
Gaining Access Phase
(…finding my foothold)
http://www.JasonDion.com

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Gaining Access Phase

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

Gaining Access

1. Identify a target vulnerability
2. Find a matching exploit
3. Select a payload

Vulnerability

- Software coding error (bug) or a misconfiguration that could allow an attacker the ability to gain access

Exploit

- Method of delivery of a payload to accomplish gaining access to the victim machine

Payload

- Effect caused by a virus or other malicious code executed by the exploit on the target computer

Deeper Dive…coming up next!

- Exploits (Buffer Overflows)

- Payloads
  - Shell Code
    - Bind & Reverse
  - Meterpreter

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Gaining Access Phase


Gaining Access Phase
(…finding my foothold)
http://www.JasonDion.com