External Network Prospecting Test

Evaluation Summary

Demo Customer C

May 31, 2024

app.vpentest.io

vPENTEST

Copyright

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:	Vonahi Security
Title:	Security Consultant
Office:	
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, ThreatAdvice 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
External Network Penetration Test	This assessment includes performing a security assessment from the perspective of a malicious attacker from public Internet environments. Threats exposed to users on the public Internet are higher severity than those of the internal environment due to the increased exposure. → **Reputational Threat Exposures** - Using information available on the public Internet (e.g. search engines, social media, etc.), vPenTest Partner attempted to discover information that could potentially harm Demo Customer C's reputation. This includes publicly disclosed information that may or may not be useful for an attack. → **External 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. Information obtained from within the Reputational Threats Exposure phase were used as part of this penetration test.

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	
External Network Prospecting Test (15)		
Outdated Microsoft Windows Systems		Critical
Microsoft SQL Servers Exposed to Public Internet		High
SMB NULL Session Authentication		High
SMB Service Exposed to Public Internet		High
SMBv1 Enabled		High
Subdomain Takeover Vulnerability		High
Application Login Interface Exposed to Public Internet		Medium
FortiGate Login Interface Exposed to Public Internet		Medium
Insecure Protocol - FTP		Medium
Misconfigured DMARC Record		Medium
Missing DMARC Record		Medium
Missing SPF Record (Email Spoofing Possible)		Medium
Remote SSH Service Exposed to Public Internet		Medium
SMB Signing Not Required		Medium
Application Discloses Default Web Page		Informational

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

Microsoft SQL Servers Exposed to Public Internet

Observation

Microsoft SQL (MSSQL) servers were found to be exposed to the public Internet. Since MSSQL is a database and typically contains valuable information for the organization, this service should only be exposed to trusted users, such as internal users or users who are connected to a Virtual Private Network (VPN).

Security Impact

Exposing MSSQL to the public Internet could present a serious threat to the organization, as this allows attackers to perform password-based attacks against the service. If an attacker is successful with guessing a valid set of credentials, they may be able to login to the database and perform enumeration, which could expose sensitive data stored within the database. Other attacks, including those leveraging zero-day exploits, could also result in privilege escalation, whereby an attacker would be able to execute system commands and pivot onto other systems within the internal network environment.

Recommendation

Disable MSSQL on the public Internet in favor of a Virtual Private Network (VPN) solution that requires two-factor authentication (2FA). Do not allow users to directly authenticate to the MSSQL service from the public Internet as this may allow for attackers to not only perform password guessing attempts, but also launch attacks that could result in full control.

If the MSSQL service is absolutely required for business operations, then it is recommended to restrict access to specific IP addresses â€“ a whitelist configuration should be necessary.

HIGH

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 for anyone to login 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.

HIGH

SMB Service Exposed to Public Internet

Observation

The Server Message Block (SMB) running on port 445/tcp is a protocol used on systems to share services such as file and print sharing. Additionally, it is possible to perform authentication over SMB prior to accessing a particular resource on the system. This service should only be exposed to the internal network environment or to a trusted network due to the possibility of exploiting weaknesses.

Security Impact

Since the SMB service is exposed to the public Internet, it is possible for an attacker to perform an authentication attack against either the local system itself or Active Directory if the system is connected to a domain. Additionally, it is a relatively common pattern for security vulnerabilities to become publicly disclosed that affect the SMB service, which usually provides full access to the system when compromised.

One perfect example of this is the popular EternalBlue vulnerability. When this vulnerability is successfully exploited, it's possible for an attacker to gain full control over the system and its resources, allowing them to interact with the system as an administrator. Such access could allow an attacker to attempt privilege escalation attacks, which may provide the attacker with more access to the network and its resources.

Recommendation

Restrict access from the public Internet to port 445/tcp (SMB). Only allow users within the internal network environment with access to this port (if necessary for business operations). Furthermore, if users on the public Internet require access to this port, consider implementing a Virtual Private Network (VPN) which requires the user to authenticate using username, password, and multi-factor authentication.

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

Subdomain Takeover Vulnerability

Observation

During security testing, a potential subdomain takeover vulnerability was identified on one or more domains that belong to the organization. This issue arises from misconfigured DNS records and could lead to potential security risks.

Security Impact

If exploited by an attacker, this subdomain takeover vulnerability could result in unauthorized control of the affected subdomain. This, in turn, could lead to the impersonation of the legitimate website or the delivery of malicious content, potentially damaging the organization's reputation and putting users at risk.

Recommendation

To address this subdomain takeover vulnerability and enhance the security of the organization's infrastructure, the following remediation steps are recommended:

Remediation Steps

1. **Remove Misconfigured DNS Records:** Immediately remove any misconfigured DNS records that are susceptible to takeover. Specifically, focus on subdomains pointing to unregistered or unauthorized services.
2. **Review DNS Configuration:** Conduct a comprehensive review of the DNS configurations to identify and rectify any misconfigurations or discrepancies. Ensure that all DNS records accurately reflect the intended services and are properly secured.
3. **Regularly Monitor DNS Records:** Establish a proactive monitoring process to regularly review DNS records for any unauthorized changes or vulnerabilities. Implement real-time alerting to detect and respond to suspicious activities promptly.
4. **Implement DNS Security Best Practices:** Follow industry best practices for DNS security, such as implementing DNSSEC (DNS Security Extensions) to protect against DNS spoofing attacks and DNS filtering to block malicious domains.

MEDIUM

Application Login Interface Exposed to Public Internet

Observation

During testing, it was possible to identify and access the login page for web application. The login page allows anyone on the public Internet to attempt authenticating to the back-end application.

Security Impact

By exposing the login page to anonymous users on the public Internet, this could present opportunities for malicious attackers to perform authentication attempts against the application. Depending on if whether or not an attacker can compromise credentials, and depending on the security permissions of the compromised user account, this could result in full control over the underlying server.

Recommendation

Disable access from the public Internet. There are a few alternative methods to administering the web application:

Restrict traffic from a specific IP address - This would prevent anonymous users from being able to access the application unless they are accessing the application from a source IP address that is permitted by the server.

MEDIUM

FortiGate Login Interface Exposed to Public Internet

Observation

FortiGate web instances were discovered that allow access to the login page from the public Internet. This allows anyone on the public Internet to try and authenticate to the back-end application.

Security Impact

The exposure of the FortiGate login page to anonymous users on the public Internet, presents opportunities for malicious actors to perform authentication attempts against the application. If an attacker manages to gain access by compromising credentials, they could perform additional attacks against the application and/or the underlying server. Depending on the security permissions of the compromised user account, this could eventually result in full control over the underlying server.

Recommendation

Disable access from the public Internet. In general, it is recommended to follow the system administrator best practices outlined in the official FortiGate documentation: https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/582009/system-administrator-best-practices

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

Misconfigured DMARC Record

Observation

During testing, it was observed that the organization has a misconfigured DMARC (Domain-based Message Authentication, Reporting, and Conformance) record for its domain(s). DMARC is an essential email authentication protocol that helps protect against email spoofing and phishing attacks. A properly configured DMARC record enables organizations to specify how email messages from their domain should be authenticated and handled by receiving mail servers.

Security Impact

A misconfigured DMARC record can have significant security implications for the organization. When the DMARC policy is set to "none" or lacks a clear definition, it leaves the organization vulnerable to email-based attacks. Malicious actors can exploit this by sending fraudulent emails that appear to come from the organization's domain, increasing the risk of successful phishing attacks, data breaches, financial losses, and damage to the organization's reputation.

Recommendation

It is crucial for the organization to review and correct its DMARC record configuration promptly. A well-configured DMARC record should include a defined policy, which can be "quarantine" or "reject" to instruct receiving mail servers on how to handle unauthenticated emails from the organization's domain. By configuring DMARC correctly, the organization can significantly enhance its email security posture, reduce the risk of successful phishing attacks, and better protect sensitive information. Furthermore, a properly configured DMARC record enables the organization to receive reports on email authentication failures, allowing for effective monitoring and response to potential threats.

MEDIUM

Missing DMARC Record

Observation

During testing, it was observed that the organization has missing DMARC (Domain-based Message Authentication, Reporting, and Conformance) records. DMARC is an essential email authentication protocol that helps protect against email spoofing and phishing attacks. It enables organizations to specify how email messages from their domain should be authenticated and handled by receiving mail servers.

Security Impact

The absence of DMARC records increases the risk of email-based phishing attacks on the organization. Without DMARC, malicious actors can more easily impersonate the organization's domain in phishing attempts, leading to potential data breaches, financial losses, and damage to the organization's reputation. Additionally, the lack of DMARC records hinders the organization's ability to receive reports on email authentication failures, making it difficult to monitor and respond to potential threats effectively.

Recommendation

It is strongly recommended that the organization immediately implement DMARC records for the primary domain(s). This involves defining policies for how an email from their domain should be authenticated and specifying actions to take when unauthorized emails are detected. By implementing DMARC, the organization can significantly enhance its email security posture, reduce the risk of phishing attacks, and gain valuable insights into email authentication issues through reporting. This proactive step will help safeguard sensitive information and protect the organization's reputation.

MEDIUM

Missing SPF Record (Email Spoofing Possible)

Observation

Email spoofing is a type of cyber-attack in which an attacker sends emails that appear to be from a legitimate source, such as a company or individual. This is done by forging the sender's address, which is possible if the recipient's domain does not have an SPF (Sender Policy Framework) record. An SPF record is a type of Domain Name System (DNS) record that identifies which mail servers are authorized to send email on behalf of a domain. Without an SPF record, it is much easier for attackers to spoof emails from a domain, as the recipient's mail server will not be able to verify the sender's identity.

Security Impact

If a domain does not have an SPF record, it is much easier for an attacker to spoof emails from that domain. This can lead to a variety of problems, including phishing attacks, malware infections, and financial fraud. It can also damage the reputation of the domain, as recipients may not trust emails from that domain in the future.

Recommendation

The following actions are recommended to mitigate this vulnerability successfully:

1. Create an SPF TXT record in your domain's DNS (Domain Name System) zone file. This record should include the authorized IP addresses or hostnames as specified in the SPF policy.
2. Test the SPF record to ensure it is properly configured and functioning as intended. Online SPF validation tools can be used to verify the correctness of your record.
3. Monitor and maintain the SPF record regularly. Update it whenever there are changes to the email infrastructure or authorized sending sources.

Implementing an SPF record will significantly reduce the risk of email spoofing, protect the domain reputation, and increase the chances of legitimate emails reaching the intended recipients' inboxes.

MEDIUM

Remote SSH Service Exposed to Public Internet

Observation

Remote administration protocols are typically used for network administrators to manage devices such as switches, routers, and even other critical systems. Exposing these services to the public Internet could expose the organization to unnecessary attack vectors.

Security Impact

Exposing this service to the public Internet presents the opportunity for an attacker to perform password-based attacks against the remote administration services. Additionally, as security researchers continuously publish research of zero-day exploits, an attacker with access to one of these could eventually gain direct access to the underlying system. This could lead to other compromises as well, such as sensitive data exposure or interception of traffic, depending on the device exposing the service.

Recommendation

The affected remote administration protocol(s) should be restricted altogether from the public Internet to minimize the attack surface. Remote administration protocols should always be restricted from the public Internet and only accessible via a trusted environment such as a Virtual Private Network (VPN) or explicit IP address configuration.

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.

INFORMATIONAL Application Discloses Default Web Page

Observation

During testing, it was possible to identify web applications that exposed default pages. Typically, when installing an application, such as Apache, Tomcat, or IIS, a default web page is stored and made public. This page could prove to be valuable to an attacker as it gives them information about the underlying application and/or operating system. For example, only certain versions of Microsoft Windows will run a particular version of IIS.

Security Impact

By exposing default web application pages, this could provide an attacker with valuable information needed to perform attacks against the web server. Although this is not a critical issue, exposing less information to an attacker ultimately helps reduce the external environment's overall attack surface

Recommendation

Disable all default pages on the web application if they are not required for business operations. Additionally, redirect the user to a standard page upon browsing to any directories that don't exist to prevent disclosing information about the underlying web application.