

Penetration Testing Report

January 8-9/2021



Confidential

Disclaimer

All information available in this document is confidential, privileged, and is available only for the party concerned. As this report should not be distributed, published, or viewed without an authorized agreement from [REDACTED] and NGPEW.

Table of Contents

Executive Summary	4
Engagement details	4
Engagement Objectives	4
Scope	4
Results and Impact Analysis	5
Regulations and Compliances	6
Mapped Network Topology	7
Methodology	8
PTES	8
OWASP Top 10	9
Risk Classification	10
Attack Scenario	11
Vulnerability Findings	12
RCE Caused by Unrestricted HTTP "PUT" Method	12
Microsoft IIS 4.0 - Remote Buffer Overflow	14
Java Debug Wire Protocol Remote Code Execution	15
MODBUS/TCP Slave Coil Access	16
OpenSSH 2.3 < 7.7 - Username Enumeration	19
Private NGPEW Info leak	21
Applied Remediations	22
Recommended Action Plan	23
Response Strategy for Improvement	23
Appendix of Tools	24



Table of Figures

Figure 1: Security Risk Level _____ 5

Figure 2: Network Topology of NGPEW _____ 7

Figure 3: PTES Methodology _____ 8

Figure 4: CVSS V3.1 Scoring System. _____ 10

Figure 5: Registration POST Request and Response _____ 22

Figure 6: Redis Credentials Spraying Result _____ 22

Figure 7: OpenSSH Version _____ 22

Executive Summary

Engagement details

██████████ pleased to submit the following report for their second penetration test of “Next Generation Power, Electric, and Water” (NGPEW), scheduled from 9:30 am to 6:00 pm EST on Jan 8th and Jan 9th of 2020. It was agreed that all sensitive information acquired through this test will be protected under the DHS’ Protected Critical Infrastructure Information (PCII) Program.

Engagement Objectives

This penetration test was conducted to ensure that NGPEW stays compliant with the North American Electric Reliability Corporation (NERC) and its Critical Infrastructure Protection guidance (CIP). The test report shows the identified security issues within the environment of NGPEW and demonstrates how they can be exploited or abused by a malicious threat actor. It also explains how these security issues can be fixed or mitigated, referencing relevant industry-standard remediation for each finding, which can be found in later sections of the report.

Scope

The focus of the penetration test was an ICS subnet, along with some other subnets containing general servers and end-user machines, the Scope of the test was limited to the following subnets:

- 10.0.1.0/24
- 10.0.5.0/24
- 10.0.10.0/24

Results and Impact Analysis



Figure 1: Security Risk Level

The performed penetration test suggests that the overall security risk level of the company is **Medium** when following the Common Vulnerability Severity Score version 3.1 (CVSS) to rate each security finding. Detailed documentation of the findings and their technical remediations can be found in later sections of the report.

The impact of an attack on NGPEW's network could range from downtime, financial losses, cascading effects down the supply chain, damage to equipment, to critical human safety hazards.

During the engagement, the testers were able to find certain vulnerabilities in NGPEW's network which could lead to exfiltration of private operational data of "SCADA" systems, as well as crafting malicious requests to the SCADA system altering the devices' behaviour, this could cause physical damage to the infrastructure, blackouts, and dam failures, all of which result in substantial financial damage and legal fines.

Moreover, some webserver vulnerabilities affect system availability, in addition to risk of compromising other machines on the same "Active Directory" domain of the target. This can lead to abuse of privileges and avoidance of access control measures, which can cause a leak of confidential data and loss of control over the systems.

Regulations and Compliances

NGPEW is a regional power company which provides services to company providers and consumers. Due to the assets that are under the NGPEW control they are mandated by law to follow the "NERC CIP V6" compliance.

The NERC Critical Infrastructure Protection (CIP) Reliability Standards define a comprehensive set of requirements that are the basis for maintaining the reliability of the National Bulk Electric System (BES) and protecting it from cyber-attacks.

The following violations of the NERC CIP standard regulations have persisted from the previous engagement:

Finding	Violation
Microsoft IIS 4.0 - Remote Buffer Overflow	CIP-007-6 R3 (Malicious code prevention)
MODBUS/TCP Slave Coil Access	CIP-004-6 R4 (Access Management)

Table 1: Violations of the NERC CIP Standard Regulations

An urgent remediation of the violations is highly recommended, as failing to meet with these compliance program standards and requirements may subject NGPEW to fines of up to one-million US dollars per day per violation of the CIP standards, according to the [NERC enforcement actions that took place in 2019](#).

Mapped Network Topology

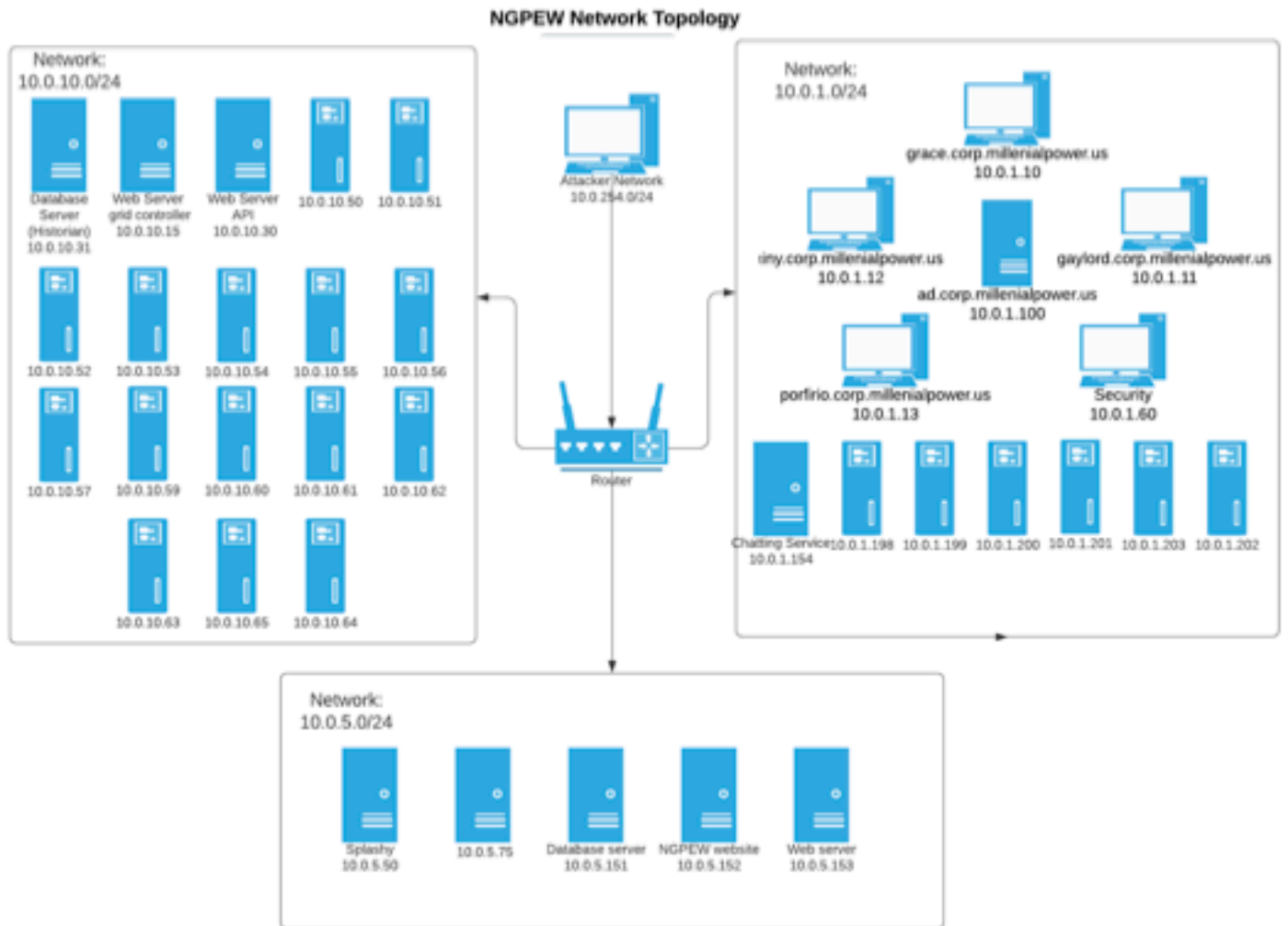


Figure 2: Network Topology of NGPEW

Methodology

To get a comprehensive security evaluation of NGPEW's systems, our consultants follow multiple industry-standard methodologies such as Penetration Testing Execution Standard (PTES) and Open Web Application Security Project (OWASP). First, open-source intelligence (OSINT) techniques are utilized to get a better understanding of the company's mission, services, and explore publicly available data that may assist in the penetration test. Afterwards, a reconnaissance phase commences after getting access on the network by scanning all hosts in the scope and identifying all services running on each host. With a clear overview of the scope, our team conducts an enterprise-wide vulnerability analysis. This analysis allows our team to quickly locate existing vulnerabilities and attack vectors to be examined for verification and to create an attack plan for the exploitation phase. The exploitation phase focuses on exploiting the vulnerabilities to gain access to systems, in which lastly privilege escalation techniques are used to locate further weaknesses within the host environment to gain higher-privilege access on the whole network.

PTES

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a penetration test, through the intelligence gathering and threat modelling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.



Figure 3: PTES Methodology

We considered the PTES penetration testing methodology since it is a great approach to such assessment. Following this methodology will give a great overview for the client on how exactly our team approached the network.

OWASP Top 10

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.



- Injection.
- Broken Authentication.
- Sensitive Data Exposure.
- XML External Entities (XXE).
- Broken Access control.
- Security misconfigurations.
- Cross Site Scripting (XSS).
- Insecure Deserialization.
- Using Components with known vulnerabilities.
- Insufficient logging and monitoring.

Our team followed the OWASP top10 as the reference to all web application testing and vulnerability detection because it is widely known that these vulnerabilities are the most found vulnerabilities on any web application.

Risk Classification

Each Vulnerability found has been classified as either Low, Medium, High, or Critical, in reference to The **Common Vulnerability Scoring System (CVSS)**.

The Common Vulnerability Scoring System (CVSS) attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores range from 0 to 10, with 10 being the most severe. As shown in *figure 4*.

CVSS 3.1 Rating	
Info	0.0-0.9
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Figure 4: CVSS V3.1 Scoring System.

Attack Scenario

Testers have noticed that two of the three subnets had network security measures that prevented access and mapping of hosts outside the internal networks, before being given access to an internal host for testing purposes. Mapping the networks from the testing host became possible, and the following assets were identified to be vulnerable:

- SCADA slave coils (PLC's) in subnet 10.0.10.0/24
- Web servers, including NGPEW website server in subnet 10.0.5.0/24

The SCADA systems were identified to be vulnerable to tampering, without exploiting them during the engagement. This was done to avoid damaging the grid or causing any physical damage to the infrastructure.

As for the identified vulnerable web servers, the testers attempted to abuse a permitted HTTP method to upload an "ASP" web-shell to gain command execution on the server, as well as identify some OWASP Top 10 vulnerabilities in the web applications.

It is important to note that the vulnerable infrastructure protected by the network security measures can prevent attacks of lower complexity but can still be exploited by a malicious threat actor if bypass of such measures succeeded, including "pivoting", and "SSH-Tunneling".

Vulnerability Findings

Critical	RCE Caused by Unrestricted HTTP "PUT" Method
Description	Microsoft IIS 4.0 vulnerable to unrestricted PUT requests which could let the attacker upload malicious files, leading to Remote Command Execution – RCE.
CVSS 3.1 Score	N/A
Affected Host(s)	10.0.5.152
Impact	High: An attacker can utilize the vulnerability and use it to execute arbitrary command and gain access to the system.
Likelihood	High
Remediation	Disable the PUT method on the web server.
Proof of Concept	Uploading a crafted payload to the vulnerable server through PUT HTTP method: <pre> root@kali04:~/dropzone/findings# curl http://10.0.5.152 --upload-file cmdasp.asp <body><h1>/cmdasp.asp was created successfully.</h1></body>root@kali04:~/dropzone/findings# </pre>



Running the uploaded file led to Remote Command Execution:

```
ipconfig      Run

\\WEBSERVER\IUSR_WEBSERVER

Windows NT IP Configuration

Ethernet adapter RTL80291:


<
    IP Address. . . . . : 10.0.5.152
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.5.1
```

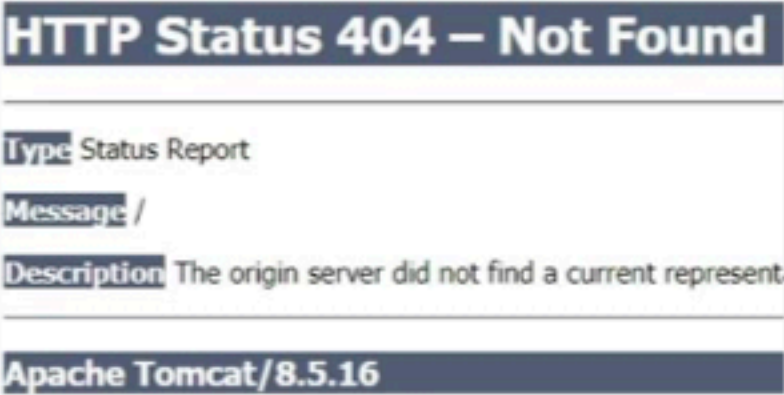
Reference N/A

Critical	Microsoft IIS 4.0 - Remote Buffer Overflow
Description	Buffer overflow in IIS 4.0 allows remote attackers to cause a denial of service via a malformed request for files with ".HTR", ".IDC", or ".STM" extensions.
CVSS 3.1 Score	9.8
Affected Host(s)	10.0.1.152
Impact	High: An attacker can utilize the vulnerability and use it to cause a denial of service on the system which will cause it to crash.
Likelihood	High
Remediation	Update the IIS service to the latest version.
Proof of Concept	The exploit was not performed due to the impact it will have on the webserver since it is a buffer overflow-based vulnerability.
Reference	https://nvd.nist.gov/vuln/detail/CVE-1999-0874

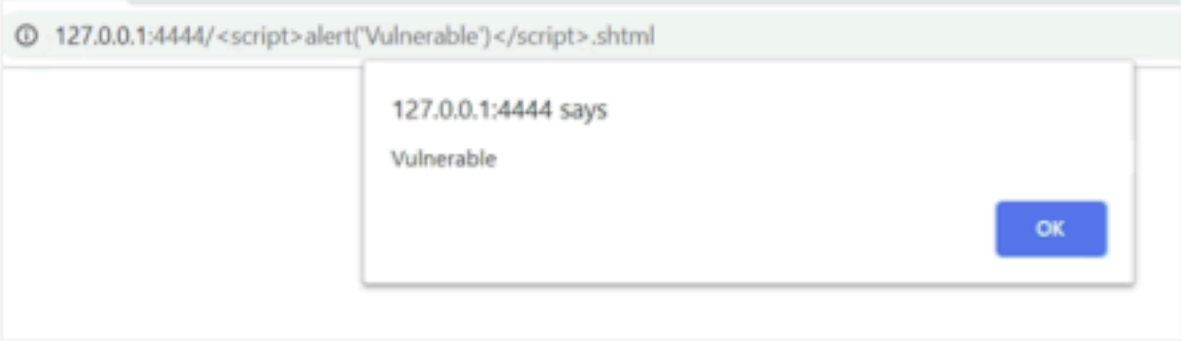
High	Java Debug Wire Protocol Remote Code Execution
Description	NetApp OnCommand Unified Manager for Linux versions 7.2 through 7.3 ship with the Java Debug Wire Protocol (JDWP) enabled which allows unauthorized local attackers to execute arbitrary code.
CVSS 3.1 Score	7.8
Affected Host(s)	10.0.5.75
Impact	High: An attacker can abuse the vulnerability and obtain remote command execution on the server.
Likelihood	Medium
Remediation	Replace with an updated version.
Proof of Concept	Metasploit was used to check if the server was affected by the vulnerability <pre>msf6 exploit(multi/misc/java_jdwp_debugger) > check [*] 10.0.5.75:12345 - The target appears to be vulnerable.</pre>
Reference	https://nvd.nist.gov/vuln/detail/CVE-2018-5486

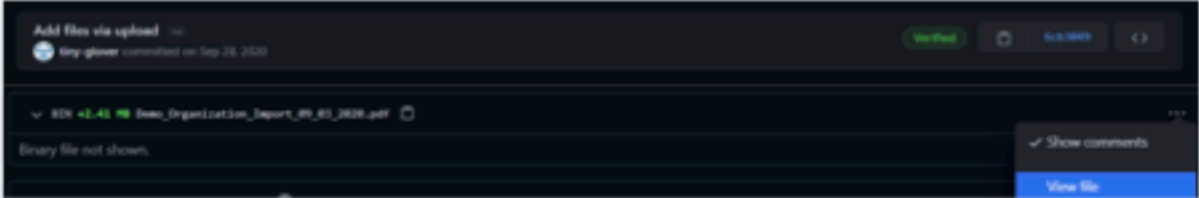
High	MODBUS/TCP Slave Coil Access
Description	Access to view and modify the state of coils and MODBUS slave registers was unrestricted. Using the open-source testing MODBUS framework "SMOD", we were able to find the Unit ID (UID) for each slave through a scanning module and then use it to read and modify coils for each one.
CVSS 3.1 Score	8.9
Affected Host(s)	10.0.10.50 - 10.0.10.53, 10.0.10.55 - 10.0.10.65
Impact	High: The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message, which will change the behaviour of the MODBUS system.
Likelihood	High
Remediation	Restrict access to the Modbus port (TCP/502) to authorized Modbus engineers.
Proof of Concept	<pre> SMOD modbus(readCoils) >set RHOSTS 10.0.10.57 SMOD modbus(readCoils) >set UID 10 SMOD modbus(readCoils) >exploit [+] Module Read Coils Function Start [+] Connecting to 10.0.10.57 [+] Response is : ###[ModbusADU]### transId = 0x2 protoId = 0x0 len = 0x4 unitId = 0xa ###[Read Coils Answer]### funcCode = 0x1 byteCount = 1L coilStatus= [0] SMOD modbus(readCoils) > </pre> <p>** As modification of MODBUS slaves' coils is possible and the PLCs are vulnerable, writing into an input register or change a coil status as a POC to this was not possible as any slight modification in the Dam PLCs could cause great damage.</p>
Reference	https://www.tenable.com/plugins/nessus/23817

High	Outdated Apache Server Version (2.4.29)
Description	The outdated apache server contains numerous vulnerabilities such as privilege execution, XSS, overflow, and DOS.
CVSS 3.1 Score	N/A
Affected Host(s)	10.0.5.153
Impact	High: An attacker may have access to a low privileged shell and then escalate to root using one of the exploits or can potentially crash the apache server to hinder the availability of the server.
Likelihood	Medium
Remediation	Update the apache server to the latest version.
Proof of Concept	<p>Apache server version is shown when opening the webpage on port 80:</p>  <p>The screenshot shows the 'Index of /' page for an Apache/2.4.29 (Ubuntu) Server at 10.0.5.153 Port 80. It includes a table header with columns: [ICO], Name, Last modified, Size, and Description. The table is currently empty.</p>
Reference	https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-241078/Apache-Http-Server-2.4.29.html

High	Outdated Tomcat 8.5.16 server
Description	The Tomcat version is an old and outdated version, which contains many vulnerabilities.
CVSS 3.1 Score	8.1
Affected Host(s)	10.0.1.75
Impact	High: An attacker can use a vulnerability present on the outdated server to gain access.
Likelihood	Medium
Remediation	Update tomcat server to the latest version.
Proof of Concept	<p>The tomcat version was shown when trying to connect to the web server:</p> 
Reference	https://www.cybersecurity-help.cz/vdb/apache_foundation/apache_tomcat/8.5.16

Medium	OpenSSH 2.3 < 7.7 - Username Enumeration
Description	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVSS 3.1 Score	5.3
Affected Host(s)	10.0.1.151, 10.0.1.153, 10.0.1.154
Impact	Medium: An attacker can use the vulnerability to enumerate all usernames on the system which is by default not publicly known.
Likelihood	Medium
Remediation	It is recommended to update the SSH version to OpenSSH 7.7 or later.
Proof of Concept	N/A
Reference	https://nvd.nist.gov/vuln/detail/CVE-2018-15473

Low	Reflected XSS on NGPEW website
Description	An attacker can request a file name containing "<script>" tags, with the extension ".shtml", the name gets reflected in the server's response with no filtering, causing the script inside the tags to be executed.
CVSS 3.1 Score	Depends on impact. Considered among OWASP Top 10 vulnerabilities.
Affected Host(s)	10.0.5.152
Impact	If an attacker got a user to click on a link, they craft on the NGPEW website, they can execute arbitrary JavaScript code to control the user's browser, which can potentially lead to conducting attacks from the user's machine, depending on the context.
Likelihood	Medium
Remediation	Implement HTML encoding for all user input before writing any of it back on the server response.
Proof of Concept	<p>If a user clicks on this link for example: <a href="http://10.0.5.152/<script>alert('Vulnerable')</script>.shtml">http://10.0.5.152/<script>alert('Vulnerable')</script>.shtml The written JavaScript will run, and an "alert" popup will appear. Other JS payloads could be used instead. The following POC does not show the actual URL since port forwarding was used to show the POC:</p> 
Reference	N/A

Info	Private NGPEW Info leak
Description	GitHub repository of NGPEW contained a commit which added the two private files, which are still viewable in the commit, although they were deleted in later commits.
CVSS 3.1 Score	N/A
Affected Host(s)	N/A
Impact	Low: Having access to this information leaks the employees list of NGPEW, which can then be used to create a user's wordlist for all employees.
Likelihood	Medium
Remediation	Change the GitHub repository to a private repository.
Proof of Concept	
Reference	https://github.com/Next-Generation-Power-and-Water/docs

Applied Remediations

From the previous engagement, multiple security measures were presented by the penetration testers. NGPEW has taken these measures into consideration by implementing strong network security measures and patching multiple severe vulnerabilities.

Implementing proper network segmentation correlatively to the corporate's systems. In addition, filtering unused ports and closing unnecessary services, which reduces the security risk in case of a network intrusion, by limiting the attacker's options and hindering their ability to move laterally.

Conducting regular penetration tests and vulnerability assessments: applying necessary security practices and testing is much more cost effective than the potential financial damage a breach can cause, not to mention the potential legal liabilities and harm of the company's reputation. Therefore, continuous scheduled assessments will ensure that the security posture of NGPEW is solid and can withstand the risk of threat actors who target companies with such reputation and size.

The rocket chat service, where attackers were able to create accounts and read sensitive messages, was remediated by closing the registration, the testers confirmed that registration closed by sending a specialized post request where the server replied with a message confirming that the registration is closed. This confirmed that there was no workaround to register a new account as rocket chat had it fully disabled.

```
root@kali04:/tmp/bundle/programs/server# curl -H "Content-type:application/json" http://
{"success":false,"error":"User registration is disabled [error-user-registration-disabled]"},
/10.0.1.154:3000/api/v1/users.register -d '{"username": "roger", "email": "roger@example.com", "pass": "123", "name": "Roger"}'
{"errorType":"error-user-registration-disabled","details":{"method":"registerUser"}}root@kali04:/tmp/bundle/programs/server#
```

Figure 5: Registration POST Request and Response

The Redis database's weak password was changed. The testers no longer have access to the Redis database. The password was changed to a more secure password. An NSE-script of the most common 500 passwords were tried on the Redis database but yielded nothing.

```
PORT      STATE SERVICE
6379/tcp  open  redis
| redis-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 5000 guesses in 11 seconds, average tps: 454.5
```

Figure 6: Redis Credentials Spraying Result

Versions of outdated services were updated; this fixed most of their vulnerabilities. OpenSSH's outdated version was updated to mitigate the ability for attackers to gain unauthorized access or information.

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1
|_ banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

Figure 7: OpenSSH Version

Recommended Action Plan

In accordance with the overall corporation security risk discovered by this penetration test, a response strategy shall be organised into a timely manner. Certain key points are proposed below to reinforce the overall security of NGPEW systems.

Response Strategy for Improvement

- Following [OWASP WSTG](#) recommendations for best security practices regarding web applications and infrastructure, as the intrusion of insecure web applications can lead to disclosure of confidential corporate data, a breach of the internal network that allows further damage, and the ability to target the application's end user directly, whether a customer or an employee.
- Replacing legacy IT solutions and protocols, with up-to-date technologies built with security in mind. Since the exploitation of old technologies has become easier, where tools and techniques used by threat actors keep advancing, investing in solutions that can keep up with the security demand is crucial, especially for key infrastructure that performs critical tasks for the company.
- Organising user awareness sessions to upskill employees about the risk of misusing social media, and how attackers could utilize unintentionally disclosed information in their attacks, along with demonstrating the best practice of account privacy. This should be followed by enforcing administrative policies and accounting measures.
- Automating management and patching of infrastructure using configuration management systems, this will ensure that software on all endpoints stays up-to-date and receives latest security patches as soon as they are available. In addition, this will ease the process of deploying and replacing devices using Infrastructure as Code (IaC), maintaining service availability and server uptime.
- Installing MODBUS Security Application Protocol to mitigate MODBUS which perhaps utilize cyber-attacks such as slave and master impersonation, frame capture and interpretation and discovery of Modbus elements in the network.

Appendix of Tools

Metasploit:

An open-source attack framework first developed by H. D. Moore in 2003. Metasploit is used for hacking into systems for testing purposes. Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research.

Dirbuster:

A multi-threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within.

Nikto:

An Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

Autorecon:

is a multi-threaded network reconnaissance tool which performs automated enumeration of services. It is a highly efficient tool which can scan an entire scope, and do follow up scans which give further information, on results of the initial scan, automatically.

Crackmapexec:

CrackMapExec (a.k.a CME) is a post-exploitation tool that helps automate assessing the security of large Active Directory networks

NMAP:

Nmap is a free and open-source network scanner created by Gordon Lyon. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides several features for probing computer networks, including host discovery and service and operating system detection.

SMOD:

SMOD is a modular framework with every kind of diagnostic and offensive feature you could need to pentest modbus protocol. It is a full Modbus protocol implementation using Python and Scapy. This software could be run on Linux/OSX under python 2.7.x.

Linpeas:

A privilege escalation tools for Linux/Unix, search for possible local privilege escalation paths that can be exploited.

Gobuster:

Is a script written in go, which can brute force directory/file, DNS, and VHost.

Hydra:

It's a tool, which brute forces credentials on numerous services, most notably HTTP, SMB, and other services.

Enum4Linux:

It is a tool for enumerating information from Windows and Samba systems. It is written in Perl and is basically a wrapper around the Samba tools smbclient, rpcclient, net and nmblookup.