Network penetration

Attacks AND Testing

IZOUNTAR
MOUHAMED

ITRODUCTION

A critical aspect of the digital landscape,in our today's world the reliance on technology is greater then ever and the need to assure the networks security against Cyber attacks become paramount,To do that Rather than waiting for malicious actors to find and exploit vulnerabilities, organizations are adopting penetration testing as a strategic tool to identify weaknesses and fortify their defenses,Networks security isn’t all about preventing unauthorized access. It's about ensuring the confidentiality, integrity, and availability of data and services. As technology advances, so do the tactics of those seeking to exploit vulnerabilities. Our goal is to stay ahead of the curve, and that's where network penetration testing comes into play.

Definition

the network penetration attacks and the network penetration testing is tow face’s of the same coin

NPA

Network penetration attacks, often simply referred to as penetration attacks or Cyber attacks, involve intentional efforts to exploit vulnerabilities in a network with the goal of unauthorized access, data theft, disruption of services, or other malicious activities. These attacks can take various forms, including exploiting software vulnerabilities, using malware, or leveraging social engineering techniques to gain access to sensitive information or compromise the integrity of the targeted system

The aim of a network penetration attack is to identify weaknesses in security defenses and exploit them for malicious purposes.

NPT

Network penetration testing, on the other hand, is a proactive and authorized approach to evaluating the security of a network. Also known as ethical hacking or pen testing, this process involves simulating real-world Cyber attacks to identify vulnerabilities and weaknesses in a controlled environment.

The primary goal of network penetration testing is to assess the effectiveness of security measures, discover potential entry points for attackers, and provide recommendations for strengthening the overall security posture.

Objectives

1

Defining Network Penetration Attacks

2

Introducing Network Penetration Testing

3

Understanding the Threat Landscape

Types of Attack

Man-in-the-Middle

Attackers intercept and potentially alter the communication between two parties without their knowledge

Denial-of-Service

Attempts to make a machine or network resource unavailable to its intended users.

Zero-Day Exploits

Exploiting vulnerabilities in software or hardware that are not yet known to the vendor or have not been patched.

Targets

In both network penetration attacks and network penetration testing, the target is networks within an organization. However, the intent and authorization differ significantly between these two activities.

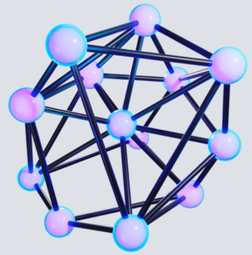
NPA

Unauthorized Access
Data Breach
Disruption of Services
Malware Deployment
System Manipulation

NPT

Authorized Assessment
Identifying Vulnerabilities
Risk Mitigation
Assessing Defenses
Providing Recommendations

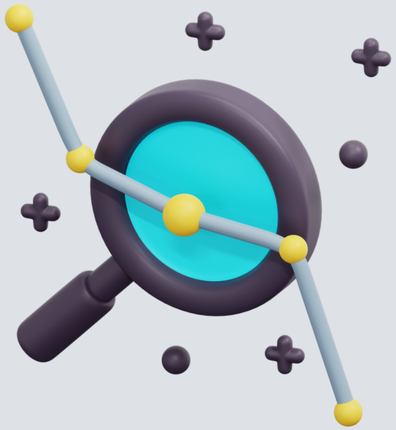
Attack Stages



it likely the same stages for the tow they only deference between the tow is the last steps witch the true interest appear for npa and npt

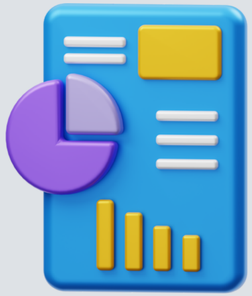
Planning — **Reconnaissance** — **Scanning** — **Gaining Access** — **Maintaining Access**

Attack Stages



Here comes the biggest deference between the npa and the npt because this steps are only in the npt to improve the security of the network

Analysis **Reporting**



Impacts

the impacts of this tow topics is letterly the opposite of each other because the motivation of the tow group is completely different in which the npa represent the black hat and the npt represent the white hat

NPA

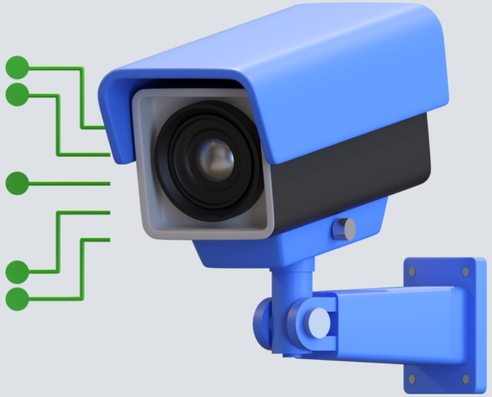
- Data Breaches
- Financial Loss
- Reputation Damage
- Disruption of Services
- Intellectual Property Theft
- National Security Concerns

NPT

- **Identification of Vulnerabilities**
- **Risk Mitigation**
- **Improved Security Awareness**
- **Validation of Security Controls**
- **Enhanced Trust and Reputation**
- **Protection of Sensitive Data**

Testing

Detection



BEHAVIORAL ANALYSIS

Analyzing user behavior to detect unusual patterns, such as unexpected access to sensitive data or irregular login times, can help in identifying insider threats or compromised accounts.

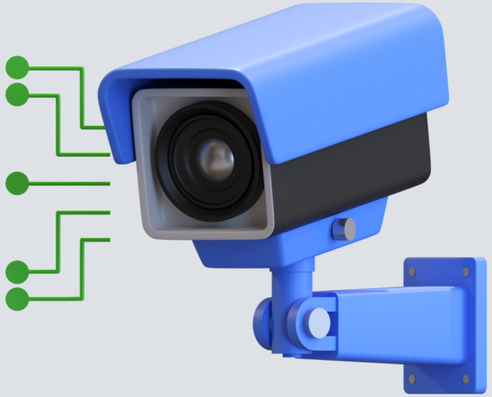
PENETRATION TESTING:

Conducting regular ethical hacking exercises to simulate real-world attack scenarios and identify vulnerabilities before attackers exploit them.

NTRUSION DETECTION SYSTEMS (IDS) AND INTRUSION PREVENTION SYSTEMS (IPS)

These systems monitor network traffic for suspicious activities or patterns that could indicate an attack. IDS detects and alerts while IPS can actively block or prevent these attacks.

Prevention



FIREWALLS

Implementing and properly configuring firewalls to control incoming and outgoing network traffic can prevent unauthorized access and filter out potentially malicious data packets.

EMPLOYEE TRAINING

Educating employees about cybersecurity best practices, including recognizing phishing attempts and avoiding suspicious links or downloads, can significantly reduce the likelihood of successful attacks.

STRONG AUTHENTICATION

Enforcing strong password policies, implementing multi-factor authentication (MFA), and using biometrics can significantly enhance network security by making it harder for unauthorized users to gain access.

Case Studies

The Stuxnet Worm

The Stuxnet worm was a sophisticated cyberweapon that was used to target Iran's nuclear program in 2010. The worm was designed to spread through infected USB drives and then attack Siemens industrial control systems that were used to operate centrifuges at the Natanz enrichment facility. Stuxnet was able to disrupt the operation of the centrifuges, causing significant damage to Iran's nuclear program.

The Forgotten PBX Account

A penetration tester was hired to test the security of a large financial services firm. After weeks of scanning and probing, the tester finally found a vulnerability – a long-forgotten PBX field-manager user account that had never been disabled. The tester was able to use this account to gain access to the company's internal network, where they found a number of other vulnerabilities that could have been exploited by attackers.

Conclusion

The Conflict between network penetration attacks and network penetration testing is the reason of the High speed in progress in the industry of network security,and the importance of the network penetration testing is non questionable and must be done Periodically to avoide any new threats

Thank you!

Do you have any questions?