vPENTEST

Internal Network Prospecting Test

Evaluation Summary

Demo Customer C

May 29, 2024

app.vpentest.io

Copyright

The methodology used to audit the computer systems is considered proprietary intellectual information of vPenTest Partner and may not be disclosed without written permission from vPenTest Partner. vPenTest Partner gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Confidentiality

This document contains company confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. vPenTest Partner treats the contents of a security audit as company confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Demo Consultant
Title:	Consultant
Office:	(844) 866-2732
Email:	support@vpentest.io

Introduction

This report provides an evaluation of your organization's network security using our pentest methodology. It is not a full penetration test and cannot be used to meet compliance or cyber insurance requirements.

Engagement Scope of Work

Prior to beginning the assessment, vPenTest Partner and Demo Customer C agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Prospecting Test	This assessment attempted to identify security threats that are exposed on the internal network environment. Threats identified within the internal environment are usually less severe than those of the external environment due to the limited exposure. → **Internal Network Penetration Test -** A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase.

Threat Severity Rankings

To assist the organization with prioritizing findings, the findings and observations have been categorized with threat severity rankings based on the following guidelines:

SEVERITY		DESCRIPTION
▂▃▅▆█	Critical	A critical threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, and/or availability of the organization's systems and data. A successful compromise of findings of this ranking leads to access to multiple systems and/or several pieces of sensitive information.
▂▃▅▆█	High	A high threat ranking requires immediate remediation or mitigation. Exploiting these vulnerabilities require a minimal amount of effort by the adversary but poses a significant threat to the confidentiality, integrity, or availability of the organization's systems or data. A successful compromise of findings of this ranking leads to access to a single system or limited sensitive information.
▂▃▅▆█	Medium	A medium threat ranking requires remediation or mitigation within a short and reasonable amount of time. These findings typically lead to a compromise of non-privileged user accounts on systems and/or applications or denote a denial-of-service (DoS) condition of the host, service, or application.
▂▃▅▆█	Low	A low threat ranking requires remediation or mitigation once all higher prioritized findings have been remediated. These findings typically leak information to unauthorized or anonymous users and may lead to more significant attacks when combined with other attack vectors.
▂▃▅▆█	Informational	An informational threat ranking does not pose a significant threat to the environment and may just be findings that could potentially disclose valuable information but do not expose the organization to any technical attacks. Findings rated as informational may be useful for an attacker performing information gathering on the organization to leverage in other attacks, such as social engineering or phishing.

Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
Internal Network Prospecting Test (14)		
IPv6 DNS Spoofing	▮▮▮▮▮	Critical
Link-Local Multicast Name Resolution (LLMNR) Spoofing	▮▮▮▮▮	Critical
Microsoft Windows RCE (BlueKeep)	▮▮▮▮▮	Critical
NetBIOS Name Service (NBNS) Spoofing	▮▮▮▮▮	Critical
Outdated Microsoft Windows Systems	▮▮▮▮▮	Critical
SMBv1 Enabled	▮▮▮▮▯	High
Weak Active Directory Account Password Policy	▮▮▮▮▯	High
Anonymous FTP Enabled	▮▮▮▯▯	Medium
Insecure Protocol - FTP	▮▮▮▯▯	Medium
Insecure Protocol - Telnet	▮▮▮▯▯	Medium
SMB NULL Session Authentication	▮▮▮▯▯	Medium
SMB Signing Not Required	▮▮▮▯▯	Medium
LDAP Permits Anonymous Bind Access	▮▮▯▯▯	Low
Egress Filtering Deficiencies	▮▯▯▯▯	Informational

CRITICAL

IPv6 DNS Spoofing

Observation

IPv6 DNS spoofing is possible due to the possibility of deploying a rogue DHCPv6 server on the internal network. Since Microsoft Windows systems prefer IPv6 over IPv4, IPv6-enabled clients will prefer to obtain IP address configurations from a DHCPv6 server when one is available.

During an attack such as the one performed during this assessment, an IPv6 DNS server was assigned to IPv6-enabled clients; however, the IPv6-enabled clients retained their pre-existing IPv4 address configurations - IP address, default gateway, and subnet mask.

Security Impact

By deploying a rogue DHCPv6 server, an attacker is able to intercept DNS requests by reconfiguring IPv6-enabled clients to use the attacker's system as the DNS server. Such an attack could potentially lead to the successful capture of sensitive information, including user credentials and other information. Resolving all DNS names to an attacker's system results in the victim's system communicating with services such as SMB, HTTP, RDP, MSSQL, etc. all hosted on the attacker's system.

Recommendation

Disable IPv6 unless it is required for business operations. As disabling IPv6 could potentially cause an interruption in network services, it is strongly advised to test this configuration prior to mass deployment. An alternative solution would be to implement DHCPv6 guard on network switches. Essentially, DHCPv6 guard ensures that only an authorized list of DHCP servers are allowed to assign leases to clients.

CRITICAL

Link-Local Multicast Name Resolution (LLMNR) Spoofing

Observation

Link-Local Multicast Name Resolution (LLMNR) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.
2. If the system does not have an entry in its local host's file, the system then sends a DNS query to its configured DNS server(s) to attempt to retrieve an IP address that matches the DNS name in question.
3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an LLMNR broadcast packet on the local network to seek assistance from other systems.

Security Impact

Since the LLMNR queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using computing modern-day computing power and brute-force techniques.

Recommendation

The most effective method for preventing exploitation is to configure the Multicast Name Resolution registry key in order to prevent systems from using LLMNR queries.

- **Using Group Policy:** Computer Configuration\Administrative Templates\Network\DNS Client \Turn off Multicast Name Resolution = Enabled (To administer a Windows 2003 DC, use the Remote Server Administration Tools for Windows 7 - http://www.microsoft.com/en-us/download/details.aspx?id=7887)
- **Using the Registry for Windows Vista/7/10 Home Edition only:** HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient \EnableMulticast

CRITICAL

Microsoft Windows RCE (BlueKeep)

Observation

During testing, systems were identified that are vulnerable to CVE-2019-0708 (BlueKeep), which is a vulnerability that exists in Microsoft Windows systems. This vulnerability is extremely valuable to an attacker due to the availability of tools and code that could take advantage of this weakness. Successful exploitation of this vulnerability typically results in full access to the exploited system(s).

Security Impact

By exploiting the BlueKeep vulnerability, an attacker could gain full control over the affected system. This typically leads to additional attacks within the organization, including extraction of cleartext passwords and hashes, along with lateral movement within the network. Since exploitation of this vulnerability does not require privilege escalation on the affected system, an attacker would typically have as much access as they need on the compromised system to start enumerating the system.

Recommendation

It is recommended to apply security updates on the affected system. Furthermore, the organization should evaluate its patch management program to determine the reason for the lack of security updates. As this vulnerability is a commonly exploited vulnerability and could result in significant access, it should be remediated immediately.

CRITICAL

NetBIOS Name Service (NBNS) Spoofing

Observation

NetBIOS Name Service (NBNS) is a protocol used amongst workstations within an internal network environment to resolve a domain name system (DNS) name when a DNS server does not exist or cannot be helpful.

When a system attempts to resolve a DNS name, the system proceeds with the following steps:

1. The system checks its local host file to determine if an entry exists to match the DNS name in question with an IP address.
2. If the system does not have an entry in its local hosts file, the system then sends a DNS query to its configured DNS server(s) to attempt retrieving an IP address that matches the DNS name in question.
3. If the configured DNS server(s) cannot resolve the DNS name to an IP address, the system then sends an NBNS broadcast packet on the local network to seek assistance from other systems.

Security Impact

Since the NBNS queries are broadcasted across the network, any system can respond to these queries with the IP address of the DNS name in question. This can be abused by malicious attackers since an attacker can respond to all of these queries with the IP address of the attacker's system. Depending on the service that the victim was attempting to communicate with (e.g. SMB, MSSQL, HTTP, etc.), an attacker may be able to capture sensitive cleartext and/or hashed account credentials. Hashed credentials can, many times, be recovered in a matter of time using computing modern-day computing power and brute-force techniques.

Recommendation

The following are some strategies for preventing the use of NBNS in a Windows environment or reducing the impact of NBNS Spoofing attacks:

- Configure the UseDnsOnlyForNameResolutions registry key in order to prevent systems from using NBNS queries (http://technet.microsoft.com/en-us/library/cc775874(v=ws.10).aspx). Set the registry DWORD to 1.
- Disable the NetBIOS service for all Windows hosts in the internal network. This can be done via DHCP options, network adapter settings, or a registry key.

CRITICAL Outdated Microsoft Windows Systems

Observation

An outdated Microsoft Windows system raises several concerns as the system is no longer receiving updates by Microsoft. This could be a prime target for an attacker as these systems typically do not contain the latest security updates, often times leaving them vulnerable to significant threats.

Security Impact

An exploited Microsoft Windows system could potentially result in an attacker gaining unauthorized access to the affected system(s). Additionally, depending on the similarities in configurations between the compromised system(s) and other systems within the network, an attacker may be able to pivot from this system to other systems and resources within the environment.

Recommendation

Replace outdated versions of Microsoft Windows with operating systems that are up-to-date and supported by the manufacturer.

HIGH **SMBv1 Enabled**

Observation

Server Message Block (or SMB) is a communication protocol used in Windows operating systems to communicate with each other over a network. SMB serves an important part in an Active Directory environment as it provides file sharing, printer sharing, and network browsing to machines in the environment. It also allows for processes to communicate with each other using a concept called named pipes, and this is what's known as inter-process communication.

Security Impact

SMBv1 has been depreciated by Microsoft since 2013. Due to this, SMBv1 has become outdated and contains multiple exploits/vulnerabilities that can allow remote control execution on the target machine using this protocol.

Recommendation

To stay protected from exploits that target vulnerabilities in this protocol, it's recommended to disable SMBv1 in favor of SMBv2/v3.

Microsoft has published documentation on their site about disabling SMBv1, as well as upgrading to SMBv2/v3 in just a few commands.

- **Disabling SMBv1:** https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server#how-to-remove-smbv1-via-powershell
- **Enabling SMBv2/v3:** https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server#how-to-remove-smbv1-via-powershell

HIGH

Weak Active Directory Account Password Policy

Observation

An Active Directory Domain Password Policy is extremely critical as it is the security settings that many domain user accounts will use when having their accounts configured. These policies include lockout thresholds, lockout durations, minimum characters required, password complexity requirements, and more. During post-exploitation, it was discovered that the password policy configured does not meet security best practices.

Security Impact

A weak password policy can be disastrous for a company in that it allows attackers to exploit the weaknesses of domain user accounts. For example, the lack of a strict account lockout threshold allows malicious attackers to perform numerous login attempts to domain user accounts prior to being locked out. Here are some of the security impacts that can be associated with domain password policies:

- **Minimum password length:** An attacker can take advantage of this by trying weak passwords that exist in the dictionary, such as Apple, Car, Dog, etc. By increasing the minimum password length, an attacker's chances of successfully guessing and/or even cracking (through password cracking techniques) a password is much lower.
- **Lockout threshold:** If the lockout threshold value is too low, an attacker can perform numerous login attempts to the user accounts before locking out an account, which then depends on the lockout duration for unlocking the domain user account.
- **Lockout duration (minutes):** If the account does not remain locked out for a long period of time, then attackers can continuously perform login attempts every X amount of minutes that the account gets unlocked. A small number increases the chances of a successful attack as the disruption to user accounts will be minimum.
- **Lockout observation window (minutes):** By default, Microsoft Windows sets this to 30. This setting indicates how many times someone can perform a login attempt before it subtracts from the lockout threshold. For example, if this setting is set to 30, then this means an attacker can perform one login attempt per 30 minutes, and the lockout threshold will never exceed the value of 1 because the observation window *resets* the counter every 30 minutes.

Recommendation

Use the references to reconfigure your domain's password policy to adhere to security best practices.

MEDIUM

Anonymous FTP Enabled

Observation

A file transfer protocol (FTP) service allows users to transfer files to/from remote FTP servers. The FTP service typically allows for setting user credentials, which could include complex usernames and passwords. However, during the case of the assessment, testing identified that anonymous FTP was found present. Anonymous FTP servers allow anyone to log in to the FTP server to browse the files that have been remotely uploaded.

Security Impact

The issue with anonymous FTP is that any individual, including an attacker, could gain remote access to the FTP server and observe the contents within the server. Depending on anonymous permissions, an attacker may also be able to leverage this default, weak configuration in order to store/transmit malicious code.

The exposure of files stored on anonymous FTP servers could present the opportunity for an attacker to compromise the confidentiality and/or integrity of sensitive files that may be deemed for authorized access only.

Recommendation

If the anonymous FTP server is not required for business operations, consider disabling the service altogether and updating the organization's configuration baseline. The configuration baseline should ensure that unnecessary services are disabled prior to deployment. If the service is required for business operations, consider disabling anonymous authentication and implementing authentication that leverages a complex password.

MEDIUM

Insecure Protocol - FTP

Observation

The File Transfer Protocol (FTP) service is used for client systems to connect to and store and retrieve files. However, FTP does not encrypt the communications between the server and the client, exposing all data in cleartext. Although FTP can negotiate to use TLS, the affected server(s) were not found to negotiate TLS.

Security Impact

Since FTP is cleartext, all of the traffic between the client and the server is exposed in cleartext. This presents the opportunity for an attacker to perform a man-in-the-middle attack and obtain sensitive user credentials as well as file contents. Such valuable information may also be useful for other attacks within the environment.

Recommendation

Disable the service if it is not needed for business operations. If transferring files is necessary for business operations, then consider implementing Secure FTP (SFTP) as SFTP uses encryption during communications to/from SFTP clients.

MEDIUM

Insecure Protocol - Telnet

Observation

The telnet service is used for network administrators to perform remote administration of network devices. This service, however, does not enforce encryption and, therefore, exposes all traffic in cleartext.

Security Impact

Since telnet communications are in cleartext, an attacker could perform a man-in-the-middle attack and obtain sensitive information such as user credentials, command outputs, and more. Such valuable information may also be useful for other attacks within the environment.

Recommendation

Disable the telnet service if it is not required for business operations. If it is required for business operations, consider using an alternative protocol, such as Secure Shell (SSH), to accomplish the same goal with encryption being implemented.

MEDIUM

SMB NULL Session Authentication

Observation

A Server Message Block protocol (SMB) service allows SMB NULL Session Authentication (i.e. without a username or password). SMB NULL sessions allow anyone to log in to SMB shares to browse the files that have been remotely uploaded.

Security Impact

The issue with SMB NULL sessions is that any individual, including an attacker, could gain remote access to the SMB share and observe the contents. If the NULL session also provides write access, an attacker may also be able to leverage this insecure configuration in order to store/transmit malicious code.

The exposure of files stored on affected SMB shares could present the opportunity for an attacker to compromise the confidentiality and/or integrity of sensitive files that may be deemed for authorized access only.

Recommendation

If the SMB server is not required for business operations, consider disabling the service altogether and updating the organization's configuration baseline. The configuration baseline should ensure that unnecessary services are disabled prior to deployment. If the service is required for business operations, consider disabling SMB NULL session authentication and implementing authentication that leverages a complex password.

MEDIUM | SMB Signing Not Required

Observation

Testing identified Microsoft Windows configuration concerns that could potentially result in an increased risk of an attack against Microsoft operating systems within the targeted environment. By default, Microsoft Windows comes pre-installed with several configuration issues that require network administrators to explicitly disable or enable to enhance security. If these options are not modified, then these systems could remain vulnerable to several attacks.

More specifically, the SMB signing feature was not found to be required at the time of testing. SMB signing is a security feature implemented by Microsoft to combat SMB relay attacks. An SMB relay attack occurs when an attacker tricks the victim system into authenticating to the attacker, and the attacker relays those credentials to another system.

Security Impact

Since many organizations use Microsoft Windows and Active Directory environments to manage users, a successful attack against a Microsoft Windows system could potentially expose the organization to other attacks, including privilege escalation and lateral movement. Furthermore, many Microsoft Windows systems share similar configurations due to Group Policy's ability to configure settings on a global scale. A single misconfiguration within Group Policy could present significant threats.

As it relates to SMB signing, a successful SMB relay attack could provide an attacker with access to a system of the attacker's choosing, depending on the permission levels of the authentication credentials being relayed. This could result in remote command execution, access to resources, and more.

Recommendation

Enforce SMB signing by configuring this across the organization's systems via Group Policy.

LOW

LDAP Permits Anonymous Bind Access

Observation

Lightweight Directory Access Protocol (LDAP) can be used by multiple services when it comes to authenticating users to Active Directory. However, information may also be enumerated from this service in order to provide functionality for certain devices, such as filling in hostnames, domain name information, and more.

Security Impact

A misconfigured LDAP server could unnecessarily expose information to unauthorized individuals, including domain information. Although LDAP is typically exposed only internally, limiting the amount of information that an attacker could get further reduces the risk of a successful attack, even if by a little. LDAP servers may also be useful for enumerating Active Directory Domain User Accounts in certain scenarios, which could be extremely valuable to an attacker that needs such information for performing password attacks against those users.

Recommendation

To disable anonymous bind, add the following line to the "slapd.conf" file:

```
disallow bind_anon
```

Depending on which server operating system your LDAP server is running on, you may also be able to leverage the ASDIEdit tool to add the "DenyUnauthenticatedBind" entry into the configuration. See the reference section for more specific details.

INFORMATIONAL | Egress Filtering Deficiencies

Observation

An egress filtering check was performed as part of the internal network penetration test. This check aims to determine if the internal environment allows excessive access to the public Internet, which could increase the risk of data exfiltration. This check was not performed against a specific in-scope target, but on the public Internet in general to evaluate this risk.

During this check, it was possible to identify access to an excessive number of ports residing on the public Internet. This particular check targeted scanme.nmap.org, which is designed for organizations to check whether or not they have access to servers on the public Internet.

Security Impact

Allowing end-users access to excessive services, such as SSH, Telnet, etc. allows for an attacker or end-user to bypass security controls by exfiltrating information through other communication channels. During an attack, an attacker may also leverage this excessive access to establish a command-and-control (C2) server to communicate commands and data back and forth between a compromised system.

Recommendation

Disable access to services that are not required for business operations. Restricting access to only services that are required for business operations allows the organizations to establish more control over communication channels, allowing for inspection of indicators of compromise (IoC) as well as malicious data exfiltration attempts.