2025/09/03

Penetration Test & Vulnerability Analysis

Presented by: ZHENGZHENG LI

Agenda

01 **Project Overview & Objectives**

02 **Testing Methodology**

03 **Key Findings & Evidence**

04 **Root Cause Analysis**

05 **Remediation & Best Practices**

06 **Conclusion**

01 Project Overview

Objective

Identifying security weaknesses

In the controlled laboratory environment, the security vulnerabilities and weaknesses in the system are comprehensively investigated to provide a basis for subsequent security improvements.

Verify the effectiveness of system hardening

Through the actual test, evaluate whether the system reinforcement measures can effectively resist potential security threats and ensure the security of the system.

Scope of Project

Internal network segment

The internal network segment involved in the project is 192.168.2.0/24, which contains multiple target systems.

Target system-Windows Server 2022

The IP address is 192.168.2.102, which is used as a file server to store important data information.

Target System-Fedora 41 Workstation

The IP address is 192.168.2.105, which undertakes the function of DNS service and is responsible for domain name resolution.

Target system-Ubuntu 24.04.2 LTS Server

The IP address is 192.168.2.103 and provides SSH services for remote connection and management.

Target system-Windows 10 Client

The IP address is 192.168.2.108, which serves as the client device for users to perform daily operations.

Project Approach

Grey-box penetration test

The tester has part of the system information and simulates the behavior of a real attacker to conduct a comprehensive penetration test on the system to find potential security vulnerabilities.

Nessus Vulnerability Scanning

Use the Nessus vulnerability scanning tool to automatically detect vulnerabilities in the target system and quickly find known vulnerabilities in the system.

Combined Approach

The combination of grey box penetration testing and Nessus vulnerability scanning can give full play to the advantages of both and improve the accuracy and comprehensiveness of vulnerability discovery.

02 Test Method

Reconnaissance

Network discovery tools

During the reconnaissance phase, network discovery is conducted using nmap and NetDiscover. For example, nmap can rapidly scan target network segments192.168.2.0/24 to identify active hosts. It efficiently detects target systems, such as hosts with IP addresses like 192.168.2.102 and 192.168.2.105.

Service enumeration method

Through service enumeration, we can understand the specific services running on the target host. For example, for the target system 192.168.2.102, we can find its running services such as WinRM (port 5985) and SMB (port 445), which provide key information for subsequent attacks.

Utilization Phase

Authentication attack methods

The authentication attack used a brute force approach. For example, the WinRM service (port 5985) on target 192.168.2.102 was guessed by the user name and password (eviluser:Password123!) to gain control of the system.

Specific service attack techniques

Service-specific attacks target different services. For example, an SMB service (port 445) on the target 192.168.2.102 was exploited for its lack of mandatory SMB signing. Combined with Nessus plugin ID 57608 and the CrackMapExec tool, this discovery identified a risk of an SMB Relay attack.

Cyber Attack Strategies

Cyber attacks employ ARP poisoning and man-in-the-middle (MITM) attacks. Taking a target network as an example, a successful ARP poisoning attack positions the attacker in an MITM role. For instance, when attacking the SMB service on target 192.168.2.102, this strategy was employed.

Post-utilization Phase

Establishing foothold process

In establishing the foothold, the Evil-WinRM tool was employed. Targeting IP address 192.168.2.102, after obtaining a weak password, we successfully established a remote PowerShell session using CrackMapExec and Evil-WinRM, thereby achieving initial control over the system.

Client attack preparation

Client attack preparation is an important part of the post-utilization stage. Through the analysis and configuration of the controlled system, it lays the groundwork for the subsequent attack on the client, so as to expand the scope and impact of the attack.

Vulnerability Verification Phase

Manual discovery results

Manual discovery results include vulnerabilities found through various tools and methods. For example, the DNS service (port 53) on target 192.168.2.105 was manually discovered using dig and dnsrecon tools to identify issues with recursive queries allowed by the DNS server.

Nessus scan results

Nessus scans can find a large number of potential vulnerabilities. For example, for the target system, Nessus plugin ID 12217 (CVSS 5.3) points out the risks of DNS services, providing an important basis for vulnerability verification.

Cross validation process

Cross-verification is to compare the manually discovered results with the Nessus scan results. For example, for DNS disclosure issues, manually verify the results with the information prompted by the Nessus plugin to ensure the accuracy and reliability of the vulnerability.

03 Key Findings

Windows Server Breached

Compromised System

The target of the attack was a Windows Server 2022 file server with the IP address 192.168.2.102.

Attacks services

The service that was attacked was WinRM (port 5985), which is often used to remotely manage Windows systems.

Proof of Compromise

Through brute force cracking, the weak credentials "eviluser:Password123!" were guessed and a remote PowerShell session was obtained using the CrackMapExec and Evil-WinRM tools.

Impact of the attack

The attacker successfully obtained full administrative control of the Windows server and was able to do whatever he wanted with the server.

SMB Signature and Man-in-the-middle Risk

Risk objectives

The target is a server with the IP address 192.168.2.102, and its running SMB service has security risks.

Aid services

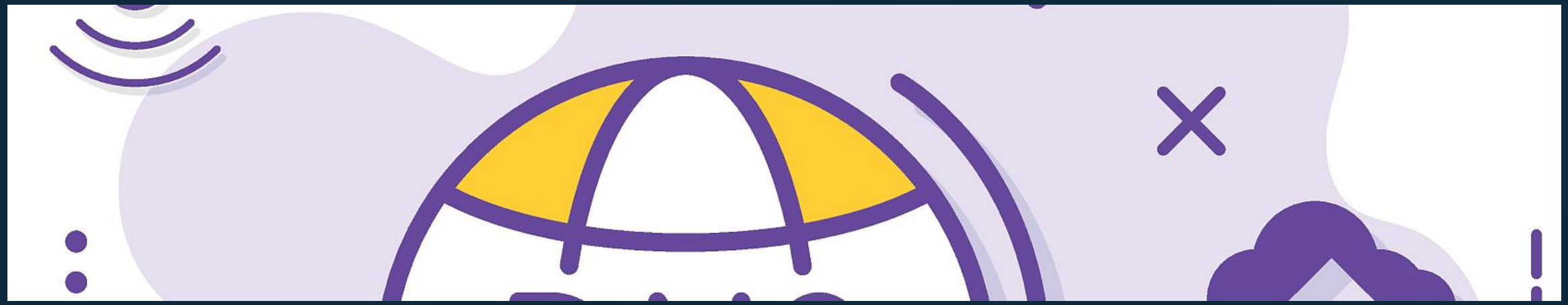
SMB (port 445) service, which is used for file and printer sharing functions.

Evidence of risk

The problem was detected through the Nessus plugin ID 57608 (CVSS 5.3), and CrackMapExec also confirmed that the SMB signature was not enabled (signing: False).

Concept validation

The successful implementation of ARP poisoning attack, which puts the attacker in the middle, proves the potential risk of SMB relay attack.



DNS Information Disclosure

Leaked targets

The target is a Fedora 41 workstation with the IP address of 192.168.2.105, which is a DNS server with information leakage problems.

Aid to Affected Services

DNS (port 53) service, responsible for domain name resolution and other functions.

Leaked evidence

The Nessus plugin ID 12217 (CVSS 5.3) detected the problem and was manually verified using dig and dnsrecon tools.

Impact of leaks

Because DNS servers allow recursive queries from untrusted clients, attackers can reveal browsing habits on the internal network through cache snooping.

Security Configuration Status

Advantages of Ubuntu servers

Ubuntu Server (192.168.2.103) only opened the SSH port and forced the use of key-based authentication, and Nessus did not find high/medium level vulnerabilities.

Windows 10 client advantages

The Windows 10 client (192.168.2.108) has no open ports, and the firewall policy effectively blocks all unrequested inbound traffic, and no web-based attack surface is found.

Finding: Secure Configurations Validated

The hardening of Ubuntu servers and Windows 10 clients is very effective, proving that good security configurations can significantly reduce system risks.

Network Attack Demonstration

ARP poisoning attack

The use of theettercap tool to successfully implement an ARP poisoning (man-in-the-middle) attack on the gateway and Windows Server demonstrates the vulnerability of the ARP protocol in the network.

LLMNR/NBT-NS poisoning attack

The responder tool successfully poisoned the request, proving that there is a risk of credential interception, which could lead to the disclosure of user account information.

SMB relay attack

Although the SMB relay attack was prepared, it was not triggered due to the lack of client traffic during testing, but it also illustrates the potential risk of such attacks on network infrastructure.

04 Root Cause Analysis

Weak Password Problem

01

Password guessing attacks

In this penetration test, the WinRM service (port 5985) on Windows Server 2022 (IP: 192.168.2.102) was successfully guessed by brute force cracking, and the weak password "eviluser:Password123!" was obtained. Then, the remote PowerShell session was obtained using CrackMapExec and Evil-WinRM tools, and the system was completely controlled.

02

Common Root Cause

Weak passwords have become the main cause of serious attacks on systems. In this test, many systems are faced with security threats due to weak passwords, highlighting the huge hidden dangers of weak passwords in the security system.

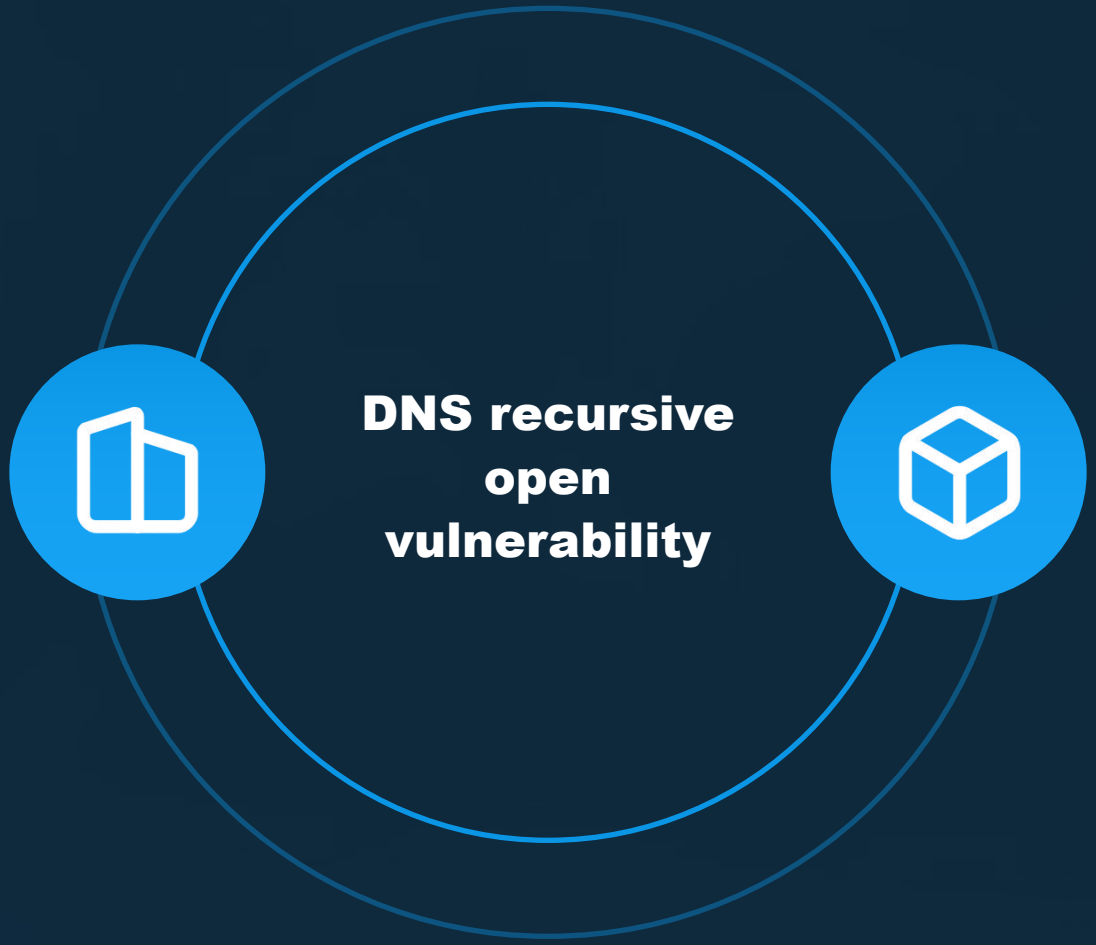
Misconfigured Services

SMB signature disable risk

The SMB service (port 445) on target 192.168.2.102 shows that the Nessus plugin ID 57608 (CVSS 5.3) does not enforce SMB signing, with CrackMapExec also confirming "signing: False". This leaves the system vulnerable to SMB Relay attacks and enables man-in-the-middle (MITM) attacks through successful ARP poisoning attempts.

Misconfigured Services

The LLMNR/NBT-Ns protocol is enabled by default, which leaves the system vulnerable to credential stuffing attacks. During testing, the "Responder" tool successfully executed a credential stuffing attack on the request, demonstrating the protocols vulnerability to credential interception.



The DNS server (IP: 192.168.2.105, port 53) allows recursive queries from untrusted clients. This vulnerability was identified through Nessus plugin ID 12217 (CVSS 5.3) and manually verified using the "dig" and "dnsrecon" tools. Such configuration enables cache probing that exposes browsing patterns within internal networks.

Insecure Protocols by Default

LLMNR/NBT-NS enabled, allowing for poisoning attacks.

Default Enabled Risk

Potential attack pathways

Due to these insecure network protocols, attackers can take advantage of their vulnerabilities and obtain sensitive information in the network, such as user credentials, through poisoning attacks, which seriously threatens network security.

Lack of Network Segmentation

Security boundaries missing

In this test environment, the critical server and client are on the same network (internal network segment192.168.2.0/24), lacking effective network segmentation. This means that once the client is attacked, the attacker can easily access the critical server, expanding the scope of the attack.

Impact of attacks expands

Without network segmentation isolation, a security breach in a single system can quickly spread across the entire network, leading to a wider range of security incidents and increasing the risk of data breaches and system damage.

05 Repair and Best Practices

Credential Hardening

Implement a strong password policy

Establish strict password guidelines requiring at least 12 characters, including uppercase letters, lowercase letters, numbers, and special symbols. For example, prohibit passwords containing common words or personal information. Mandate regular password changes (e.g., every 90 days) to minimize the risk of password cracking.

Implement multi-factor authentication

Where possible, implement multi-factor authentication (MFA) using methods such as SMS verification codes, authenticator apps, or hardware tokens. For example, when logging in, users should enter a verification code received via SMS in addition to their password, thereby enhancing account security.

Secure Configurations

Enable SMB signing

Enable SMB signatures on all servers to prevent SMB Relay attacks. Configure SMB signatures as mandatory through server settings or group policies. Refer to the recommendations in Nessus Plugin ID 57608 for promptly addressing vulnerabilities caused by non-mandatory SMB signature activation.

Limit DNS recursion

Limit DNS recursive queries to authorized clients. By modifying the DNS server configuration file, you can precisely specify the IP address range of clients permitted to perform recursive queries. For example, restrict recursive queries to specific departments or devices within the internal network, preventing unauthorized recursive queries from causing information leaks.

Network Hardening

Disable LLMNR/NBT-NS

Block LLMNR/NBT-NS poisoning attacks by disabling these protocols through group policy. In a domain environment, administrators can block LLMNR and NBT-NS services using Group Policy Objects (GPO) to reduce the risk of network attacks.

Implement network segmentation

Implement network segmentation to isolate critical assets. For example, deploy financial servers and core business systems in dedicated subnets with firewall access controls. This approach restricts the spread of attacks, ensuring that compromising one subnet wont compromise others security.

Maintain Secure Baselines

Continue the practice of Ubuntu system hardening

Keep the Ubuntu system with only necessary ports open (e.g., SSH) and enforce key-based authentication. Regularly update system patches to ensure there are no high or medium-level vulnerabilities. Continuously monitor system logs to promptly detect abnormal activities.

Continue Win10 system reinforcement practice

Windows 10 systems should maintain closed unnecessary open ports by implementing effective firewall policies to block all unrequested inbound traffic. Regularly review security settings to ensure no new attack surfaces are created. Continuously optimize security configurations to address evolving threats in the digital landscape.

06 Conclusion

Test Validation Status

Verify the existence of vulnerabilities

In this penetration test, a number of vulnerabilities were successfully verified by various attack methods, such as successful intrusion into Windows Server 2022 using weak passwords, and the vulnerability that DNS server allows recursive query was found by Nessus scan and manual verification, which effectively proved the accuracy of vulnerability assessment.

Assess validity confirmation

The results of the penetration test are highly consistent with the expected results of the vulnerability assessment. For example, in the test of the SMB service, it is found that the SMB signature is not forced to open, which is consistent with the risk indicated by the Nessus plug-in, which fully verifies the effectiveness of the vulnerability assessment.

Attack surface reduction achievements

Ubuntu server performance

Ubuntu 24.04.2 LTS Server only opens the SSH port and forces the use of key-based authentication. Nessus scan did not find high/medium level vulnerabilities, indicating that its attack surface is effectively controlled.

Win10 client effectiveness

The Windows 10 client does not open any ports, and the firewall policy effectively blocks all unrequested inbound traffic. No web-based attack surface is found, fully demonstrating the significant effectiveness of the reduced attack surface.

Root Causes of Critical Vulnerabilities

Weak credentials problem

One of the most serious vulnerabilities in this test was that Windows Server 2022 was cracked by brute force due to the use of weak password "eviluser:Password123!". The attacker obtained remote PowerShell session through CrackMapExec and Evil-WinRM, which shows that weak credentials are an important source of system intrusion.

Service configuration error

The SMB service is not forced to open the signature, and the DNS server allows recursive query and other service configuration errors, which make the system face risks such as SMB relay attack and cache snooping. This indicates that the service configuration error is another important source of the critical vulnerability.

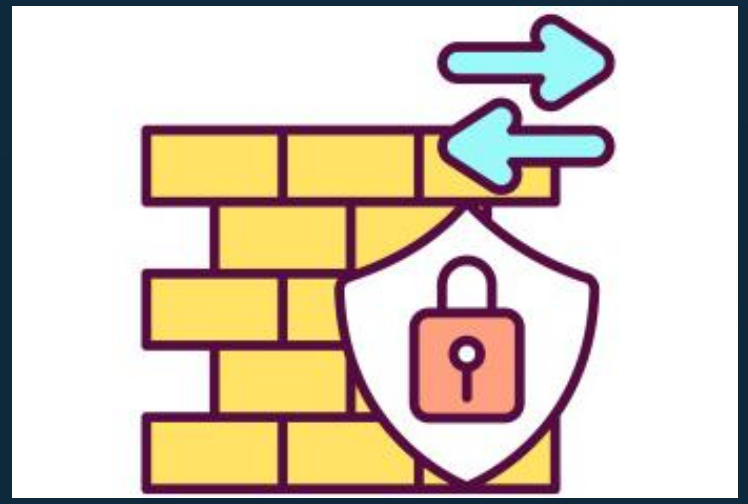
Layered Defense Strategy

Configuration-level defense

By properly configuring services, such as enabling SMB signature and limiting DNS recursive query, the risk of system being attacked can be effectively reduced, which is the basic layer of the layered defense strategy.

Certificate management assurance

Implementing a strong password policy and using multi-factor authentication (MFA) as much as possible can prevent system intrusion caused by weak credentials, which is an important guarantee of the layered defense strategy.



Network isolation is strengthened

By isolating critical assets through network segmentation and disabling insecure network protocols (such as LLMNR/NBT-NS), the risk of network-level attacks can be reduced and the overall defense capability can be enhanced.

THE END

Thanks