Penetration Testing

Introduction

Penetration testing is a structured form of testing defenses using the methodologies employed by attackers.

Penetration testing is useful in

- They can show relationships between a series of "low-risk" items that can be sequentially exploited to gain access (making them a "high risk" item in the aggregate).
- They can be used to test the training of employees, the effectiveness of your security measures, and the ability of your staff to detect and respond to potential attackers.
- They can often identify and test vulnerabilities that are difficult or even impossible to detect with traditional scanning tools.

Most recognized methodologies:

- Open Source Security Testing Methodology Manual (OSSTMM) method.
- Open Web Application Security Project (OWASP) — Most recognized
- SP 800-115, "Technical Guide to Information Security Testing and Assessment" (Released by the The National Institute of Standards and Technology (NIST)) — Most basic
- The Penetration Testing Methodologies and Standards framework (PTES)
- Information System Security Assessment Framework (ISSAF)

Figure 8-1 NIST Penetration Test process model from SP 800-115

All of these frameworks define a process to be followed by the pen testers

Exam Tips

Penetration tests are focused efforts to determine the effectiveness of the security controls used to protect a system.

Footprinting is the first step in gaining active information on a network during the reconnaissance process.

Unknown environment testers have no knowledge of the inner workings and perform their tests from an external perspective.

Known environment testers have detailed knowledge of the inner workings and perform their tests from an internal perspective.

Partially known environment testers have partial knowledge.

Lateral movement and pivoting work hand in hand. The purpose of lateral movement is to go to where the data is, and pivoting is one of the key methods of learning where to move next.

OSINT describes using public information sources to gain information about a target and find methods that will improve the odds of a successful campaign.

The differences between active and passive reconnaissance techniques, is an easy test question.

Passive reconnaissance is stealthy and doesn't actively engage the target system.

Active reconnaissance engages the system or network and can gather much more information, but it can also be traced.

A bug bounty program is a formal approach to identifying bugs. These programs are often open to the public, and the firm that runs the program sets the rules of engagement.

Lateral movement, privilege escalation, and persistence are common tools in the toolbox of attackers and penetration testers. They are frequently used together, but each has its unique characteristics. For questions involving them, be sure to examine to which unique characteristic the question is referring in order to pick the correct answer.

Remember that the red team is the attacker, the blue team is the defender, the white team is the exercise manager/judge, and the purple team is composed of a combination of red and blue team members.

Techniques

Lateral movement

The process used by attackers to move deeper into a network to get to the target data.

Privilege Escalation

- The process of gaining increased privileges for an account.
- Gaining root or admin access is always a goal for an attacker.
- 2 Types
  - Horizontal — The attacker expands their privileges by taking over another account and misusing the legitimate privileges granted to the other user. (Other users in the same levels)
  - Vertical — The attacker attempts to gain more permissions or access with an existing account they have already compromised. (Other users that are of higher level)

Lateral Movement

Persistence

The ability to exist beyond a machine reboot or after disconnection.

The term advanced persistent threat (APT) refers to a methodology that is focused first and foremost about maintaining persistence.

Cleanup

- Attacking a system can leave a lot of evidence laying around.
- It is one of the important steps that can be taken to avoid detection

Pivoting

- In pivoting, the attacker moves to a new location in a network and begins the attack process over again, performing scans to see machines that were not visible from the outside
- One of the giveaways of this activity is internal scanning.
- Slowing down their scans is one method an attacker can use to avoid detection, but this stretches out their engagement.

Teams

Red Team

Red teams are composed of members who are focused on offense.

Red teams are frequently third-party contractors, as their skill set is specialized and the required skill level is high.

Blue Team

The blue team is the defense team and, as such, is typically an in-house operation, unless the defensive efforts are outsourced.

Typically have 2 functions one to establish defense and the other is to monitor and response for any unauthorized behaviors.

White Team

White team members are there to ensure that the actual exercise stays on track and employs the desired elements of a system.

Purple Team

A purple team is composed of both red team and blue team members.

These team members work together to establish and test defenses.

Environments

Known Environment (white box)

- Test the internal structures and processing within an application for bugs, vulnerabilities, and so on.
- white box tester will have detailed knowledge of the application they are examining.
- Known environment testing is often used to test paths within an application (if X, then go do this; if Y, then go do that), data flows, decision trees, and so on.

Unknown Environment (black box)

- Unknown environment techniques test the functionality of the software, usually from an external or user perspective.
- Testers using black box techniques typically have no knowledge of the internal workings of the software they are testing.
- They put input in and look at the output as they don't have internal knowledge of the system.
- Test cases for unknown environment testing are typically constructed around intended functionality (what the software is supposed to do) and focus on providing both valid and invalid inputs.

Partially Known Environment (gray box)

In a partially known environment test, the testers typically have some knowledge of the software, network, or systems they are testing.

Bug Bounty

- Bug bounty programs are mechanisms where companies pay hackers for revealing the details of vulnerabilities that they discover, providing the companies an opportunity to correct the issues.
- For bug hunting to be legal, the firm must have an established bug bounty program, and the hunting activity must be in accordance with that program.
- Finding a vulnerability and attempting to sell it to a company without a bug bounty program is often met with a very strong legal response and potentially a criminal investigation.

Rules of Engagement

- The rules of engagement specify the legal authority that the penetration testers have in performing their duties. The rules of engagement also establish the boundaries associated with the test so that it is actually exercising the functions desired by the customer.
- Importance
  - The activities associated with a penetration test are illegal if not authorized.
  - Incident response team might respond and waste resources if an attack out of the scope that they are informed with is performed
- Typical rules of engagement will include a boundary of what is in scope and what is not. (i.e. IP addresses, domains, subdomains, etc..)
- Other items might be elements such as time of testing activity.
- Any changes to the environment should be noted and either removed or clearly provided to the blue team.
- How the penetration testers should interact with other employees when discovered should also be included, as should a complete contact list of whom to call when something happens that requires immediate enterprise attention.

Reconnaissance

2 Types

Passive

- Reconnaissance is performed using methods to gain information about targeted computers and networks without actively engaging with the target systems and thus avoiding detection.
- Has limits on how much an attacker can learn, but it's completely stealthy

Active

- The attacker engages with the target system, typically conducting a port scan to find any open ports.
- Active reconnaissance involves using packets that can be traced; it involves engaging services that can be logged.
- Much more informative, but it tells the machines they are being "attacked."

Footprinting

- The first step in gaining active information on a network.
- The primary method of gathering this information is via network sniffing and the use of scanning software.

Open Source Intelligence (OSINT)

- The technique of using publicly available information sources to gather information on a system.
- Not a single method but rather an entire set of both qualitative and quantitative methods that can be used to collect useful information.

Drones & Special Techniques

- Drones are unmanned aerial platforms capable of carrying cameras, mobile devices, and other items across normal boundaries.
- This provides pen testers a means of getting closer to signals such as wireless networks and then recording traffic.

War Flying

- The act of using a drone to fly over a facility and capture wireless network traffic

War driving

- Same concept as war flying, but rather than using a drone to capture the traffic, one simply drives past the points of access.

War Shipping

- The attacker ships a specially set up mobile phone to a location.
- This device has a large external battery and special software.
- The phone is constantly running and collecting network data, and at periodic intervals, it uses its cellular capability to package and send out bursts of collected data.