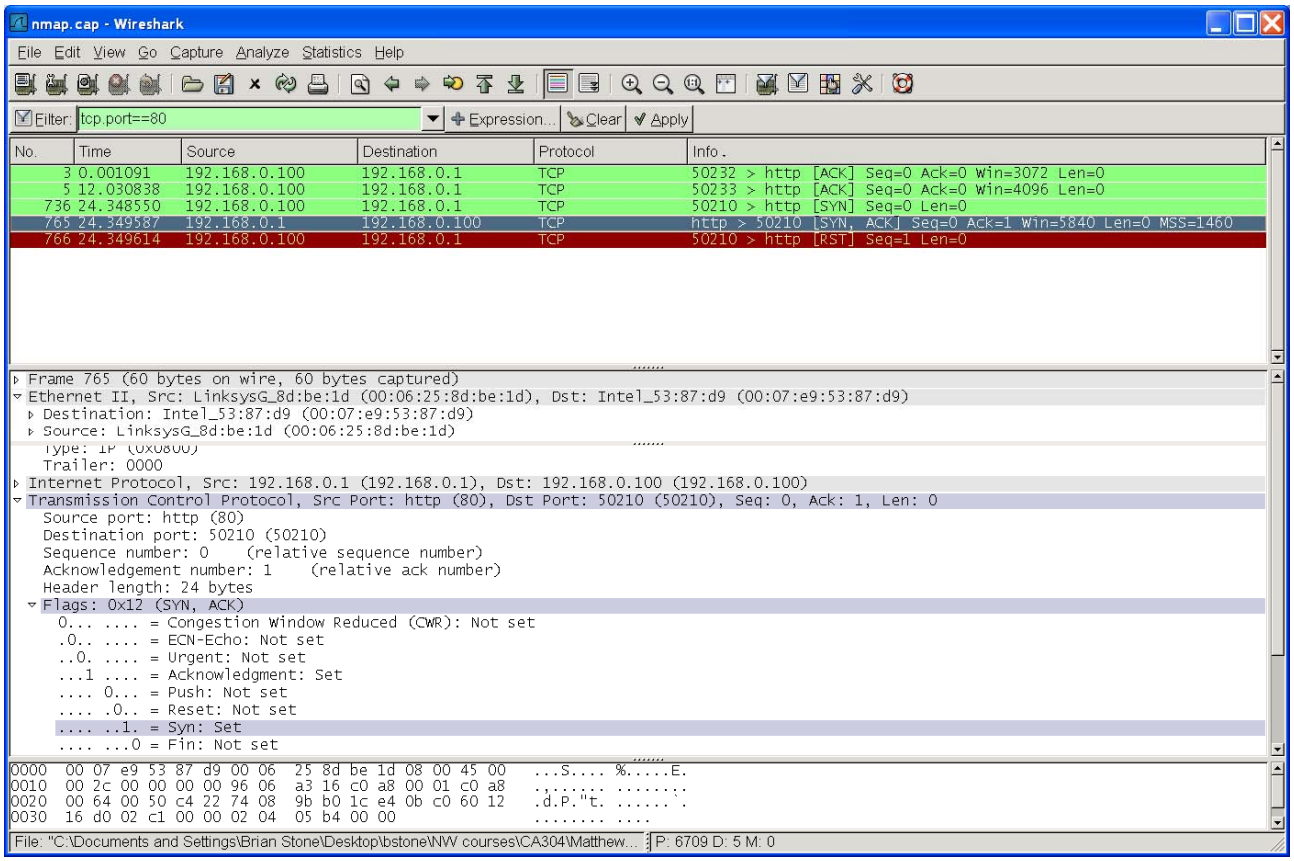


Nmap Trace

- To identify a hit…
  - `tcp.flags.syn ==1 && tcp.flags.ack ==1`
  - Identifies SYNACK messages
- Only port 80 is open, isolate this
  - `tcp.port == 80`
- As soon as server responds, **nmap** closes the port with a RST bit set



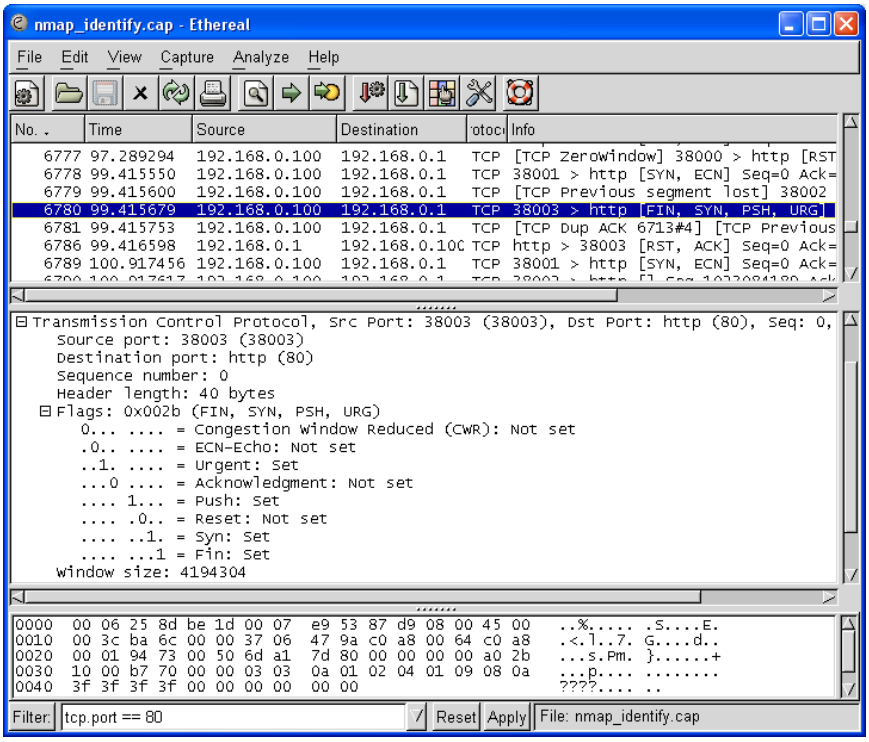
tcp.flags.syn ==1 && tcp.flags.ack ==1



tcp.port == 80

Nmap Probes

- Nmap can also find out what type of machine and OS are running the server.
- Fingerprinting may point to particular implementations of TCp protocols
- Initial TCP sequence number choice points to OS, also which TCP options are supported and ICMP data in error messages.



Xmas tree probe: FIN, SYN, PSH & URG all set

Nmap Fingerprint

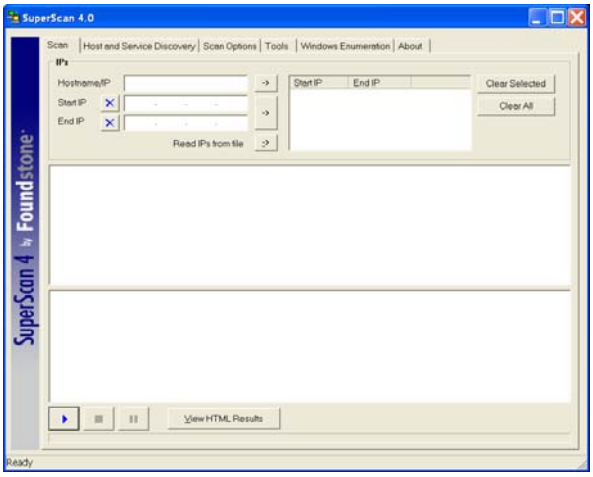
- Packet 6780 has FIN, SYN, PSH and URG all set, how weird is that?
  - This is an Xmas tree scan, target should send back an RST for all closed ports, according to RFC 793.
- Different implementatiopns of TCP will react differently.
- By studying the behaviour of various OS and implementations, nmap can discover what OS and architecture is running.

nmap can identify users

- Try…
  - `nmap -I 136.206.11.72`
  - This scans port 113, ident - old server identification system, still used by IRC servers to identify its users
- Watch out for port 80 running as root instead of nobody. Root could compromise the system
- Some versions no longer support this

SuperScan

- Windows port scanner
- Supports TCP and UDP
- Very sophisticated, allows user to choose from many scanning techniques
- Available free from *foundstone.com*



OS Detection

- Active Stack fingerprinting
  - Requires sending traffic to target, also requires having at least one open port.
- Passive Stack fingerprinting
  - Quietly monitor passing traffic
  - Requires no sending traffic, but must be on the target network.

Active Stack Fingerprinting [1]

- **FIN probe**: correct behaviour – no response, Windows NT/200/2003 respond with FIN/ACK
- **Bogus flag probe**: set a flag in a SYN packet (should not be set), Linux responds with a flag set in response packet
- **ISN sampling**: Different OS set different seq no according to a patters (WIN increments, others use exact sizes)
- **DF bit monitoring**: Some set it to enhance performance
- TCP initial window size: Some OS use unique size
- **ACK value**: some send back what you sent , others increment, others random

Active Stack Fingerprinting [2]

- **ICMP error message quenching**: Monitor rate at which error messages are sent, use EDP on hi-numbered port
- **ICMP message quoting**: ICMP quotes varying amounts of frame that caused error, OS differ on amount
- **ICMP error message-echoing integrity**: some OS mangle the IP header of frame being reported, varies according to stack implementation
- TOS: “ICMP port unreachable” messages use 0 in TOS, Linux not
- **Fragmentation handling**: Some stacks will overwrite older fragments, others not.
- **TCP options**: More advanced options implemented in most current implementations. By sending packets with multiple options set, can make some assumptions about OS in use.

Passive Stack Fingerprinting

- Passively monitor NW traffic
  - TTL: what the OS sets as thetime-to-live on the outbound packet
  - Window size: what the OS sets as the window size
  - DF Does the OS set the Don’t Fragment bit
- More stealthy, but in your face, not as remote.
- Not foolproof, but a good guess is possible

Countering Port Scanners

- Not a good idea to hack the OS to increase robustness
- Best defence is good firewall and secure proxies
- Intruder Detection Systems (IDS) like Snort are used to detect scans
- www.snort.org, mostly runs under Unix
- Uses signatures which intruders generate when scanning, like a knock sequence.
- IDS should have good log analyser

Snort

- IDS and is free!
- Uses signatures to spot scanning attacks

Automating Discovery

- Cheops is a graphical network mapping tool
  - www.marko.net/cheops
- Automatically integrates ping, traceroute, port scanning and OS detection
- Protection against these systems is the same as individual tools.

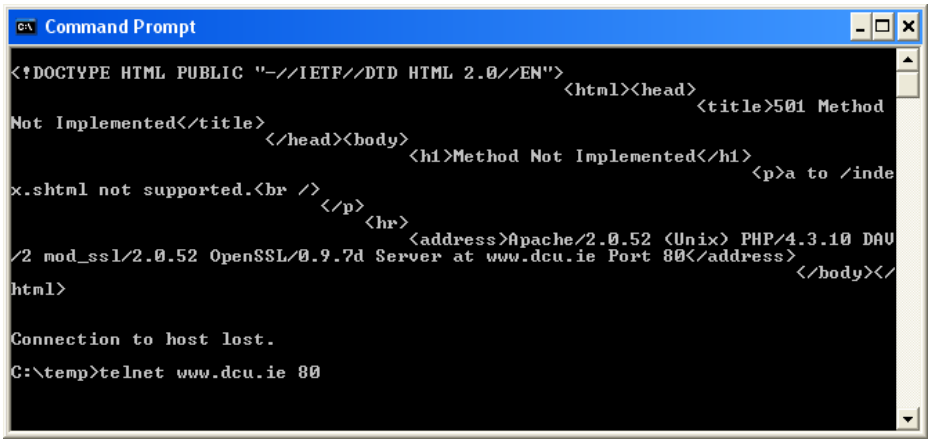
Enumeration

- Scanning lights up live hosts
- Enumeration involves live connections and directed queries
- All such activity should be logged or monitored.
- Tend to be platform specific
- Can involve using sophisticated tools (freely available on WWW)
- Some enumeration techniques are more fruitful to the hacker than others.

Enumeration Techniques

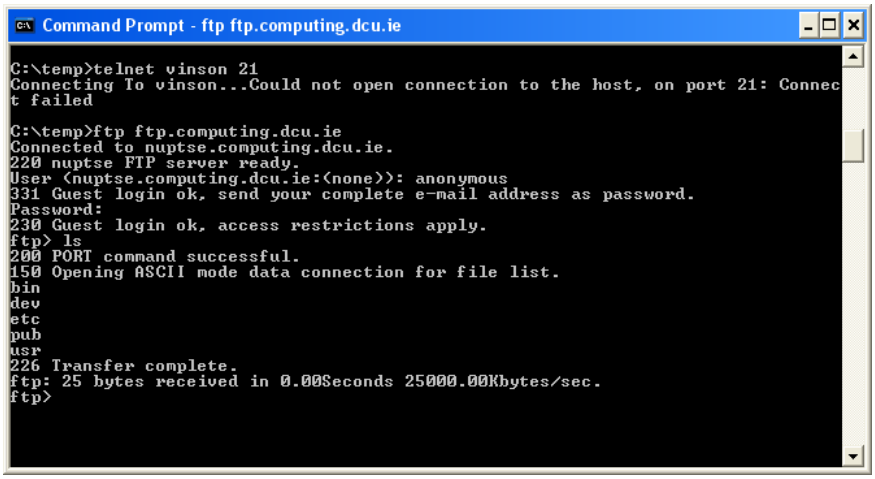
- Basic banner grabbing
  - Using telnet and netcat
- Enumerating common network services
  - Enumerating FTP, TCP/UDP 69
  - Enumerating TFTP, TCP 21
  - DNS Zone transfers, TCP 53
  - Enumerating TFTP, TCP/UDP 69
  - Finger, TCP/UDP 79
  - Enumerating HTTP, TCP 80
  - Enumerating Microsoft Endpoint Mapper (MSRPC), TCP 135
  - Enumerating NetBIOS Name Service, UDP 137
  - Enumerating NetBIOS Session, TCP 139
  - Enumerating SNMP, UDP 161
  - Enumerating BGP, TCP 179
  - Netware, Unix RPC, SQL, NFS etc. all have weaknesses, and the list goes on, and on, and on.

Using telnet and netcat



- Simply telnet to port 80 on a host, it tells what is running there.
- Netcat does similar. Netcat is listed by Symantec as a “hack tool”

Enumerating FTP, TCP 21

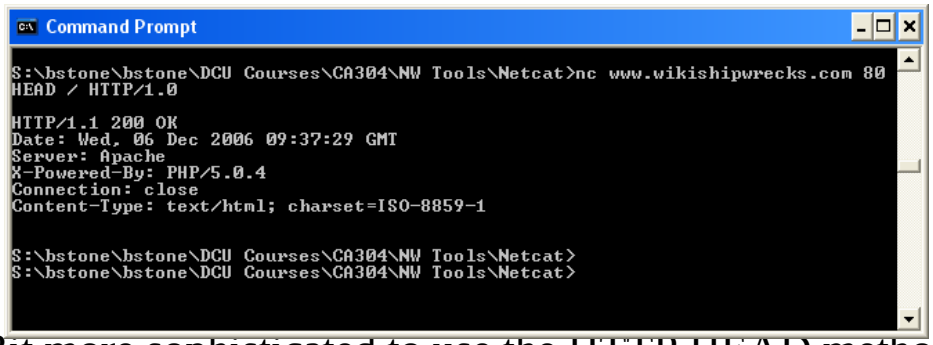


- May hold lots of info on how to do stuff on a network, embarrassing .
- Hackers use it to upload malicious software.V simple to do, simpler to protect against – just turn it off!

DNS Zone transfers, TCP 53

- Using nslookup, to query the DNS.
- Badly configured DNS can dump entire contents of files, giving information like hostname-to-IP address mappings as well as the Host Information Reckord (HINFO)
- Defence: block transfers to to only authorised machines.

Enumerating HTTP, TCP 80



- Bit more sophisticated to use the HTTP HEAD method
- This may trigger an intruder detection system
- Sam Spade tools may be used to trawl through web sites and their source HTML looking for interesting info like passwords. (samspade website experiencing problems at present)

References

- Fyodor : just what it says…
  - `www.insecure.org/nmap/nmap-fingerprinting-article.html`
- Snort: `www.snort.org`
- Lance Spritzner, passive stack fingerprinting:
  - `project.honeynet.org`
- Hacking Exposed, 5th Ed, McClure et al, ISBN 0-07-226081.
- http://en.wikipedia.org/wiki/DNS_zone_transfer