Dynamic policies
- Change as system security state/load changes
- GAA architecture
  - Extended access control lists
  - Pre-, mid- and post-conditions, request-result conditions
  - Speak about security posture, system states, authentication mechanisms, etc.

Intrusion scenario
- Reconnaissance, scanning, break-in and misuse, maintaining access, covering tracks
- Reconnaissance: low-tech, Web-based

Intrusion scenario
- Reconnaissance, scanning, break-in and misuse, maintaining access, covering tracks

What does DNS do?
- How does DNS work?
- Types of information an attacker can gather:
  - Range of addresses used
  - Address of a mail server
  - Address of a web server
  - OS information
  - Comments

Interrogating DNS – Zone Transfer
$ nslookup
Default server: evil.attacker.com
Address: 10.11.12.13
server 1.2.3.4
Default server: dns.victimsite.com
Address: 1.2.3.4
set type=any
ls -d victimsite.com
system1 1DINA 1.2.2.1
1DINHINFO “Solaris 2.6 Mailserver”
1DMX 10 mail1
web 1DINA 1.2.11.27
1DINHINFO “NT4www”

Split–horizon DNS
- Show a different DNS view to external and internal users

Protecting DNS
- Provide only necessary information
  - No OS info and no comments
- Restrict zone transfers
  - Allow only a few necessary hosts
- Use split–horizon DNS

Reconnaissance Tools
- Tools that integrate Whois, ARIN, DNS interrogation and many more services:
  - Applications
  - Web–based portals
    - http://www.network–tools.com
At The End Of Reconnaissance
- Attacker has a list of IP addresses assigned to the target network
- He has some administrative information about the target network
- He may also have a few “live” addresses and some idea about functionalities of the attached computers

Phase 2: Scanning
- Detecting information useful for break-in
  - Live machines
  - Network topology
  - Firewall configuration
  - Applications and OS types
  - Vulnerabilities

Network Mapping
- Finding live hosts
  - Ping sweep
  - TCP SYN sweep
- Map network topology
  - Traceroute
    - Sends out ICMP or UDP packets with increasing TTL
    - Gets back ICMP_TIME_EXCEEDED message from intermediate routers

Traceroute
1. ICMP_ECHO to www.victim.com
   TTL=1
   1a. ICMP_TIME_EXCEEDED from R1
   A: R1 is my first hop to www.victim.com!

2. ICMP_ECHO to www.victim.com
   TTL=2
   2a. ICMP_TIME_EXCEEDED from R2
   A: R1-R2 is my path to www.victim.com!

3. ICMP_ECHO to www.victim.com
   TTL=3
   3a. ICMP_TIME_EXCEEDED from R3
   A: R1-R2-R3 is my path to www.victim.com!
Traceroute

A: R1-R2-R3-www is my path to www.victim.com

Repeat for db and mail servers

Network Mapping Tools

Cheops
- Linux application
- http://cheops-ng.sourceforge.net/
  Automatically performs ping sweep and network mapping and displays results in GUI

Defenses Against Network Mapping And Scanning

Filter out outgoing ICMP traffic
- Maybe allow for your ISP only
- Use Network Address Translation (NAT)

How NATs Work

For internal hosts to go out
- B sends traffic to www.google.com
- NAT modifies the IP header of this traffic
  - Source IP: B ⇒ NAT
  - Source port: B’s chosen port Y ⇒ random port X
- NAT remembers that whatever comes for it on port X should go to B on port Y
- Google replies, NAT modifies the IP header
  - Destination IP: NAT ⇒ B
  - Destination port: X ⇒ Y

For public services offered by internal hosts
- You advertise your web server A at NAT’s address (1.2.3.4 and port 80)
- NAT remembers that whatever comes for it on port 80 should go to A on port 80
- External clients send traffic to 1.2.3.4:80
- NAT modifies the IP header of this traffic
  - Destination IP: NAT ⇒ A
  - Destination port: A’s service port 80
- A replies, NAT modifies the IP header
  - Source IP: A ⇒ NAT
  - Source port: 80 ⇒ 80
How NATs Work
- What if you have another Web server C
  - You advertise your web server A at NAT’s address (1.2.3.4 and port 55) – not a standard Web server port so clients must know to talk to a diff. port
  - NAT remembers that whatever comes for it on port 55 should go to C on port 80
  - External clients send traffic to 1.2.3.4:55
  - NAT modifies the IP header of this traffic
    - Destination IP: NAT \rightarrow C
    - Destination port: NAT’s port 55 \rightarrow C’s service port 80
  - C replies, NAT modifies the IP header
    - Source IP: C \rightarrow NAT, source port: 80 \rightarrow 55

Port Scanning
- Finding applications that listen on ports
  - Send various packets:
    - Establish and tear down TCP connection
    - Half-open and tear down TCP connection
    - Send invalid TCP packets: FIN, Null, Xmas scan
    - Send TCP ACK packets – find firewall holes
    - Obscure the source - FTP bounce scans
    - UDP scans
    - Find RPC applications

Port Scanning Tools
- Nmap
  - Unix and Windows NT application and GUI
  - http://nmap.org/
  - Various scan types
  - Adjustable timing

Defenses Against Port Scanning
- Close all unused ports
- Remove all unnecessary services
- Filter out all unnecessary traffic
- Find openings before the attackers do
- Use smart filtering, based on client’s IP

Firewalk: Determining Firewall Rules
- Find out firewall rules for new connections
- We don’t care about target machine, just about packet types that can get through the firewall
  - Find out distance to firewall using traceroute
  - Ping arbitrary destination setting TTL=distance +1
  - If you receive ICMP_TIME_EXCEEDED message, the ping went through
Defenses Against Firewalking
- Filter out outgoing ICMP traffic
- Use firewall proxies
  - This defense works because a proxy recreates each packet including the TTL field

Vulnerability Scanning
- The attacker knows OS and applications installed on live hosts
  - He can now find for each combination
    - Vulnerability exploits
    - Common configuration errors
    - Default configuration
- Vulnerability scanning tool uses a database of known vulnerabilities to generate packets
- Vulnerability scanning is also used for sysadmin

Vulnerability Scanning Tools
- SARA
  - [http://www-arc.com/sara](http://www-arc.com/sara)
- SAINT
  - [http://www.saintcorporation.com](http://www.saintcorporation.com)
- Nessus
  - [http://www.nessus.org](http://www.nessus.org)

Defenses Against Vulnerability Scanning
- Close your ports and keep systems patched
- Find your vulnerabilities before the attackers do

At The End Of Scanning Phase
- Attacker has a list of "live" IP addresses
- Open ports and applications at live machines
- Some information about OS type and version of live machines
- Some information about application versions at open ports
- Information about network topology
- Information about firewall configuration