Pentest +

Exploitation Process

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

Exploitation

General Steps in Exploitation

1. Recon and Information Gathering
2. Analysis and choosing initial target(s)
3. Exploit and pivot
   - Persistent access
   - Conceal evidence
4. From a pen-tester perspective
   - Consider SOW / rules of engagement
   - Consider goals of pen-test
   - Consider combination of skills and information at your disposal

Steps to the Cyber Kill Chain

1. **Reconnaissance** (Info gathering and vulnerability identification)
   - Gather OSINT of the target
   - Detect potential target endpoints / vulnerabilities
2. **Weaponization** (attacking and exploiting)
   - Develop specific attack tool
   - Use automated toolkits
3. **Delivery** (attacking and exploiting)
   - Attacking a network endpoint or application
   - Conducting social engineering attack
   - Distributing malware
   - Dropping infected USB
   - Sending phishing email
4. **Exploitation** (attacking and exploiting)
   - Triggering the malware payload
   - Attacker gains foothold on network
   - May occur directly with delivery or afterwards depending on attack type
5. **Installation** (attacking and exploiting)
   - Establish persistent access to the target system
6. **Command and Control** (attacking and exploiting)
   - Further the attack by issuing commands to the compromised target
7. **Action on Objectives** (attacking and exploiting)

    - Attain objectives of the attack
    - Exfiltrate data
    - Attain DOS
    - Use unauthorized resources
    - Delete or modify target information

Exploitable Test Environments

Metasploitable V2 and V3

- VM's that have vulnerabilities for practice
- Older versions of OS or Applications
- Windows XP, 7, 2008 Server
- Older Linux OS

Websites for Pentesting

- **Hack the Box**
    - https://www.hackthebox.eu/
- **CTFlearn**
    - https://ctflearn.com/
- **bWAPP**
    - http://www.itsecgames.com/
- **HackThisSite**
    - https://www.hackthissite.org/
- **Google Gruyere**
    - https://google-gruyere.appspot.com/
- **Hellbound Hackers**
    - https://www.hellboundhackers.org/
- **OWASP Mutillidae II**
    - https://github.com/webpwnized/mutillidae
- **HackThis!!**
    - https://defendtheweb.net/
- **WebGoat**
    - https://github.com/WebGoat/WebGoat
- **Root Me**
    - https://www.root-me.org/
- **OverTheWire**
    - https://overthewire.org/wargames/

Mobile Apps for Pentesting

- **Damn Vulnerable iOS App – DVIA**

  - https://github.com/prateek147/DVIA-v2

Vulnerability Databases & Exploit Code

Exploit Code

- Can be dangerous because could contain other unexpected malware
- Downloading exploit code can set of virus scanners on host
- Should verify that checksum matches if available

Exploit Database

- https://www.exploit-db.com/
- Specific details about exploits
- Shellcode sometimes available for proof-of-concept
- Security research papers
- Google Hacking Database (Google Dorks)

Rapid 7 Vulnerability and Exploit Database

- https://www.rapid7.com/db/
- Plugins for Metasploit Framework and Metasploit Pro

NVD – National Vulnerability Database

- https://nvd.nist.gov/
- Does not provided exploit code
- References may mention if exploits are available and their names

VULDB

- https://vuldb.com/
- Crowd-sourced vulnerability database
- Includes estimated prices and rankings for exploit code
- Can help understand market focus and lead the scoping process of a penetration test

Mitre CVE

- https://cve.mitre.org/cve/
- A list of publicly disclosed cybersecurity vulnerabilities that is free to search, use, and incorporate into products and services

CVE Details

- https://www.cvedetails.com/
- https://www.itsecdb.com/oval/
- Provides a web interface to all IT security related items including patches, vulnerabilities and compliance checklists
- Collects OVAL (Open Vulnerability and Assessment Language) definitions from many sources

Bugtraq ID (BID)

- https://www.securityfocus.com/bid/
- CVE to BugTraq ID concordance
  - https://cve.mitre.org/data/refs/refmap/source-BID.html

Developing Exploits

- The media release / announcement of a vulnerability includes details on how and why they occur
- Exploit developers can probe the software, service, tools, OS that contains the vulnerability
- Develop code that can automate the exploitation process
- **Exploit Writing Tutorials**
  - https://www.corelan.be/index.php/articles/
- **Fuzzy Security**
  - http://www.fuzzysecurity.com/tutorials.html
- **Proof-of-concept exploits**
  - Do not deliver malicious payload, but rather focus on proving that the vulnerability can be exploited
  - **Exploit Development Tutorials and Courses:**
    - https://www.anitian.com/a-study-in-exploit-development-part-1-setup-and-proof-of-concept/
    - **SANS**
      - https://www.sans.org/event/cyber-defense-initiative-2019/courses?unavailable
- **Exploit Modification**
  - Exploit code can require configuration or modification
    - Can help it bypass virus scanning software / IDS
  - Proof-of-concept exploits can be modified to deliver more extensive payloads
  - Metasploit framework plugins are written in a standardized format
- **Exploit Chaining / Combination Attack**
  - Exploitation can require a series of exploits to gain the desired level of access
  - Multiple steps involved in privilege escalation and arbitrary code execution