Intrusion Penetration

CSC 154

Outline

- Network Auditing tools vs. Host-based Auditing tools
  - What information can be gathered respectively?
- Remote Exploits vs Local Exploits
- 3 typical penetration scenarios
- 7 typical steps of penetration
  - monitoring tools
  - stealth and backdoor tools

Network Auditing tools

- Remote scan to collect network information: alive IP addresses and network configuration;
  - IP range that is assigned to a particular domain
  - operating system type or specific versions
  - port scanning to find out running network applications (like port 80, 25, 22)
  - hardware and software information

- Specific version information indicates particular vulnerabilities;
- Nmap, as an example, a security scanner;

Host-based Auditing tools

- Local scan to gather local host information for vulnerabilities
  - physical access to the computer;
  - access to files, specific paths, directories;
  - operating system information (type, version);
  - access to password file;
    - login credentials;
    - user account information;
    - scan for passwords (like brute-force key guessing);
  - previous security holes left if compromised (like backdoors);

Remote Exploits

- attacks without authentic remote accounts
- usually after remote network auditing (nmap)
  - steal a password and then login in (packet sniffer)
  - attempts for firewall evasion (IP spoofing);
  - attack encryption weakness (brute-force key guessing attack)
  - exploit vulnerabilities with the operating system(buffer overflow)
  - exploit vulnerabilities with any running service program (sendmail)
  - email attachments with malicious code (virus);
  - solicit users to run malicious code (malicious applets);
  - execute remote commands (remote shell attacks);

Local Exploits

- What if the attacker has already gotten a local account?
  - He already has low privilege;
  - He can use local vulnerabilities to elevate himself to root (super-user) privilege;
    - password cracking;
    - kernel vulnerabilities;
      - Buffer overflow;
      - Null pointer dereference;
    - vulnerabilities of poorly written applications;
      - Buffer overflow;

Monitoring tools

- Monitor are typically passive;
  - Admin tools monitor user activities, like login, important events (file add, file delete);
  - Can be used for troubleshooting;

- Two popular monitors: sniffers and snoopers;
  - sniffer logs network raw data;
  - snoopers watch user operations. For example, snoopers can gain keystroke data;
  - Snooper needs local access, while sniffer does not need;

Stealth and Backdoor tools

- What's the goal of stealth?
  - The goal is not to steal;
  - Instead, its goal is to remove traces;
  - Trace information usually stored in audit files and logs;
  - The main way is to open the audit file and only remove the entries of attacker's action;

- What's the goal of backdoor?
  - The front door is NOT friendly to attackers due to the requirement of authentication;
  - If backdoors can be opened up (like using Trojan horses), then attacks can come into the house without the permission of the owner (no password is required);
  - Moreover, the use of backdoor itself is not under any monitoring (un-logged use);
  - Besides, the attacks can come back again and again later (continue use for reentry);
  - Normally more than one backdoor;

- Final result: unauthorized users to hide their trails in compromised systems.

Summary: what we have now

- Attack weapons
  - Denial-of-service
  - Virus
  - Worm
  - Packet sniffers
  - Spoofing
  - Malicious applets
  - War dialers
  - Logic bombs
  - Trojan horses
  - Buffer overflow
  - Social engineering
  - Dumpster diving
  - Password crackers
- Intrusion tools
  - Scanners
  - Remote exploit tools
  - Local exploit tools
  - Monitoring tools
  - Stealth and backdoor tools

3 typical penetration scenarios

- Remote to Local (Blind Remote Attack):
  - no user access to system;
  - generally only with the address or name of the target system;
  - attempts to gain more information (remote scanners);
  - remote exploit;
  - local to root attack;
- Local to Root (User Level Attack):
  - has un-privileged user account;
  - authorized or through earlier-stage hacking (blind remote attack);
- Physical Access:
  - with physical access to the computer;
- Combinations:
  - generally use blind attack first; then use the user level attack to get privileged access;
  - when someone leaves the computer on, you can gain the privilege of that user based physical access attack (password cracking)

7 typical steps of penetration

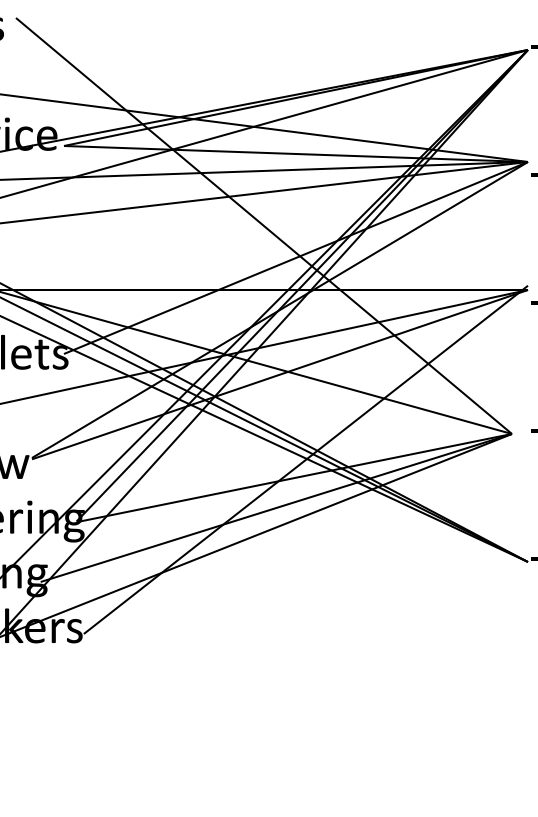
- 1. reconnaissance
  - use scanners to get public information about target systems or network
  - DNS queries, IP address queries, ping sweep, port scanning
- 2. probe and attack
  - uses reconnaissance information to probe the systems for more detailed information, such as the weakness information, usually in terms of specific vulnerabilities
- 3. toehold
  - exploit vulnerabilities found in Step 2 and gain entry into the system
  - remote exploits and local exploits
- 4. advancement
  - elevation from unprivileged access to privileged access
  - gain full internal access to establish a firebase to attack the whole internal network
  - local exploit tools
- 5. stealth
  - hide all traces and destroy all evidence
  - Install backdoors to enable reentry and remote control
  - stealth and backdoor tools
- 6. listening post
  - internal privileged access to data transmissions over the network
  - reconnaissance based on a firebase in internal network
  - sniffer programs and backdoor tools
- 7. takeover
  - move deeper into the network, take over more hosts in the network … finally the whole network if possible
  - sniffers, remote exploits and local exploits
- Penetration test: companies can do penetration attacks in order to find vulnerabilities before they are exploited

7 typical steps of penetration

- 1. scan to gather information;
- 2. use collected information to find vulnerabilities to use next;
- 3. exploit the vulnerability and get entry;
- 4. upgrade account from normal user to root;
- 5. remove traces and install backdoors;
- 6. listen to the target network to collect other hosts' info;
- 7. exploit and take over other hosts;

Attack Weapons and Intrusion Tools

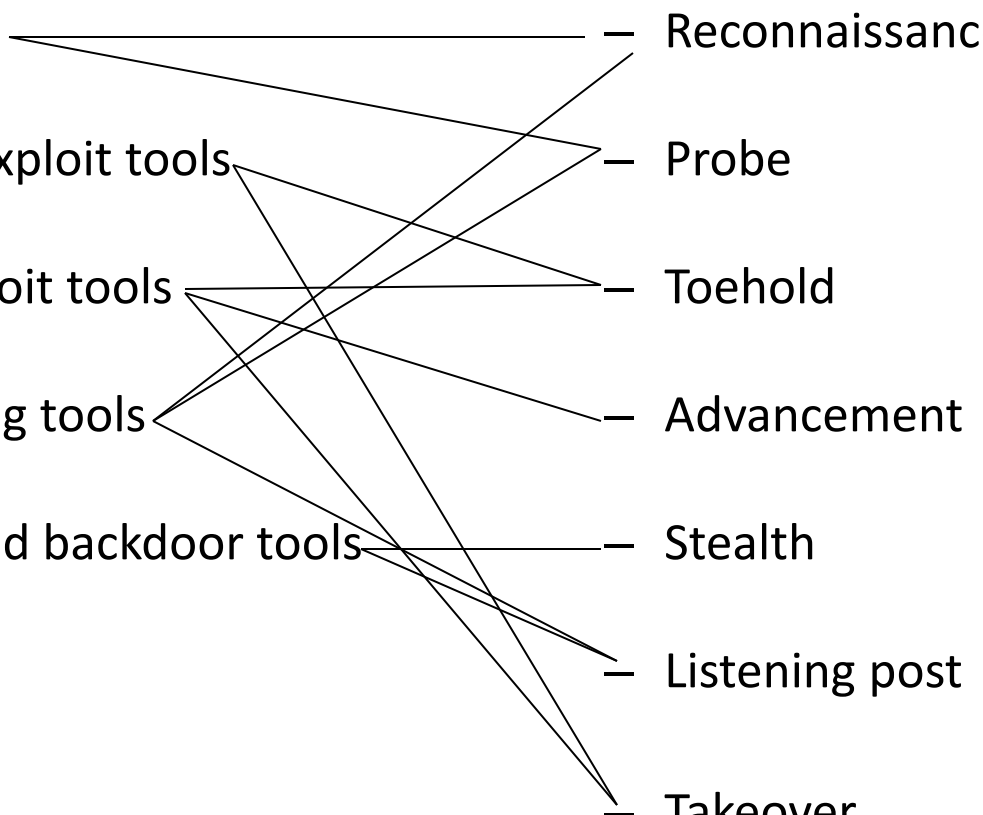
- Attack weapons
  - Packet sniffers
  - Spoofing
  - Denial-of-service
  - Virus
  - worm
  - Trojan horses
  - Malicious applets
  - Logic bombs
  - Buffer overflow
  - Social engineering
  - Dumpster diving
  - Password crackers
  - Snooper
  - Nmap
  - Nessus



- Intrusion tools
  - Scanners
  - Remote exploit tools
  - Local exploit tools
  - Monitoring tools
  - Stealth and backdoor tools

Intrusion Tools and Penetration Steps

- Intrusion tools
  - Scanners
  - Remote exploit tools
  - Local exploit tools
  - Monitoring tools
  - Stealth and backdoor tools
- Penetration steps
  - Reconnaissance
  - Probe
  - Toehold
  - Advancement
  - Stealth
  - Listening post
  - Takeover



The Big Picture (3)