Computer Network Defense

reconnaissance and footprinting
- useful to see if we might want to gain access to a system we don't have access to
- we might want to know a few things about the system:
  - what OS it runs
  - what hardware it has
  - what servers are running and on what ports
- forums and testimonials are a good resource
  - funny how many it techs post their problems (help!) and system specifics online
    - we give out too much information
      - do you facebook? myspace?
    - once we have this, we can head over to millworm to see if any exploits exist
  - anti-virus/anti-spam/firewall testimonials tell us what people are using
    - if exploits exist, we might find a way in
    - many malwares try to shut off protection software like mcafee, norton/symantec, etc
- many tools exist to help you in reconnaissance
  - nmap: security scanner for network exploration and security audits
  - zenmap: gui for nmap (oooo a GUI!)
  - unicornscan: distributed tcp/ip stack (exploit vulnerabilities)
  - strobe: essentially an fast and efficient nmap (on steroids)

useful reconnaissance tools
- telnet
  - simple bidirectional interactive communication
  - command line interface on remote host
  - over TCP
- port scanning
  - probes remote host for open ports
  - used to verify security policies
  - used to identify running services
  - portscan: scan for listening ports
  - portsweep: scan multiple hosts for a specific port
    - some worm may portsweep many hosts for a single port (vulnerability)
  - port status
    - open/accepted: something is listening
    - closed/denied/not listening: connection is denied
    - filtered/dropped/blocked: no reply
  - tcp scanning
    - use OS network functions
    - in nmap, called a connect scan
    - on connect, handshake performed and connection closed
    - no special privileges required
    - no low level control
  - syn scanning
    - uses raw ip packets and monitors for responses
    - known as half-open scanning because never actually opens a full TCP connection
    - port scanner generates a SYN packet
    - if target port is open, host responds with SYN-ACK
    - port scanner responds with RST and closes connection before handshake
    - we can get many details this way
    - target service never actually receives a connection

- usually requires privileges
- udp scanning
  - udp is a connectionless protocol
  - response comes only if a port is closed
  - so absence of response implies port is open
  - most scanners use this method
  - firewalls can fool scanner
- ack scanning
  - does not determine whether a port is open/closed
  - instead, if it is filtered
  - useful to probe for firewalls and its rulesets
- nmap
  - network mapper
  - creates a “map” of the network
  - features:
    - host discovery
    - port scanning
    - version detection
    - OS detection
  - used to:
    - security audits (identify connections, identify unexpected new servers)
    - open port identification
    - network inventory

network sniffing (particularly under the same subnet)

- packet analysis
- “sniffer”
- intercepts/logs network traffic (packets)
- we can then decode/analyze these packets
- uses:
  - analyze network problems
  - detect network intrusion attempts
  - gain info for possible network intrusion
  - monitor network usage
  - gather/report network stats
  - filter content from traffic
  - spy on users/collect sensitive information
  - reverse engineer proprietary protocols
  - debug client/server communication
  - debug network protocols
- carnivore
  - FBI's version
  - designed to monitor email and electronic communication
- tcpdump
- wireshark (formerly ethereal)
- cain and abel
  - mainly a password recovery tool
  - but can sniff passwords transmitted through packets
  - exhaustive methods to “recover” passwords

milworm

- group of hacktivists
- penetrated computers at BARC (bhabha atomic research center)
- maintain an online database of vulnerabilities and exploits

- arp spoofing
  - address resolution protocol
  - can be used to poison (arp poisoning)
  - essentially a sniffer on steroids
    - can stop traffic
    - can modify traffic
  - can only be used on networks that make use of arp
  - cain and abel
    - again...
  - ettercap
- profiling (systems and users)
  - we can find out a lot about the vulnerabilities a system may have via profiling
  - mostly, profiling is legal and available through legitimate means
  - we like to brag, don't we?
- browsing habits
  - very useful information about people
  - lariat
    - network traffic generator (down to the individual!)

the triad

- patch updates, malware protection, firewall
- firewall
  - take care of what's on your system
  - stateful vs. stateless
    - do we treat each packet uniquely (no past memory)? → stateless
    - or do we use the past to infer something about the now? → stateful
  - h/w (router) vs. s/w (zone alarm, windows firewall)
    - how cool would it be to be able to “program” hardware networking equipment?
    - we have some FPGA-based devices to let us create any device—and program it!
  - application based vs. port based
    - what makes more sense?
  - ports/protocols
    - exploitation occurs through ports
  - firestarter, ufw, iptables
- patch updates
  - #1 most overlooked security technique
  - some problem exist
    - no windows update in firefox
  - might make you safe from *most* attacks
- malware protection
  - viruses
  - worms
  - bacteria
  - trojans
  - rootkits
    - blacklite
    - unhooker
  - spyware
    - sniffers
    - keyloggers
  - adware
    - clickster

- wardialing
- spam
- phishing
- anti-virus
- anti-spam/anti-adware
- spybot s&d, avast, ad-aware, avg, comodo, mcafee, norton, clamav
- anti-malware
  - hash detection

honeypots

- no production value
- lures attackers
- we want to know what they do, what they use, how they do it
- no production value
- quasi-honeypot
  - make it more “useful?”