



True Network PenTest

TECHNICAL REPORT

Demo Client 3

June 15, 2024

whiterookcyber.com.au

Copyright

© White Rook Cyber. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of White Rook Cyber and may not be disclosed without written permission from White Rook Cyber. White Rook Cyber gives permission to copy this report for the purpose of disseminating information within your organizationhite Rook Cyber, 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. White Rook Cyber 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:	1300 794 777
Email:	contact@whiterookcyber.com.au

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 access 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 Penetration Test (4)		
MySQL Servers Exposed to Public Internet		High
PostgreSQL Servers Exposed to Public Internet		High
Insecure Protocol - FTP		Medium
Insecure Protocol - POP3		Medium

MITRE ATT&CK Mappings

This section of the report contains details about the tactics, techniques, and procedures as defined by the MITRE ATT&CK Framework. For additional details relating to these tactics, techniques, and procedures (TTPs), White Rook Cyber recommends that Demo 3 visit the specific URLs provided within the table below. Furthermore, White Rook Cyber has also elaborated on how these TTPs were used during the penetration test in this report's Penetration Test Narrative section.

White Rook Cyber recommends Demo 3 thoroughly leverage this report section to investigate and improve network security policies, procedures, and controls within the organization's environment. All of the attacks mentioned in this report section should have been detected and properly logged for investigation purposes by the organization.

MITRE ATT&CK			
Time	Name	Tactic	TTPID
Thu, Jun 15, 2023 @ 07:50:19 PM EDT	Active Scanning: Scanning IP Blocks	Reconnaissance	T1595.001
Thu, Jun 15, 2023 @ 07:50:19 PM EDT	Network Service Discovery	Discovery	T1046
Thu, Jun 15, 2023 @ 07:50:37 PM EDT	Active Scanning: Scanning IP Blocks	Reconnaissance	T1595.001
Thu, Jun 15, 2023 @ 07:50:37 PM EDT	Network Service Discovery	Discovery	T1046
Thu, Jun 15, 2023 @ 07:58:08 PM EDT	Active Scanning: Scanning IP Blocks	Reconnaissance	T1595.001
Thu, Jun 15, 2023 @ 07:58:09 PM EDT	Network Service Discovery	Discovery	T1046
Thu, Jun 15, 2023 @ 08:07:21 PM EDT	Network Service Discovery	Discovery	T1046
Thu, Jun 15, 2023 @ 08:07:22 PM EDT	Network Service Discovery	Discovery	T1046
Thu, Jun 15, 2023 @ 08:11:12 PM EDT	Brute Force: Password Guessing	Credential-access	T1110.001
Thu, Jun 15, 2023 @ 08:11:23 PM EDT	Brute Force: Password Guessing	Credential-access	T1110.001

Reputational Threat Findings

This section addresses information that was discovered when performing information gathering about the organization. This information include data that could be leveraged by an adversary to perform an attack, including social engineering attacks. Findings in this area focus on identifying vulnerabilities that could be used to affect the reputation, brand image, or users of the organization's various external presences.

The threat severity ranking of each finding is based on the recommended priority and order of importance as outlined in this section.

Tasks Performed

To fully assess the organization for reputational threats, White Rook Cyber performed the following tasks as part of this phase of testing:

TASK PERFORMED	DOMAIN(S) ASSESSED
Performed Information Gathering: Whois, NSLookup, and ARIN Queries	www.demo3.com
Performed DNS Enumeration for Hostnames	www.demo3.com
Performed Username and Email Address Harvesting	www.demo3.com
Performed Doppelganger Domain Searches	www.demo3.com
Performed Derogatory Domain Searches	www.demo3.com



Observation

One of the first things that an attacker does to gather information about an organization is perform lookups of their domain names, identify subdomains, mail servers, etc. The objective of this process is to gather as much information about the target domain so that an attacker could begin to map out the external environment of the organization. Such information could then later be used in an attack, such as social engineering.

White Rook Cyber also reviewed DNS records to determine if any email spam controls are in place. This is accomplished by the use of DMARC and SPF records. Once implemented, email servers that receive emails from your domain will double check your domain's DNS records to determine if the originating email is from an authorized source. If not, the email may be completely dropped or moved to the spam folder.



Recommendation

According to public DNS records publicly available, White Rook Cyber was unable to identify any SPF records that belong to your domain. This means that an attacker may be able to send out malicious emails spoofing your domain and destination mail servers will not treat it as spam.

Learn more about how to implement an SPF record for your domain at the following URL:

<https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability>

According to public DNS records publicly available, White Rook Cyber was unable to identify any DMARC records that belong to your domain. This means that an attacker may be able to send out malicious emails spoofing your domain and destination mail servers will not treat it as spam.

Learn more about how to implement a DMARC record for your domain at the following URL:

<https://support.google.com/a/answer/2466563?hl=en>



Evidence

No additional domains were discovered as part of this domain information gathering process.



Observation

A Doppelganger domain is a domain that has been registered by an adversary that takes advantage of common typing mistakes or browser assumptions that target a legitimate domain. As an example, a common doppelganger domain for "www.abc.com" would be to register "wwwabc.com" or even "www.abccom.com".

Doppelganger domains have a potent impact when leveraged via email or bogus websites, as adversaries could potentially gather information such as trade secrets, usernames and passwords, and other employee information during social engineering attacks. Additionally, doppelganger domains have been commonly used to spread malware to users who accidentally misspell a legitimate domain in their web browser.

During testing against targeted domains, seventy (70) doppelganger domains were discovered to be registered. Demo 3's network staff should review these results and determine the legitimacy of these domains.



Recommendation

By leveraging tools such as [URLCrazy](#), your organization may perform its own periodic review of its domains to determine if anyone has attempted to register a doppelganger domain. If a doppelganger domain is discovered, gather the registrar information, and lodge a complaint with the registrar to have the doppelganger domain removed or registered to your organization.

Additionally, it is recommended that your organization register the most common variations of its domain names and spellings as a preemptive measure to combat this form of attack.

Furthermore, the organization may consider implementing a blacklist in its mail server configuration to ensure that these doppelganger domains are not used to send phishing emails to the organization.



Evidence

MISSPELLING TECHNIQUE	DOMAIN NAME	IP ADDRESS ASSOCIATED WITH DOMAIN	COUNTRY
Original	www.demo3.com	64.190.63.111	UNITED STATES
Character Omission	ww.demo3.com	64.190.63.111	UNITED STATES
Character Omission	www.dem3.com	206.188.192.67	UNITED STATES
Character Omission	www.deo3.com	52.58.78.16	UNITED STATES
Character Omission	www.dmo3.com	3.64.163.50	UNITED STATES
Character Repeat	wwwwww.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	eww.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	qww.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	wew.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	wqw.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	wwe.demo3.com	64.190.63.111	UNITED STATES
Character Replacement	wwq.demo3.com	64.190.63.111	UNITED STATES

Character Replacement	www.demo2.com	63.143.33.122	UNITED STATES
Character Replacement	www.demo4.com	13.248.169.48	UNITED STATES
Character Replacement	www.semo3.com	156.244.131.248	SEYCHELLES
Double Replacement	eew.demo3.com	64.190.63.111	UNITED STATES
Double Replacement	qqw.demo3.com	64.190.63.111	UNITED STATES
Double Replacement	wee.demo3.com	64.190.63.111	UNITED STATES
Double Replacement	wqq.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	weww.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	wqww.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	wwew.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	wwqw.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	wwwwe.demo3.com	64.190.63.111	UNITED STATES
Character Insertion	wwwq.demo3.com	64.190.63.111	UNITED STATES
Missing Dot	wwwwww.demo3.com	64.190.63.111	UNITED STATES
Insert Dash	w-ww.demo3.com	64.190.63.111	UNITED STATES
Insert Dash	ww-w.demo3.com	64.190.63.111	UNITED STATES
Insert Dash	www-.demo3.com	64.190.63.111	UNITED STATES
Singular or Pluralise	demo3.com	64.190.63.111	UNITED STATES
Vowel Swap	www.damo3.com	156.235.213.25	SEYCHELLES
Vowel Swap	www.domo3.com	3.64.163.50	UNITED STATES
Bit Flipping	7ww.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	gww.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	sww.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	uww.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	vww.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	w7w.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wgw.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wsw.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wuw.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	www.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	ww7.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wwg.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wws.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wwwu.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	wwwv.demo3.com	64.190.63.111	UNITED STATES
Bit Flipping	www.demo1.com	64.190.63.111	UNITED STATES
Bit Flipping	www.demo7.com	199.59.243.223	UNITED STATES
Bit Flipping	www.demos.com	34.206.39.153	UNITED STATES
Homoglyphs	vwwwv.demo3.com	64.190.63.111	UNITED STATES
Homoglyphs	vwww.demo3.com	64.190.63.111	UNITED STATES
Homoglyphs	vwwwv.demo3.com	64.190.63.111	UNITED STATES
Homoglyphs	vwww.demo3.com	64.190.63.111	UNITED STATES
Homoglyphs	wwwv.demo3.com	64.190.63.111	UNITED STATES

Homoglyphs	www.demo3.com	64.190.63.111	UNITED STATES
Homoglyphs	www.demo3.com	64.190.63.111	UNITED STATES
Wrong TLD	demo3.asia	112.213.88.136	VIET NAM
Wrong TLD	demo3.at	85.13.144.100	GERMANY
Wrong TLD	demo3.click	46.101.125.248	NETHERLANDS
Wrong TLD	demo3.cpa	44.198.11.225	UNITED STATES
Wrong TLD	demo3.dk	94.231.106.113	DENMARK
Wrong TLD	demo3.fr	46.30.211.38	DENMARK
Wrong TLD	demo3.gq	103.90.235.138	VIET NAM
Wrong TLD	demo3.io	34.74.37.249	UNITED STATES
Wrong TLD	demo3.net	38.238.107.39	UNITED STATES
Wrong TLD	demo3.org	198.50.252.65	CANADA
Wrong TLD	demo3.se	185.76.65.46	SWEDEN
Wrong TLD	demo3.site	118.27.125.218	JAPAN
All SLD	demo3.co.za	41.203.0.50	SOUTH AFRICA
All SLD	demo3.com.tr	176.235.83.115	TURKEY

True Network PenTest

Engagement Scope of Work

Through discussions with Demo 3's staff, the following target applications, IP addresses, and/or ranges were included as part of the engagement scope.

IP ADDRESSES & RANGES

sample1.com			
-------------	--	--	--

Agent Information

To perform this assessment, White Rook Cyber used an agent consisting of the necessary tools to conduct discovery, enumeration, attacks, etc. The agent used in this assessment contained the following information:

DESCRIPTION

DETAILS

Agent Name	White Rook Cyber External Agent
Public IP Address	3.141.152.255

Task Performed

To assess the targets listed above fully, White Rook Cyber performed the following tasks:

TASK PERFORMED

DEVICES/LOCATIONS ASSESSED

Performed information gathering: NSlookup, and Ping/SNMP sweeping	All targets
Performed port scans	All active targets identified
Performed vulnerability scanning	All active targets identified
Performed web application vulnerability testing	Active/Select targets
Performed vulnerability validation	All active targets identified
Performed penetration testing	Active/Select targets

Rules of Engagement

White Rook Cyber and Demo 3 agreed to the following rules of engagements:

ACTIVITY

DEFINITION

PERMISSION

Exploitation	White Rook Cyber consultants will cautiously execute exploitation techniques to gain access to sensitive data and/or systems.	Permitted
Post Exploitation	If exploitation is successful, White Rook Cyber will attempt to escalate privileges within the environment to gain further access to systems and/or data.	Permitted

Penetration Test Narrative

This phase of the external network penetration test describes some of the action performed as part of the penetration test, including host discovery, enumeration, exploitation, and post-exploitation (if opportunities were identified). It should be noted that this portion of the report does not represent the entire list of activities that were performed as part of this assessment, primarily just those that led to some level of access, significant exposure to information, and other activities relevant to the goal of the assessment.

Host Discovery

The first process that was performed during the penetration test was host discovery. Host discovery includes several tasks, including port scanning and ping sweeps, to identify the active systems within the environment. This is a crucial step in the penetration test as it allows attackers to determine what systems are active within the targeted IP addresses and/or ranges.

Of the one (1) IP address/range that was provided as part of the scope, White Rook Cyber was able to identify a total of one (1) system to be active within the targeted environment.

MITRE ATT&CK®	
Name	Active Scanning: Scanning IP Blocks
Tactic	Reconnaissance
TTP ID	T1595.001
Note	White Rook Cyber also performed a port scan against one (1) target to identify opened ports and running services. Port scanning is also important in that it allows one to identify which ports are opened and visible from the tested system. By discovering opened ports within the environment, it is then possible to determine which services are running and if any of the running services are vulnerable.

Of the one (1) address/range that was scanned, White Rook Cyber found thirteen (13) ports opened.

Enumeration

After identifying the available hosts within the network, the next phase is to conduct enumeration. Enumeration consists of scanning the identified ports to determine what services are running. Additional scans are performed based on the running services to attempt enumerating information from the running services (if possible). Such information may be useful for identifying additional vulnerabilities or knowledge for performing an attack against the service.

To help understand the operating systems and ports that were found to be most common within the environment, the following tables display the top 10 operating systems and top 10 ports.

PORT/PROTOCOL	COUNT
5432/tcp	1
3306/tcp	1
2525/tcp	1
995/tcp	1
993/tcp	1
587/tcp	1
465/tcp	1
443/tcp	1
143/tcp	1

110/tcp	1
---------	---

White Rook Cyber identified one (1) PostgreSQL service present within the tested environment. While this discovery does not indicate any significant issues were found, PostgreSQL services are often targeted by attackers in a form of a password attack. A successful password attack will usually result in limited or elevated privileges to the SQL service, at which point an attacker can begin to run SQL commands or execute system level commands.

MITRE | ATT&CK®

Name	Network Service Discovery
Tactic	Discovery
TTP ID	T1046
Note	White Rook Cyber performed an enumeration to identify information about the PostgreSQL services found during the discovery phase.

The following information was enumerated from the PostgreSQL service(s) found during this assessment:

```
[*] 35.212.46.254:5432 Postgres - Version Unknown (Pre-Auth)
```

White Rook Cyber identified one (1) MySQL service present within the tested environment. While this discovery does not indicate any significant issues were found, MySQL services are often targeted by attackers in a form of a password attack. A successful password attack will usually result in limited or elevated privileges to the SQL service, at which point an attacker can begin to run SQL commands or execute system level commands.

MITRE | ATT&CK®

Name	Network Service Discovery
Tactic	Discovery
TTP ID	T1046
Note	White Rook Cyber performed an enumeration to identify information about the MySQL services found during the discovery phase.

The following information was enumerated from the MySQL service(s) found during this assessment:

```
[+] 35.212.46.254:3306 - 35.212.46.254:3306 is running MySQL 5.7.39-42-log (protocol 10)
```

Testing was performed against FTP services that contained port 21/tcp opened. This scan attempted to identify FTP services that accepted anonymous login credentials. Anonymous login credentials would allow an attacker to identify files that may exist on an FTP server. If permissions allow for write access, an attacker could also attempt to use this to store malicious code. The one (1) system that was found to contain port 21/tcp opened, did not accept or permit anonymous FTP logins.

Targeting one (1) web application identified running on port 443/tcp, White Rook Cyber performed a hidden directory brute force scan to determine if any directories could be identified that may contain sensitive information. During this process, an attacker would usually provide a wordlist containing common names, such as "administrator", "admin", "login", and more. Depending on whether or not one of the web services has a directory containing these common names, the attacker would then attempt to log in or enumerate additional information that may aid other attacks.

After completing the directory enumeration scan on port 443, White Rook Cyber was unable to identify any directories that contain information that may be valuable to an attacker.

Targeting one (1) web application identified running on port 80/tcp, White Rook Cyber performed a hidden directory brute force scan to determine if any directories could be identified that may contain sensitive information. During this process, an attacker would usually provide a wordlist containing common names, such as "administrator", "admin", "login", and more. Depending on

whether or not one of the web services has a directory containing these common names, the attacker would then attempt to log in or enumerate additional information that may aid other attacks.

After completing the directory enumeration scan on port 80, White Rook Cyber was unable to identify any directories that contain information that may be valuable to an attacker.

MITRE | ATT&CK®


Name	Brute Force: Password Guessing
Tactic	Credential-access
TTP ID	T1110.001
Note	White Rook Cyber also reviewed a list of one (1) MySQL server and conducted a limited password attack to determine if any weak or default credentials could be discovered.

Weak credentials configured for a MySQL server could result in significant issues, including remote command execution. No servers were found to contain weak or default credentials at the time of testing. The following code snippet shows sample output results of this scan:

```
[+] 35.212.46.254:3306 - 35.212.46.254:3306 - Found remote MySQL version 5.7.39
[-] 35.212.46.254:3306 - 35.212.46.254:3306 - LOGIN FAILED: root:password (Incorrect: Access denied for user 'root'@'ec2-3-18-225-214.us-east-2.compute.amazonaws.com' (using password: YES))
[-] 35.212.46.254:3306 - 35.212.46.254:3306 - LOGIN FAILED: root:root (Incorrect: Access denied for user 'root'@'ec2-3-18-225-214.us-east-2.compute.amazonaws.com' (using password: YES))
[-] 35.212.46.254:3306 - 35.212.46.254:3306 - LOGIN FAILED: root: (Incorrect: Access denied for user 'root'@'ec2-3-18-25-214.us-east-2.compute.amazonaws.com' (using password: NO))
```

External Network Environment Exposures

This phase of the security assessment focused on the security of network assets within the external network environment. During this phase, White Rook Cyber used a comprehensive set of tools, custom scripts, and manual techniques to thoroughly identify possible threats to the environment. Like a traditional penetration test, all identified threats were tested and validated to evaluate the depth of compromise. Unlike a traditional penetration test, this evaluation of threats was not isolated or limited to a handful of threats, but rather across all threats identified.

HIGH

MySQL Servers Exposed to Public Internet



Observation

MySQL servers were found to be exposed to the public Internet. Since MySQL 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 MySQL 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.



Top Affected Nodes

ONE (1) NODE AFFECTED		
IP Address	Host Name	Operating System
35.212.46.254		Undetected



Recommendation

Disable MySQL 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 MySQL 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 MySQL service is absolutely required for business operations, then it is recommended to restrict access to specific IP addresses – a whitelist configuration should be necessary.



Reproduction Steps

Scan the affected servers with the Nmap portscanning tool, using the following syntax:

```
nmap -sS -p 3306 -vv -n --open <ip_address>
```


Alternatively, you can provide a file with IP addresses to scan:

```
nmap -sS -p 3306 -vv -n --open -iL <file_with_ips_to_target>
```



Evidence

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:43 UTC for 434s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
3306/tcp  open  mysql        syn-ack ttl 114
```


 **PostgreSQL Servers Exposed to Public Internet**

 **Observation**

PostgreSQL servers were found to be exposed to the public Internet. Since PostgreSQL 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 PostgreSQL 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.

 **Top Affected Nodes**

ONE (1) NODE AFFECTED

IP Address	Host Name	Operating System
35.212.46.254		Undetected

 **Recommendation**

Disable PostgreSQL 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 PostgreSQL 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 PostgreSQL service is absolutely required for business operations, then it is recommended to restrict access to specific IP addresses – a whitelist configuration should be necessary.

 **Reproduction Steps**

Scan the affected servers with the Nmap portscanning tool, using the following syntax:

```
nmap -sS -p 5432 -vv -n --open <ip_address>
```

Alternatively, you can provide a file with IP addresses to scan:

```
nmap -sS -p 5432 -vv -n --open -iL <file_with_ips_to_target>
```



Evidence

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:43 UTC for 434s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
5432/tcp  open  postgresql  syn-ack ttl 119
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:58:14 UTC for 433s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
5432/tcp  open  postgresql  syn-ack ttl 119
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:24 UTC for 3s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
5432/tcp  open  postgresql  syn-ack ttl 119
```

 **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.

 **Top Affected Nodes**

ONE (1) NODE AFFECTED		
IP Address	Host Name	Operating System
35.212.46.254		Undetected

 **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.

 **Reproduction Steps**

Use an FTP client to connect to one of the affected servers on port 21/tcp. The following syntax can be used to attempt connecting to an FTP server:

```
ftp <server_ip_address>

Furthermore, if an FTP client does not exist and the available operating system leverages the native telnet command, connectivity can be tested against an FTP server using the following syntax and leveraging the Telnet command:

telnet <server_ip_address> 21
```

If the command above works, then the remote server is listening on port 21/tcp.

 **References**

- <https://www.ipa.go.jp/security/rfc/RFC2577EN.html>



Evidence

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:43 UTC for 434s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 119
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:58:14 UTC for 433s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 119
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:24 UTC for 3s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 119
```

**MEDIUM**

Insecure Protocol - POP3

Observation

Post Office Protocol (POP) is used by email clients to retrieve emails for user accounts. By default in some POP servers, it is configured to use an insecure protocol. With the combination of email clients retrieving email contents from a cleartext protocol, this could present a significant threat to the organization's environment, depending on the user account that's configured to retrieve the emails.

Security Impact

Since POP3 is running over a cleartext protocol, 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 email contents. Such valuable information may also be useful for other attacks against the organization's network.

Top Affected Nodes

ONE (1) NODE AFFECTED		
IP Address	Host Name	Operating System
35.212.46.254		Undetected

Recommendation

Disable the service if it is not needed for business operations. If transferring files is necessary for business operations, then consider implementing Secure POP3 (POP3S) as POP3S uses encryption during communications to/from email clients.

Reproduction Steps

Use an email client to connect to one of the affected servers on port 110/tcp with the proper credentials.

Furthermore, if an email client does not exist and the available operating system leverages the native telnet command, connectivity can be tested against a POP3 server using the following syntax and leveraging the Telnet command:

```
telnet <server_ip_address> 110
```

If the command above works without requiring any SSL/TLS handshakes and do not support this in the available commands, then the server is accepting cleartext communications.

References

- <https://www.ipa.go.jp/security/rfc/RFC2577EN.html>



Evidence

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:58:14 UTC for 433s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
110/tcp   open  pop3         syn-ack ttl 119
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:24 UTC for 3s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
110/tcp   open  pop3         syn-ack ttl 116
```

```
Nmap scan report for sample1.com (35.212.46.254)
Host is up, received user-set (0.012s latency).
Scanned at 2023-06-15 23:50:43 UTC for 434s
Not shown: 483 filtered tcp ports (no-response), 4 closed udp ports (port-unreach)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
110/tcp   open  pop3         syn-ack ttl 116
```

Appendix A: Host Discovery (Operating Systems)

External Network Penetration Test

During testing, it was not possible to discover the specific operating systems running on the in-scope targets. This indicates that the targets are configured correctly to not disclose sensitive operating system information, which could be extremely valuable to an attacker looking to exploit vulnerabilities in known operating systems.

Appendix B: Identified Nodes Without Ports

During testing, all systems were found to have at least one (1) opened port. As a result, no table will be displayed in this section.

Appendix C: Host Discovery (Opened Ports)

External Network Penetration Test

IP Address	DNS Name	Port	Protocol
35.212.46.254		21	tcp
35.212.46.254		25	tcp
35.212.46.254		80	tcp
35.212.46.254		110	tcp
35.212.46.254		143	tcp
35.212.46.254		443	tcp
35.212.46.254		465	tcp
35.212.46.254		587	tcp
35.212.46.254		993	tcp
35.212.46.254		995	tcp
35.212.46.254		2525	tcp
35.212.46.254		3306	tcp
35.212.46.254		5432	tcp