Penetration testing steps in Kali Linux

Module #13

Penetration testing concepts

Step 1: Reconnaissance

Step 2: Target Evaluation

Step 3: Exploitation

Step 4: Privilege escalation

Step 5: Maintaining a foothold

Penetration testing: Reconnaissance

Step 1: Reconnaissance

- learn as much as possible about a target's environment and system traits prior to launching an attack
- first step of a Penetration Testing service engagement
- begins by defining the target environment based on work scope
- Once the target is identified, research is performed to gather intelligence on the target like:
    - Ports used
    - Hosting location
    - Place of hosting
    - Type of services offered to clients

Penetration testing: Reconnaissance

Reconnaissance services include:

- Researching a targets footprint in Internet
- Monitoring resources, people and processes
- Scanning for network information such as IP Addresses
- Use social media or social engineering public services

Deliverables from reconnaissance service:

- List of all assets being targeted
- List of applications being used
- Possible asset owners for targets

Reconnaissance in Kali Linux

"Information Gathering" menu bar

- Tools include methods to research network, data center, wireless, and host systems.

The following is the list of Reconnaissance goals:

- Identify target(s)
- Define applications and business use
- Identify system types
- Identify available ports
- Identify running services
- Passively social engineer information
- Document findings

Step 2: Target evaluation

- Pre-requisite for entering this phase:
  - Tester should know enough about a target for analyzing vulnerabilities or weakness

Examples for testing for weakness:

- How the web application operates, identify services, communication ports, or other means

Vulnerability Assessments and Security Audits typically conclude after this phase of the target evaluation process.

Step 2: Target evaluation (Contd.)

Detailed information through Reconnaissance:

- Improves accuracy of targeting possible vulnerabilities
- Shortens execution time to perform target evaluation services
- Helps to avoid existing security.

Example: Running a generic vulnerability scanner against a web application server

- Would probably alert the asset owner
- Take a while to execute and only generate generic details about the system and applications

Scanning a server for a specific vulnerability based on data obtained from Reconnaissance would be harder for the asset owner to detect, provide a good possible vulnerability to exploit, and take seconds to execute.

Step 2: Target evaluation (Contd.)

Evaluating targets for vulnerabilities could be manual or automated through tools.

There is a range of tools offered in Kali Linux grouped as a category labeled Vulnerability Analysis.

Tools range from assessing network devices to databases.

The following is the list of Target Evaluation goals:

- Evaluation targets for weakness
- Identify and prioritize vulnerable systems
- Map vulnerable systems to asset owners
- Document findings

Step 3: Exploitation

To verify if the vulnerabilities are real and what possible information or access can be obtained.

Exploitation separates Penetration Testing services from passive services such as Vulnerability Assessments and Audits.

Exploitation and all the following steps have legal ramifications without authorization from the asset owners of the target.

Step 3: Exploitation (Contd.)

The success of this step is heavily dependent on previous efforts.

Most exploits are developed for specific vulnerabilities and can cause undesired consequences if executed incorrectly.

Best practice is identifying a handful of vulnerabilities and developing an attack strategy based on leading with the most vulnerable first.

Step 3: Exploitation (Contd.)

Exploiting targets can be manual or automated depending on the end objective. Some examples are running

SQL Injections to gain admin access to a web application

Social engineering a Helpdesk person into providing admin login credentials.

Kali Linux offers titled Exploitation Tools for exploiting targets that range from exploiting specific services to social engineering packages.

The following is the list of Exploitation goals:

- Exploit vulnerabilities
- Obtain foothold
- Capture unauthorized data
- Aggressively social engineer
- Attack other systems or applications
- Document findings

Step 4: Privilege escalation

Having access to a target does not guarantee accomplishing the goal of a penetration assignment.

In many cases, exploiting a vulnerable system may only give limited access to a target's data and resources. The attacker must escalate privileges granted to gain the access required to capture the flag, which could be sensitive data, critical infrastructure etc.

Privilege Escalation can include

identifying and cracking passwords, user accounts, and unauthorized IT space.

An example is achieving limited user access, identifying a shadow file containing administration login credentials, obtaining an administrator password through password cracking, and accessing internal application systems with administrator access rights.

Step 4: Privilege escalation(Contd.)

Kali Linux includes a number of tools that can help gain Privilege Escalation through the Password Attacks and Exploitation Tools catalog. Since most of these tools include methods to obtain initial access and Privilege Escalation, they are gathered and grouped according to their toolsets.

The following is a list of Privilege Escalation goals:

- Obtain escalated level access to system(s) and network(s)
- Uncover other user account information
- Access other systems with escalated privileges
- Document findings

Step 5: Maintaining a foothold

The final step is maintaining access by establishing other entry points into the target and, if possible, covering evidence of the penetration.

It is possible that penetration efforts will trigger defenses that will eventually secure how the Penetration Tester obtained access to the network. Best practice is establishing other means to access the target as insurance against the primary path being closed.

Alternative access methods could be backdoors, new administration accounts, encrypted tunnels, and new network access channels.

Step 5: Maintaining a foothold(Contd.)

The other important aspect of maintaining a foothold in a target is removing evidence of the penetration. This will make it harder to detect the attack thus reducing the reaction by security defenses.

Removing evidence includes erasing user logs, masking existing access channels, and removing the traces of tampering such as error messages caused by penetration efforts.

Step 5: Maintaining a foothold(Contd.)

Kali Linux includes a catalog titled Maintaining Access focused on keeping a foothold within a target. Tools are used for establishing various forms of backdoors into a target.

The following is a list of goals for maintaining a foothold:

- Establish multiple access methods to target network
- Remove evidence of authorized access
- Repair systems impacting by exploitation
- Inject false data if needed
- Hide communication methods through encryption and other means
- Document findings

Thank You