Hacker's Methodology

(…a malicious mindset)

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

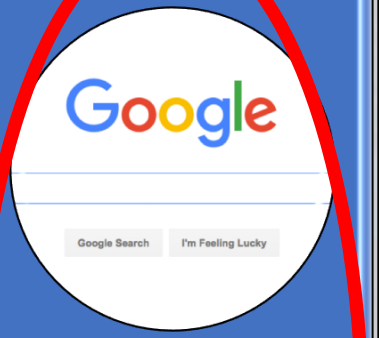
Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Hacker's Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

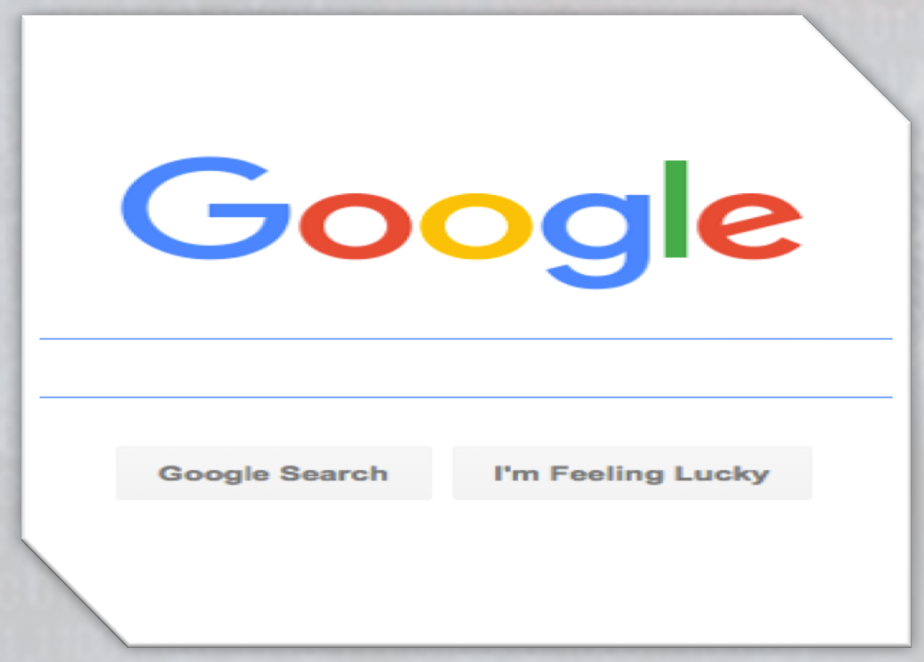
Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 1 - Performing Reconnaissance



- Systematic attempt to locate, gather, identify, and record information about a target (aka “Footprinting”)
- Reconnaissance techniques include:
  - Social engineering
  - Dumpster diving
  - Email harvesting
  - Internet or open-source research
- Only PASSIVE information gathering occurs

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 2 - Scanning & Enumeration

- Scanning
  - Actively connecting to the system and get response to identify open ports & services
- Enumeration
  - In-depth information gathering
    - Open shares
    - User accounts information
    - Software versions
- Compile the information gathered to build a target map before beginning your attack

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 3 - Gaining Access

- Performing exploits for the first time to attempt to gain access to target
- Client-side or remote exploitation attacks
  - Social engineering techniques
  - Open wireless connections
  - Unsecured or unpatched system
  - System vulnerability
  - Web applications vulnerabilities
  - Backdoors
  - Buffer overflows
  - Trojans

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 4 - Escalation of Privilege

- Gain administrative, system or root access by escalating the account's privileges
- Exploit a vulnerability or a bug in an application or the operating system
- After privilege escalation, attackers have full control over the system and/or network
- Gain administrator access over the workstation, then expand to domain administrator (if possible)

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 5 - Maintaining Access

- Attackers use techniques to maintain access:
  - Network sniffers
  - Steal additional passwords
  - Lateral movement to other targets
  - Opening ports and starting services
- Survey the host and understand its posture
  - Look for others on the system…are you alone?
- Goal is keep persistent access
- Now, you are ready for data exfiltration, data compromise, system takeover, ...

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Step 6 - Covering Tracks

- Erase evidence of their attack
  - Temp files
  - Log files
  - Previous stage malware (if used)
- Modifying log files
  - Access times
  - User identity
- Hiding files and folders
- Alternate Data Streams (ADS)
- Installing rootkits
- Installing backdoors
- Setup call backs for designated times

Hacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Hacker's Methodology

(…a malicious mindset)