Next-Generation Power and Water
PENETRATION TEST REPORT

January 9, 2021

[redacted]

CONFIDENTIAL

TABLE OF CONTENTS

EXECUTIVE SUMMARY

[redacted] was contracted by Next-Generation Power and Water ("NGPEW") to conduct a follow-up penetration test in order to determine NGPEW's exposure and risk to a targeted attack. This assessment was performed on January 8, 2021 and January 9, 2021. The scope of engagement encompassed the corporate, services, and power networks located at 10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24 respectively. This report documents the assessment and a high-level overview of our test findings as well as detailed technical descriptions for each specific risk finding. The document also includes steps for remediation for each finding as well as overall business strategies to help improve security posture. The figure below shows the number of vulnerabilities discovered, rated by severity from Critical to Informational.

Critical	High	Medium	Low	Informational
6	5	2	4	2

[redacted] began with limited visibility of the corporate network, and no visibility of the service or power networks. [redacted] was eventually able to discover authentication vulnerabilities as a result of weak passwords found within the corporate network, allowing the team to gain access to NGPEW workstations and establish a foothold. From the foothold [redacted] was able to gain visibility to the power and service networks and begin assessing targets in those net[redacted] conducted a thorough analysis of all systems on the target networks and documented as many security issues as possible. These flaws, which include unauthenticated remote access, vulnerabilities in web servers, and exposure of passwords, pose a significant risk to the security of critical business assets. The assets at risk, if compromised, could potentially lead to a loss of power, damage to the power plant and distribution grid facilities, or loss of life.

Many security issues outlined in this report are in violation of the NERC CIP requirements, which establish security baselines for companies that maintain critical infrastructure. Failing to meet the security requirements specified by NERC CIP could result in financial and regulatory penalties. [redacted] financial analysts examined public data detailing the fines incurred by NERC CIP violations over the years 2009-2019 and have included the results in Appendix D. Average fines have been increasing and reached a peak individual fine of 1.7 million dollars in 2019.

NGPEW is a rapidly expanding power company and with its recent announcement of going public, it is crucial that NGPEW operates with vigilance to ensure compliance with NERC CIP as well as maintain public trust. [redacted] recommends immediate action be taken towards critical findings to reduce the possibility of a network compromise and a potential data breach. While NGPEW has taken precautions to secure its network, [redacted] strongly recommends taking additional measures to further reduce risk to the business. Given the increasing occurrence of data breaches and destructive nature of these attacks, our security analysts are committed to working proactively with the NGPEW team to mitigate the risks detailed in this report.

STRATEGIC RECOMMENDATIONS

Key Security Strengths

Throughout the assessment, [redacted] identified several strong security controls within NGPEW network. These controls should be continually regulated in conjunction with resolving the identified weaknesses in order to bolster NGPEW's security posture. [redacted] has included the findings below:

- **Hardened Windows Services:**
  [redacted] did not identify any significant vulnerabilities found with Windows related services. Due to the number of hosts running Server Message Block ("SMB") and Remote Desktop Protocol ("RDP"), [redacted] emphasized scanning for potential exploitation with major vulnerabilities in Windows such as EternalBlue (MS017-010), BlueKeep (CVE-2019-0708), and ZeroLogon (CVE-2020-1472). [redacted] recognizes that NGPEW secured its Windows infrastructure from trivial exploitation. These actions included disabling anonymous access of SMB shares which would otherwise allow attackers the ability to view files shared across NGPEW's network. [redacted] also identified the precautions placed on RDP, where Network Level Authentication ("NLA") was enabled, protecting NGPEW systems from exploitation of BlueKeep. [redacted] advises NGPEW to continue patching regularly and ensure Windows systems are kept up to date against vulnerabilities.

- **Network Segmentation**
  Following [redacted]'s advice after the first engagement, NGPEW established network segmentation within its core infrastructure. [redacted] was unable to directly access industrial control systems or other critical internal resources from the attacker network. Proper network segmentation prevents trivial attempts from attackers to gain access against the infrastructure.

- **Lack of Cross-Site Scripting ("XSS") Vulnerabilities**
  [redacted] discovered applications present from the first engagement that are no longer vulnerable to XSS. Lack of this vulnerability resolves the issue where an attacker could compromise interactions that a user would normally have with a vulnerable NGPEW application.

- **Improved Rocket.Chat Registration Process**
  In the first assessment, [redacted] had the ability to freely create accounts on NGPEW's communication platform which allows [redacted] analysts to monitor interactions between employees and observe sensitive information passed through the chat. During this assessment, [redacted] noted Rocket.Chat had registration disabled which prevented these actions from happening.

Key Areas for Improvement

[redacted] identified several areas of improvement for NGPEW throughout the course of the assessment and has included the most significant findings below:

- **Weak Password Policy:**
  During [redacted] assessment, many user passwords were encountered that were easily guessable and could be found in many common password lists. This made it clear that the current password policy of NGPEW is in direct violation of NERC CIP compliance. [redacted] recommends NGPEW reevaluate its password policy immediately and ensure the new policy is in compliance with NERC CIP standards[1].

- **Plaintext Credentials Discovered:**
  Our security analysts observed NGPEW employees practicing poor operational security by exchanging plaintext credentials over Rocket.Chat. If a threat actor were to capture the observed credentials they could potentially leverage them to gain access to NGPEW critical services and infrastructure. [redacted] recommends all employees receive training in best security practices and are reminded to never share credentials over insecure channels.

- **No Multi Factor Authentication:**
  [redacted] identified services such as Rocket.Chat and RDP that did not have multi-factor authentication enabled. If credentials were compromised during an attack, these services could be leveraged by threat actors to access key services across the network. [redacted] recommends NGPEW implement a form of multi-factor authentication on all services as soon as possible.

- **Lack of Authentication:**
  None of the NGPEW Programmable Logic Controllers ("PLCs") required authentication to access. Our security analysts were able to connect to all PLCs and run arbitrary commands. If a threat actor can compromise the internal network of NGPEW, then the attacker could gain access to these infrastructure critical devices. Due to the high risk factor these PLCs represent [redacted] recommends implementing a form of authentication on all PLCs immediately.

- **Use of Privileged Access Workstations:**
  Privileged Access Workstations ("PAWs") are computers isolated from the internet that are dedicated to managing sensitive assets. Firewalls on the sensitive asset are then configured to only allow access to remote administration tools through PAW computers and specific users via Network Level Authentication. This approach ensures that only users and computers that are authorized can connect, and that administrative accounts are never required to logon to computers that access the internet or are used for other general purpose work.

[1] https://nfrontsecurity.com/compliance/nerc-cip-password-policy-compliance.php

SCOPE

[redacted] performed security testing on NGPEW's network infrastructure. The testing was conducted from the perspective of an attacker with a connection to NGPEW's internal networks. NGPEW provided the team with the network ranges shown in Figure 1 as the scope for the penetration test. All networks contained live hosts and were enumerated by the team. [redacted] did not test any systems outside of the IP Address ranges in Figure 1. [redacted] recognizes the fragility of Supervisory Control and Data Acquisition ("SCADA") systems and performed tests with the oversight of NGPEW's management team, ensuring that availability of systems would not be affected during the course of the engagement.

Network Ranges
10.0.1.0/24
10.0.5.0/24
10.0.10.0/24

Figure 1: Network Ranges

TESTING DETAILS

Penetration Testing Execution Standard

[redacted] references the Penetration Testing Execution Standard[2] ("PTES") which is designed to provide both businesses and security service providers with a common language and scope for performing assessments:

Figure 2: Main sections of the Penetration Testing Execution Standard

OWASP Top 10

[redacted] also references the Open Web Application Security Project ("OWASP") Top 10[3] when web applications are in scope for the assessment. OWASP Top 10 focuses on the top critical web application security risks and vulnerabilities:

1. Injection	6. Security Misconfiguration
2. Broken Authentication	7. Cross Site Scripting
3. Sensitive Data Exposure	8. Insecure Deserialization
4. XML External Entities	9. Using Components with Known Vulnerabilities
5. Broken Access Control	10. Insufficient Logging and Monitoring

Figure 3: Top 10 Web Application Vulnerabilities

Open Source Intelligence Gathering

Open Source Intelligence ("OSINT") is part of the Intelligence Gathering phase. From October 19th, 2020 to January 8th, 2021, [redacted] gathered intelligence on NGPEW through its website, GitHub, and social media platforms such as LinkedIn and Twitter. On NGPEW's GitHub, [redacted] discovered an internal organization chart that listed employee names and their role in NGPEW. This information was utilized to identify high value targets to compromise during the testing phase. More detailed information on OSINT Findings can be found in *Appendix A: OSINT Artifacts*.

[2] http://www.pentest-standard.org/index.php/Main_Page
[3] https://owasp.org/www-project-top-ten/

Host Discovery

In order to find and maintain an updated list of in-scope targets, [redacted] developed and utilized nVis, a lightweight collaborative nmap scanning framework, in order to perform reconnaissance on the NGPEW internal network. The framework relies on multiple clients to quickly provide nmap scans in parallel. The nmap scans are forwarded to a central server, which then provides a real-time front-end interface for the team. Further information about the tool can be found in *Appendix C: Tools*. During the reconnaissance phase, [redacted] identified several Windows, Linux, and Programmable Logic Controllers systems on the corporate network. On the Power Network subnet, there were systems that were listening over ModBus protocol. The Services Network contained 5 systems that were mainly used for hosting public facing information.

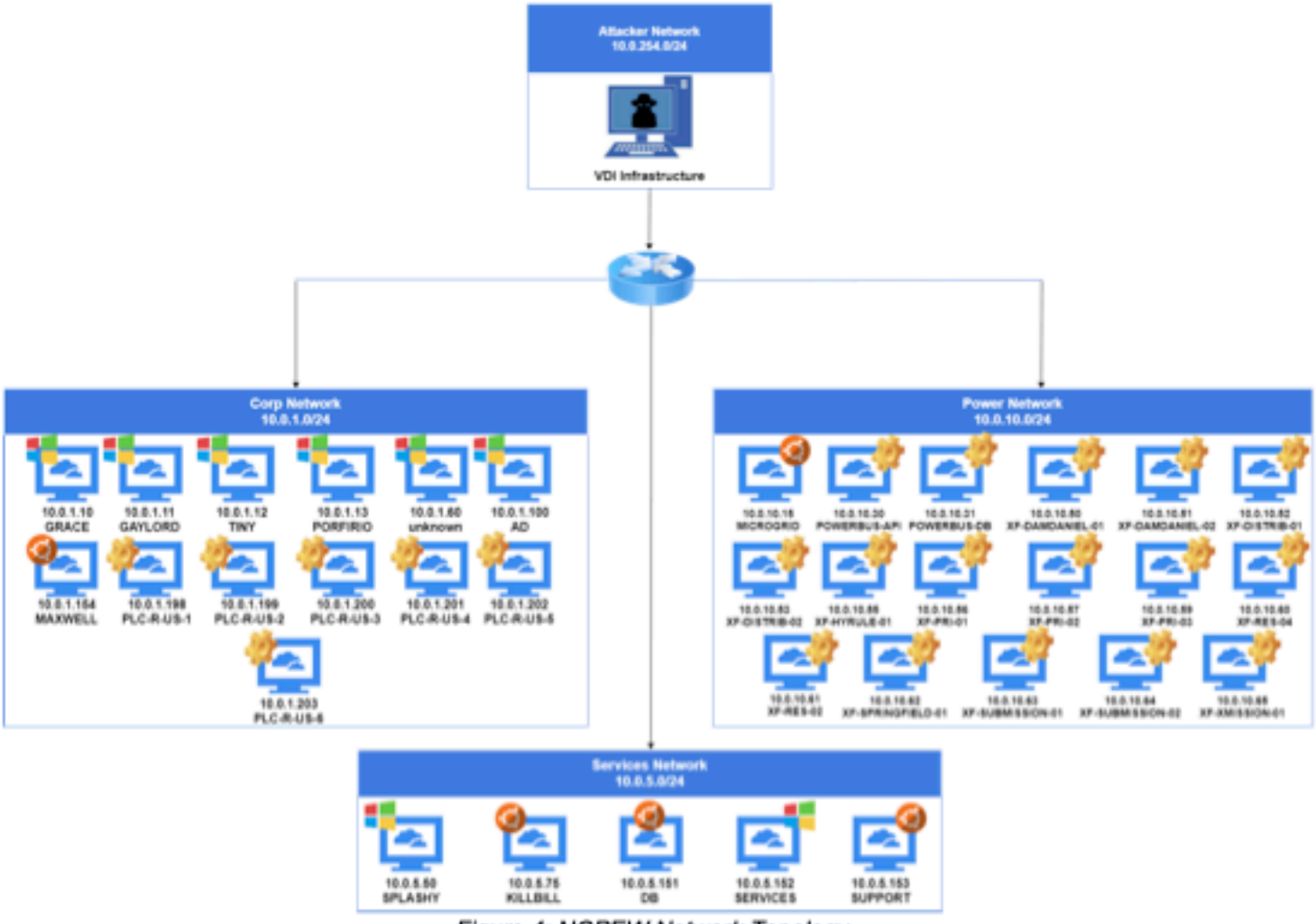


Figure 4: NGPEW Network Topology

Manual Testing / Validation

The following section illustrates a high level attack narrative that [redacted] conducted on NGPEW's network.

Lightweight Directory Access Protocol ("LDAP")

[redacted] utilized tools such as `ldapsearch`[4] to enumerate LDAP. Enumerating LDAP with tools such as `ldapsearch` can allow an attacker to identify the system's base domain name using published naming contexts. With the base domain name of the system, an attacker can filter LDAP queries to gain further information on the hierarchy of the system, usernames, passwords, password policies, etc. if anonymous bind is allowed.

Figure 5: ldapsearch enumeration on 10.0.1.100

Server Message Block ("SMB")

For SMB, [redacted] ran `enum4linux`[5] and `smbmap` to enumerate information on the service. When secure policies are overlooked for SMB such as allowing null authentication, an attacker can have possible access to user shares which can result in information disclosure and malicious files being on a system.

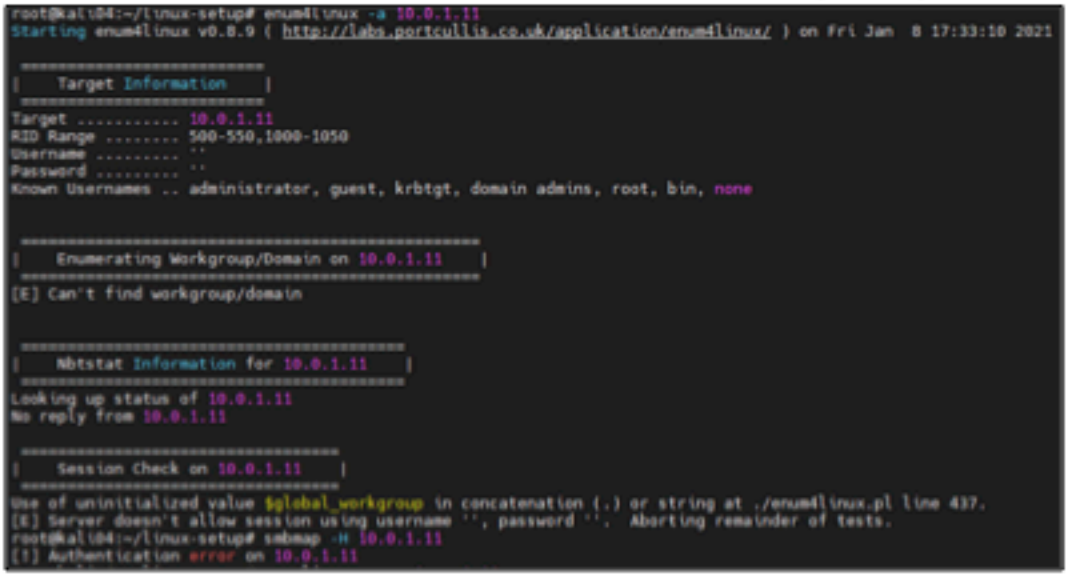


Figure 6: enum4linux enumeration on 10.0.1.11

[4] https://linux.die.net/man/1/ldapsearch
[5] https://tools.kali.org/information-gathering/enum4linux

Remote Procedure Call ("RPC")

RPC is a way that allows Windows machine processes to communicate with one another. When null authentication is allowed with RPC, an attacker can gain detailed system information, user information, and a list of client information of shared resources through SMB. This information can act as leverage for an attacker by presenting more information about the system and users which may lead to further persistence within the environment.

```
root@kali04:~/linux-setup# rpcclient -U "" 10.0.1.11
Enter WORKGROUP\'s password:
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
```

Figure 7: rpcclient being used to check for null authentication

Kerberos

[redacted] implemented tools such as GetNPUsers.py[6] which attempts to list and get ticket-granting tickets ("TGT") for user accounts that do not require Kerberos preauthentication set. Users that do not have Kerberos preauthentication set will have their password outputted from the `GetNPUsers.py` in the form of a Kerberos 5 AS-REP type 23 hash. This hash can be cracked using password cracking tools such as `hashcat` which ultimately can lead to compromised accounts if Kerberos preauthentication is not required for users on the domain controller.

Figure 8: Using GetNPUsers.py to test for Kerberos preauthentication disabled

EternalBlue Vulnerability Scanner

Using Metasploit Framework's (MFS) EternalBlue vulnerability scanner, an attacker can search for systems that are using SMBv1 and are vulnerable to EternalBlue. EternalBlue allows an attacker to execute arbitrary code execution on a target system due to how Windows mishandles crafted packets on particular versions of SMBv1.

[6] https://github.com/SecureAuthCorp/impacket

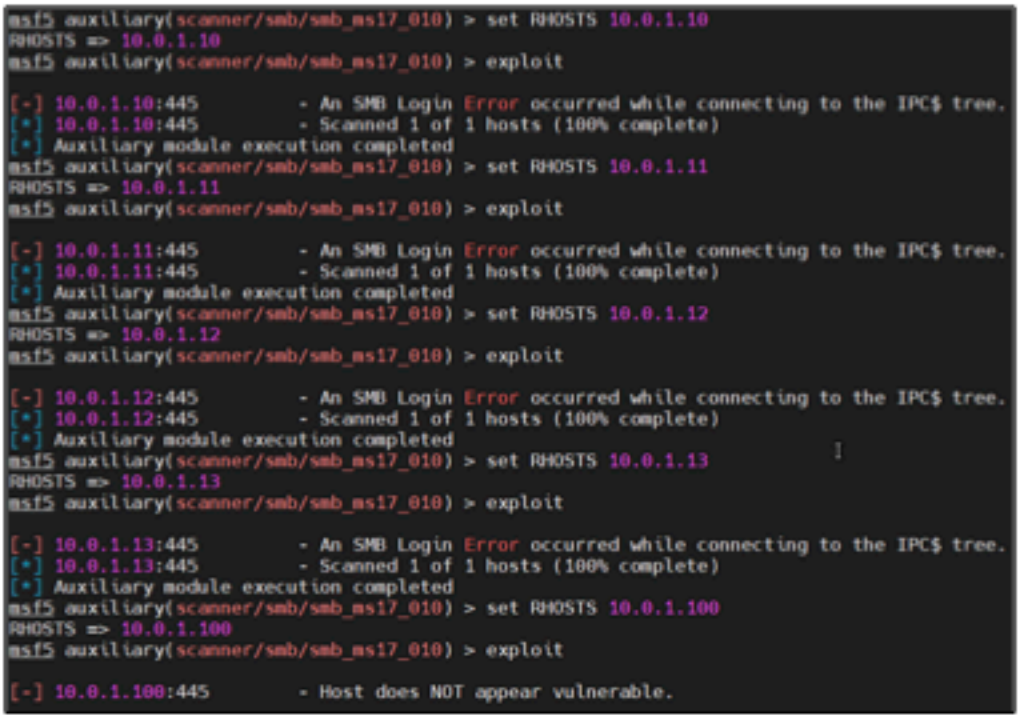


Figure 9: Running Metasploit Framework's EternalBlue scanner to detect any systems vulnerable to EternalBlue

CrackMapExec

[redacted] was able to gain access to the Administrator user on the following IP addresses: `10.0.1.10`, `10.0.1.11`, and `10.0.1.13`. The Administrator user was accessed through the three Windows Workstations by bruteforcing user's passwords using CrackMapExec[7], which is a tool that helps in assessing security of large networks through HTTP, SMB, or MSSQL protocols by utilizing bruce forcing, password spraying, and validation of user credentials that can successfully log in. Furthermore, crackmapexec contains options to expose information on specific permissions for specific users that have been compromised. After verifying the use of weak credentials from the 10.0.1.10, 10.0.1.11, and 10.0.1.13, [redacted] began testing the entire NGPEW network for weak credentials and unauthenticated access to services which led to a compromise of multiple user accounts, systems, and services detailed in the findings section of the report.

[7] https://github.com/byt3bl33d3r/CrackMapExec

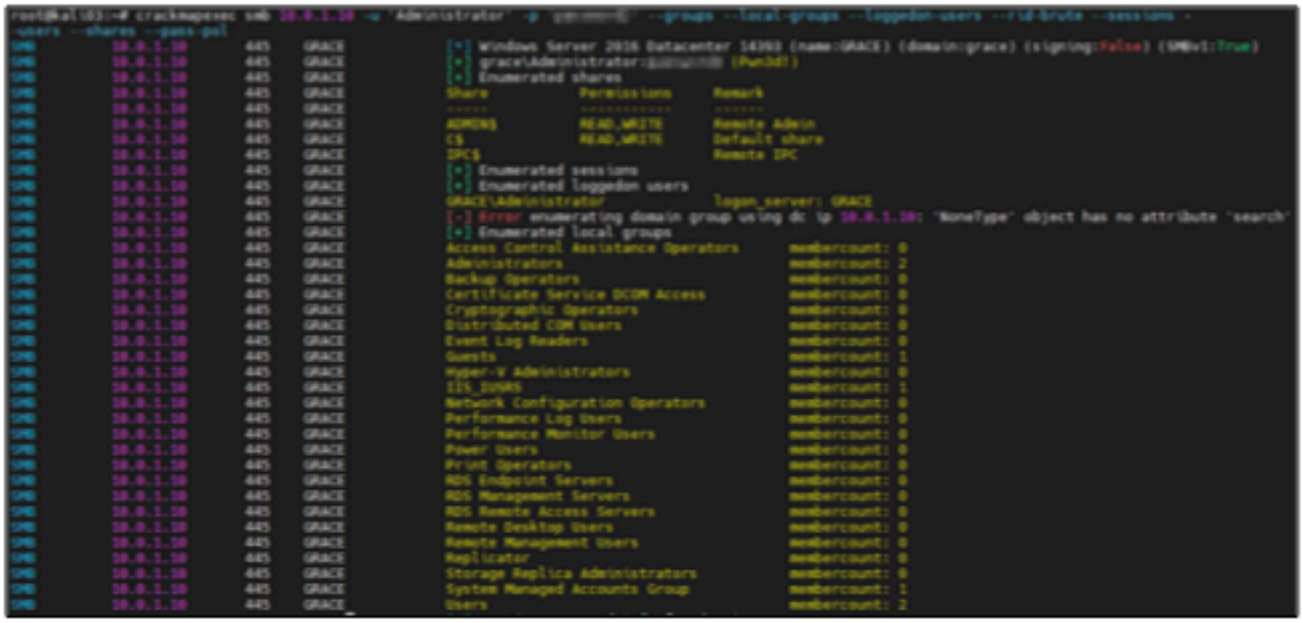


Figure 10: CrackMapExec being ran to identify user permissions

Internet Information Services ("IIS")

[redacted] compromised NGPEW's public-facing Internet Information Services ("IIS") website after validating that a remote code execution vulnerability from a previous penetration testing engagement was still accessible. [redacted] analysts uploaded a malicious ASP file to the 10.0.5.152 web server using the PUT HTTP method with OWASP ZAP and [redacted] gained system access to the server.

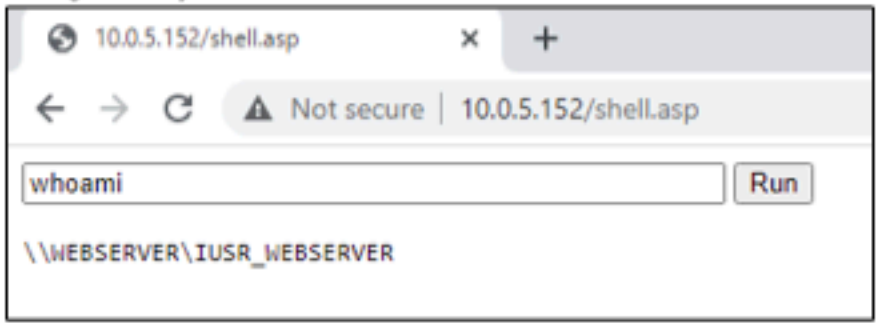


Figure 11: System access on the IIS web server

MySQL and PostgreSQL

[redacted] security analysts successfully gained access to the billing and support internal databases hosted by NGPEW on its services subnet. [redacted] gained access to the internal MySQL billing database on 10.0.5.75 after discovering default credentials and compromised the PostgreSQL helpdesk database on 10.0.5.151 by exploiting weak credentials.

```
root@kali06:~/XSSwagger# proxychains mysql -h 10.0.5.75 -u root -p
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
|S-chain|-<>-127.0.0.1:1080-<><>-10.0.5.75:3306-<><>-OK
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 2848
Server version: 10.3.14-MariaDB-1:10.3.14+maria~bionic mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Figure 12: Accessing MariaDB with weak credentials

Industrial Control Systems ("ICS")

[redacted]s security analysts validated the findings and successfully built upon the research made during the first penetration testing engagement. [redacted] confirmed Programmable Logic Controllers ("PLC's") to be accessible from the internal network and was able to directly interface with them, gaining the ability to tamper with their configuration and firmware. [redacted] analysts expanded on their knowledge of the dam API by reverse engineering the Human Machine Interface ("HMI") application and discovering ways to tamper with its functionality.

```
PS C:\Users\tiny.glover\Desktop> .\nc64.exe 10.0.1.198 8080


PLC DEBUG v0.1
[c] PLC-R-US 1994
```

Figure 13: PLC accessed from internal network

RISK ASSESSMENT OVERVIEW

[redacted] follows a standardized risk assessment gradient. This rubric assesses the two crucial factors of a risk: possibility of exploitation & the potential impact on the business. The chart below illustrates the methodology, with likelihood of the exploit on the X-axis and the impact on the Y-axis. If a finding is not assessed to be within [redacted]s risk matrix, it will be listed as informational. Findings listed in the informational section are slight deviations from security best practices, but may pose a greater risk in the future.

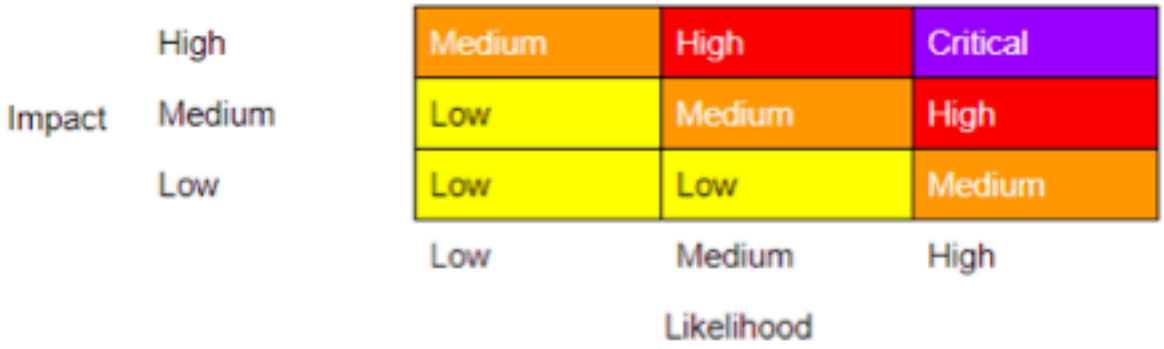


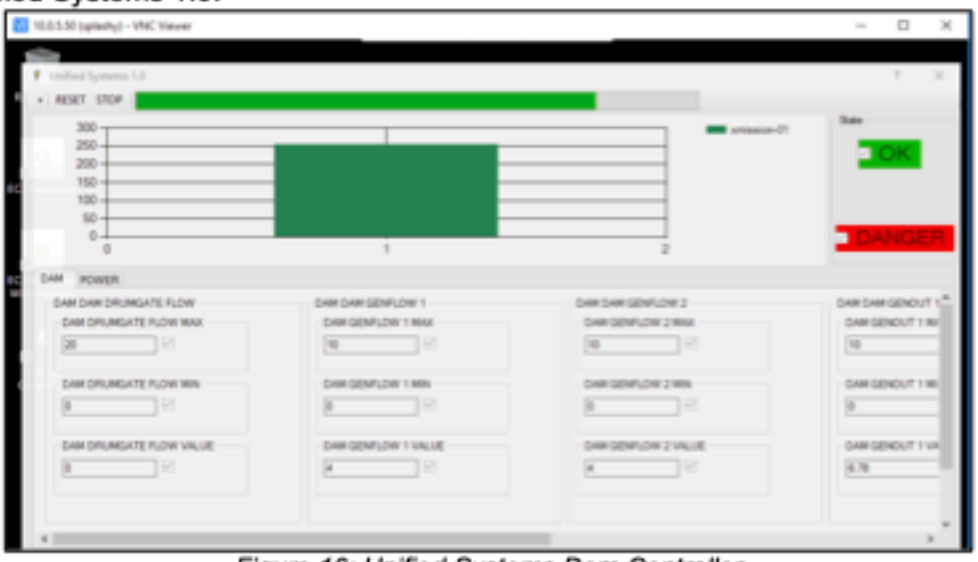
Figure 14: Risk matrix

The pie chart below is a summary of the vulnerabilities found during the penetration test. Each vulnerability is rated by severity, as calculated by the risk matrix.

Figure 15: Pie chart listing number of vulnerabilities identified

CRITICAL FINDINGS

Critical - 01	Unauthenticated Administrative VNC Access to Dam	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	Administrative access over a Virtual Network Computing ("VNC") protocol was enabled without a password for the server running the Human Machine Interface ("HMI"),used to administer the dam controls. The HMI acts as a display for dam operators and provides important information on power generation and safety systems. [redacted] was able to read and write data relating to the HMI application, as well as have full administrative access to all functions of the server.	
Affected Scope	• VNC (TCP/3900) ○ 10.0.5.50 (SPLASHY)	
Business Impact	The access gained allows attackers to manipulate or destroy critical telemetry data coming from the dam PLC. This could leave plant operators in the dark regarding the status of the power plant and unable to see when a malfunction is occurring, which could lead to loss of life if a catastrophic error occurs and is not corrected. Because the dam is one of NGPEW's core business services, it is important that this system maintains uptime.	
Exploitation Likelihood	Unauthenticated administrative VNC access to the dam allows an attacker to use the VNC protocol to connect to the `10.0.5.50` server without a username and password. Unauthenticated access to the `10.0.5.50` server through VNC is highly probable due to an absence of authentication and poses a significant risk. A threat actor would be able to easily access information on power generation and safety systems as well as tamper with or deface these critical systems as the HMI application is displayed on the desktop by default.	

Exploitation Details	After initial network scanning, [redacted] discovered that VNC was open on the `10.0.5.50` server. [redacted] security analysts logged in over the network using VNC Viewer[8] without providing credentials and were granted access to the Local Administrator account on the server. Figure 16 presents [redacted] gaining VNC access to the `10.0.5.50` system due to lack of authentication and having administrative access to Unified Systems 1.0.  *Figure 16: Unified Systems Dam Controller*
Remediation	[redacted] recommends that any remote access requires strong passwords and two-factor authentication, especially for systems that contain critical infrastructure. If the HMI needs to be accessible remotely and quickly from the power plant floor, it could also be configured with a hardware security key that can be used for quick authentication. Firewalling with Network Level Authentication could also be used to ensure that only dedicated systems are able to access the HMI remotely.. [redacted] also recommends that the HMI application run in the context of a non-administrative user with only the permissions required to perform its job. If the HMI application is the only application used on the system, it could also be configured as a kiosk. The dam control and monitoring network should be completely isolated from all other networks to provide maximum security.
Compliance Violations	NERC CIP 5 R2.2 Interactive remote access sessions are not encrypted NERC CIP 5 R2.3 Multi factor authentication is no required for remote sessions More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf[9]

[8] https://www.realvnc.com/en/connect/download/viewer/
[9] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf

Critical - 02	Weak Domain Administrator Credentials	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	[redacted]s security analysts were able to obtain a working credential to the Domain Administrator account [redacted] identified that this password did not meet complexity requirements and can be commonly found in password lists online. The credentials were validated by using the Remote Desktop Connection service to log in to the Domain Controller.	
Affected Scope	• Active Directory ○ 10.0.1.100 (AD)	
Business Impact	An attacker after attaining the aforementioned credentials would enable them to have complete control over NGPEW's Active Directory environment. An attacker with this type of access would further be allowed to alter NGPEW's infrastructure such as changing employee passwords, disabling connected workstations, or even taking down critical systems NGPEW relies on in managing its utility grid, leading to financial and human loss. Although [redacted] did not identify workstations connected to the domain, any future systems that connect to the domain could be vulnerable. Furthermore, with the ability to exfiltrate sensitive customer and employee data from the Active Directory environment, NGPEW may face several regulatory violations.	
Exploitation Likelihood	The password discovered by [redacted] is a common password that can easily be brute forced. In addition, NGPEW did not have any form of account lockout policies, allowing an attacker to brute force without any restrictions. Domain Controllers are usually high value targets for threat actors, making this a highly likely attack.	
Exploitation Details	With the initial discovery of the weak Local Administrator credentials, [redacted] security analysts attempted variations of the password and were able to successfully RDP onto the Domain Controller. The attack could be simulated by using Hydra[10], a network logon cracker, to brute force an RDP session on NGPEW's Domain Controller.	

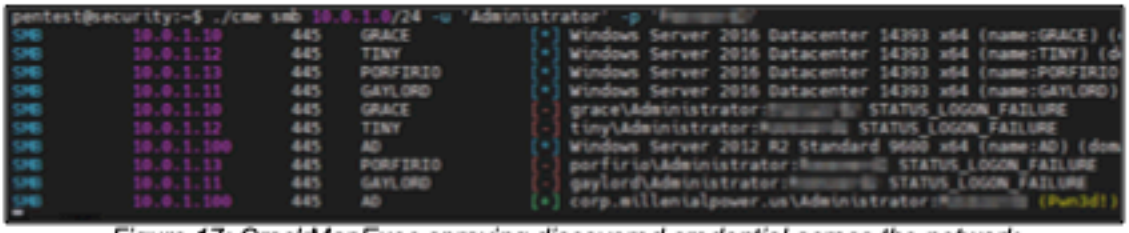


Figure 17: CrackMapExec spraying discovered credential across the network

[10] https://github.com/vanhauser-thc/thc-hydra

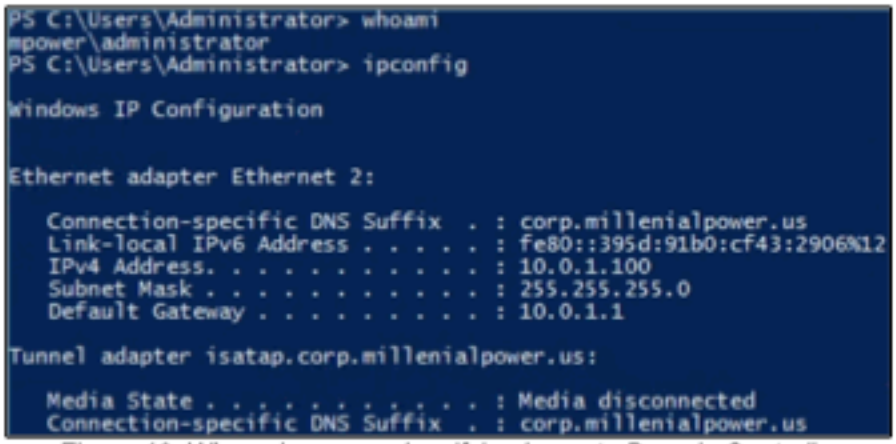


Figure 18: Whoami command verifying logon to Domain Controller

Remediation	[redacted] recommends that NGPEW implements a strong password policy enforced by Microsoft Group Policy[11]. In doing so, this will ensure that future passwords made by users on the Domain will be less vulnerable from brute force attacks as well as stay within compliance to NERC CIP requirements[12].
Compliance Violations	NERC CIP 7 R5.5.1 Password-only authentication length requirements are not met NERC CIP 7 R5.5.2 Password-only authentication complexity requirements are not met More information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[13]

[11] http://woshub.com/password-policy-active-directory/
[12] https://nfrontsecurity.com/compliance/nerc-cip-password-policy-compliance.php
[13] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

Critical - 03	Weak Local Administrator Credentials	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	[redacted] discovered, through brute forcing Windows Remote Management ("WinRM"), that several Windows systems on the NGPEW network had the default Local Administrator account enabled with weak credentials. With the Local Administrator account, [redacted] security analysts were able to gain remote access onto systems within the corporate network. Enumerating through the workstations, [redacted] was able to find instances of plaintext credentials located in several users' mailboxes.	

Affected Scope	• Workgroup
	  ◦ 10.0.1.10 (GRACE)
	  ◦ 10.0.1.11 (GAYLORD)
	  ◦ 10.0.1.12 (TINY)
	  ◦ 10.0.1.13 (PORFIRIO)
	  ◦ 10.0.5.50 (SPLASHY)
	  ▪ Account Affected
	  • Local Administrator	

Business Impact	Due to these systems being connected to the corporate network, an attacker could leverage the credentials in order to enumerate sensitive Active Directory information, creating a path to a full domain takeover. With this access, it would allow the attacker to make arbitrary changes to both the internal and external facing company infrastructure. Without a functioning Active Directory environment, employees may not be able to authenticate to their workstations and any resulting service downtime could bring business operations to a halt. Furthermore, because the discovered password does not meet NERC CIP password complexity requirements, NGPEW may face regulatory violations.	
Exploitation Likelihood	The passwords discovered by [redacted] are commonly found in password lists online and should not be used anywhere in the corporate network. [redacted] identified that NGPEW did not have any form of account lockout policies, allowing an attacker to brute force without any restrictions. In addition, [redacted] identified the compromised computer systems as likely belonging to NGPEW executives due to the system's hostname. Executives would be a valuable target to a threat actor during an attack, making this vulnerability highly likely to be exploited.	

Exploitation Details	[redacted] utilized the metasploit module, `auxiliary/scanner/winrm/winrm_login`, to brute force Windows systems running the WinRM service. Using the rockyou.txt[14] wordlist, [redacted] was able to obtain a successful login with the Administrator account. The following figure shows the Metasploit settings used for bruteforcing.
Remediation	Passwords on all workstations should meet complexity requirements. [redacted] recommends NGPEW implement Microsoft's Local Administrator Password Solution. Microsoft's LAPS[15] solution provides a solution by setting a unique, random password for the local administrator account on every system in the domain.

```
msf5 auxiliary(scanner/winrm/winrm_login) > show options

Module options (auxiliary/scanner/winrm/winrm_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DOMAIN            WORKSTATION                    yes       The domain to use for Windows authentification
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE         /usr/share/wordlists/rockyou.txt  no     File containing passwords, one per line
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                                           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             5985                           yes       The target port (TCP)
   SSL               false                          no        Negotiate SSL/TLS for outgoing connections
   STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   URI               /wsman                         yes       The URI of the WinRM service
   USERNAME          administrator                  no        A specific username to authenticate as
   USERPASS_FILE                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts
   VHOST                                            no        HTTP server virtual host

[+] 10.0.1.13:5985 - Login Successful: WORKSTATION\Administrator:[redacted]
```

Figure 19: Credential found with winrm_login module

After credentials were confirmed, CrackMapExec was used to spray credentials across the network. This allowed for [redacted] security analysts to discover vulnerable machines and move laterally.

```
pentest@security:~$ ./cme smb 10.0.1.0/24 -u 'Administrator' -p 'Password2'
SMB         10.0.1.10       445    GRACE            [*] Windows Server 2016 Datacenter 14393 x64 (name:GRACE) (domain:grace) (signing:False) (SMBv1:True)
SMB         10.0.1.12       445    TINY             [*] Windows Server 2016 Datacenter 14393 x64 (name:TINY) (domain:tiny) (signing:False) (SMBv1:True)
SMB         10.0.1.13       445    PORFIRIO         [*] Windows Server 2016 Datacenter 14393 x64 (name:PORFIRIO) (domain:porfirio) (signing:False) (SMBv1:True)
SMB         10.0.1.11       445    GAYLORD          [*] Windows Server 2016 Datacenter 14393 x64 (name:GAYLORD) (domain:gaylord) (signing:False) (SMBv1:True)
SMB         10.0.1.10       445    GRACE            [-] grace\Administrator:Password2 STATUS_LOGON_FAILURE
SMB         10.0.1.12       445    TINY             [-] tiny\Administrator:Password2 STATUS_LOGON_FAILURE
SMB         10.0.1.100      445    AD               [*] Windows Server 2012 R2 Standard 9600 x64 (name:AD) (domain:corp.willenialpower.us) (signing:True) (SMBv1:True)
SMB         10.0.1.13       445    PORFIRIO         [-] porfirio\Administrator:Password2 STATUS_LOGON_FAILURE
SMB         10.0.1.11       445    GAYLORD          [-] gaylord\Administrator:Password2 STATUS_LOGON_FAILURE
SMB         10.0.1.100      445    AD               [+] corp.willenialpower.us\Administrator:[redacted] (Pwn3d!)
```

Figure 20: CrackMapExec SMB Spray

```
cmedb (ngpew)(smb) > creds

+Credentials---------+-----------+-----------+---------------+-----------+
| CredID | Admin On   | CredType  | Domain    | UserName      | Password  |
+--------+------------+-----------+-----------+---------------+-----------+
| 1      | 1 Host(s)  | plaintext | CORP      | Administrator | [redacted] |
| 2      | 1 Host(s)  | plaintext | TINY      | Administrator | [redacted] |
| 3      | 1 Host(s)  | plaintext | SPLASHY   | Administrator | [redacted] |
| 4      | 1 Host(s)  | plaintext | PORFIRIO  | Administrator | [redacted] |
| 5      | 1 Host(s)  | plaintext | GAYLORD   | Administrator | [redacted] |
| 6      | 1 Host(s)  | plaintext | GRACE     | Administrator | [redacted] |
+--------+------------+-----------+-----------+---------------+-----------+
```

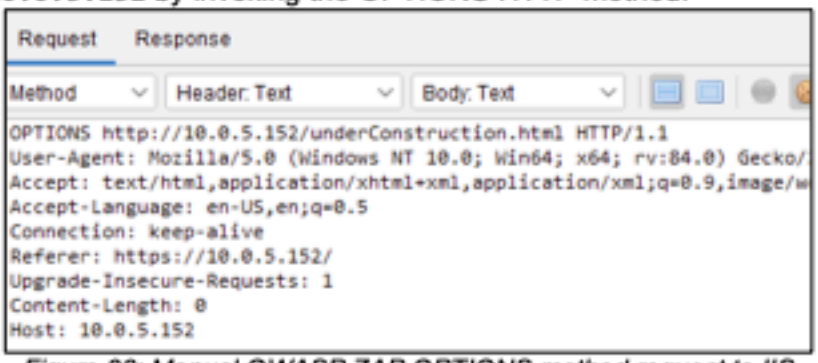
Figure 21: CrackMapExec database listing compromised credentials

[14] https://github.com/praetorian-inc/Hob0Rules/blob/master/wordlists/rockyou.txt.gz

[15] https://support.microsoft.com/en-us/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps

Compliance Violations	NERC CIP 7 R5.5.1 Password-only authentication length requirements are not met NERC CIP 7 R5.5.2 Password-only authentication complexity requirements are not met More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[16]

[16] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf

Critical - 04	Remote Code Execution via PUT HTTP Method	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	After recommending remediation during the first penetration testing engagement, [redacted] sought to verify that the previously outlined vulnerabilities have been mitigated. Once foothold was established, [redacted] discovered that the public-facing website, being developed with sensitive billing functionality for NGPEW's residential customers and vendors, retained the PUT HTTP method publicly enabled without authentication, which allows an attacker to upload arbitrary files to the web server and execute code on the system.	
Affected Scope	• Internet Information Services (TCP/80) ○ 10.0.5.152 (WEBSERVER)	
Business Impact	NGPEW's website is being developed to include billing functionality for its vendors and residential customers. The vulnerability allows an attacker to gain complete control over the IIS web server. A breach of integrity or confidentiality of the server risks causing significant financial and reputational damage to NGPEW and makes it subject to relevant laws and regulations governing the confidentiality of financial data.	
Exploitation Likelihood	Discovery of this vulnerability is trivial and automatic with common web application vulnerability scanners such as Nikto[17]. The IIS 4.0 version is vulnerable by default, exploit code is prevalent and included within popular penetration testing distributions such as Kali Linux, therefore exploitation is highly likely.	
Exploitation Details	[redacted] found the PUT method to be publicly allowed on NGPEW's web server running at `http://10.0.5.152` by invoking the OPTIONS HTTP method.  *Figure 22: Manual OWASP ZAP OPTIONS method request to IIS* The vulnerability was validated in the OPTIONS response body from IIS, showing that the PUT method is still accessible.	

[17] https://tools.kali.org/information-gathering/nikto

Figure 23: Manual OWASP ZAP OPTIONS method response from IIS

Once the vulnerability was validated, [redacted]s security analysts successfully uploaded an ASP payload[18] using OWASP ZAP with the PUT HTTP method, allowing remote code execution on the web server.

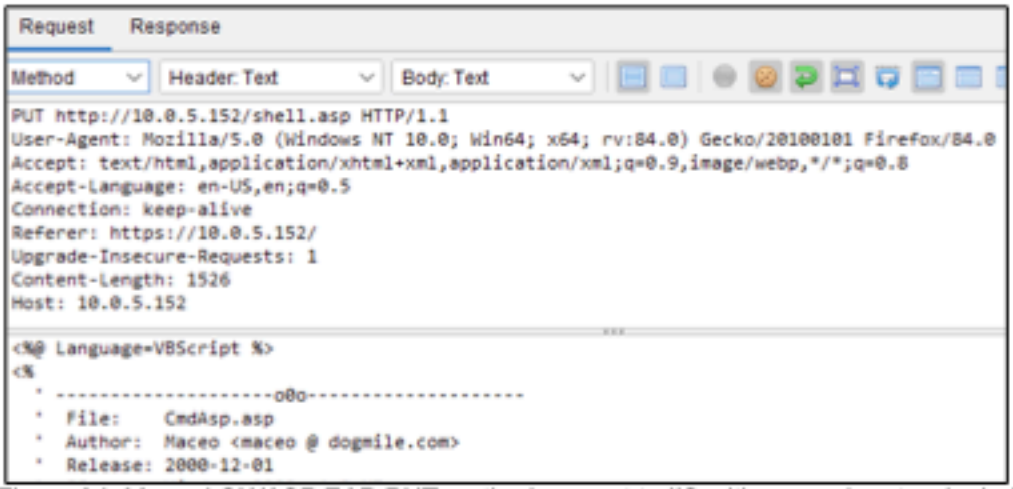


Figure 24: Manual OWASP ZAP PUT method request to IIS with a prominent web shell

[redacted]s security analysts confirmed exploitation by navigating to the URL of the uploaded ASP payload and issuing a "whoami" command to list the user it runs as.

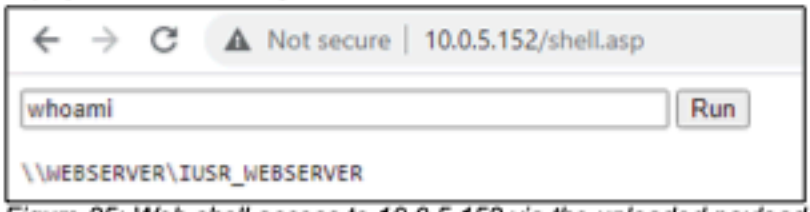


Figure 25: Web shell access to 10.0.5.152 via the uploaded payload

Remediation

[redacted]recommends NGPEW to deploy a more up-to-date version of Windows and IIS. Until an update is made, HTTP methods that allow modifications to the web server should be restricted. IIS versions older than 7.0 do not include request filtering functionality by default, therefore the UrlScan IIS tool should be used. UrlScan allows for HTTP requests to be rejected based on file extensions and HTTP methods on older versions of the IIS web server, such as the one running on 10.0.5.152.

[18] https://github.com/rutsky/cmdasp/blob/master/cmdasp.asp

	More information: Microsoft - URLScan Overview[19] Microsoft - Use Request Filtering[20]
Compliance Violations	CIP 7 R3.1 No method to deter, detect, or prevent malicious code More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[21]

[19] https://docs.microsoft.com/en-us/iis/extensions/working-with-urlscan/urlscan-overview
[20] https://docs.microsoft.com/en-us/iis/manage/configuring-security/use-request-filtering
[21] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

Critical - 05	Unauthenticated Access to Programmable Logic Controllers	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	[redacted] discovered that all Programmable Logic Controllers ("PLCs") on NGPEW networks did not require any form of authentication to access. [redacted] security analysts were able to connect to each of the PLCs using public networking tools and interact with systems.	

Affected Scope	• Programmable Logic Controllers (TCP/502)
	  ○ 10.0.1.198 (PLC-R-US-1)
	  ○ 10.0.1.199 (PLC-R-US-2)
	  ○ 10.0.1.200 (PLC-R-US-3)
	  ○ 10.0.1.201 (PLC-R-US-4)
	  ○ 10.0.1.202 (PLC-R-US-5)
	  ○ 10.0.1.203 (PLC-R-US-6)
	  ○ 10.0.10.57 (XF-PRI.02)
	  ○ 10.0.10.59 (XF-PRI-04)
	  ○ 10.0.10.60 (XF-RES-01)
	  ○ 10.0.10.61 (XF-RES-02)
	  ○ 10.0.10.62 (XF-SPRINGFIELD-01)
	  ○ 10.0.10.63 (XF-SUBMISSION-01)
	  ○ 10.0.10.64 (XF-SUBMISSION-02)
	  ○ 10.0.10.65 (XF-XMISSION-01)	

Business Impact	PLCs are a critical part of Industrial Control Systems. They provide real time data to Human Machine Interface applications, which are used to monitor the environments of key infrastructure and ensure the safety of employees and the public. [redacted] security analysts connected to each PLC and identified executable commands that could overwrite memory registers, dump firmware, and read memory registers. The execution of these commands could lead to memory corruption or aid an attacker in gathering sensitive information. Any kind of interface to these devices could result in the loss of life and highly impact the reputation of NGPEW.	
Exploitation Likelihood	[redacted] had to establish a foothold on the corporate network in order to gain access to the PLCs. Once on the network, it was trivial to gain access to each PLC with well-known networking tools. It is highly likely that an adversary could connect to these devices and issue commands that could severely damage the functionality of each PLC. Due to the sensitive nature of the PLCs and the risk they represent, testing was limited.	
Exploitation Details	[redacted] established a foothold in the corporate network using the steps described in finding Critical - 02. Once on the corporate network, [redacted] security analysts were able to download netcat[22] and QModMonitor[23] to the compromised host and connect to each PLC mentioned in scope.	

[22] http://netcat.sourceforge.net/
[23] https://sourceforge.net/projects/qmodmaster/

Netcat was used to connect to the devices located on the corporate network, as seen in Figure 26, and connections did not require any form of authentication. Once connected, [redacted] security analysts were able to interact with these devices by issuing commands.

```
PS C:\Users\tiny.glover\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : corp.millenialpower.us
   Link-local IPv6 Address . . . . . : fe80::395d:91b0:cf43:2906%12
   IPv4 Address. . . . . . . . . . . : 10.0.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.1

Tunnel adapter isatap.corp.millenialpower.us:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : corp.millenialpower.us
PS C:\Users\tiny.glover\Desktop> .\nc64.exe 10.0.1.198 8080


PLC DEBUG v0.1
[c] PLC-R-US 1994
=======================
1> READ CPU REG
2> READ STATE DEBUG
3> DUMP FIRMWARE
4> DUMP CONFIG
5> CHANGE SAVED PARAM
6> ENABLE DEV MODE
7> PRINT DEBUG LOG
=======================
CMD: 1

A: 5FE68F2D
B: FCD6734C
C: 8D73A2EA
D: D55623A5
E: F1213B33
X: 6D06B285
Y: 6E821498
Z: 491BC69D
```

Figure 26: Unauthenticated access to PLC's with netcat

QModMonitor was used to connect to the device located on the power network, As seen in Figure 27 . All connections did not require any authentication. Once connected, our analysts were able to interact with these devices by issuing commands.

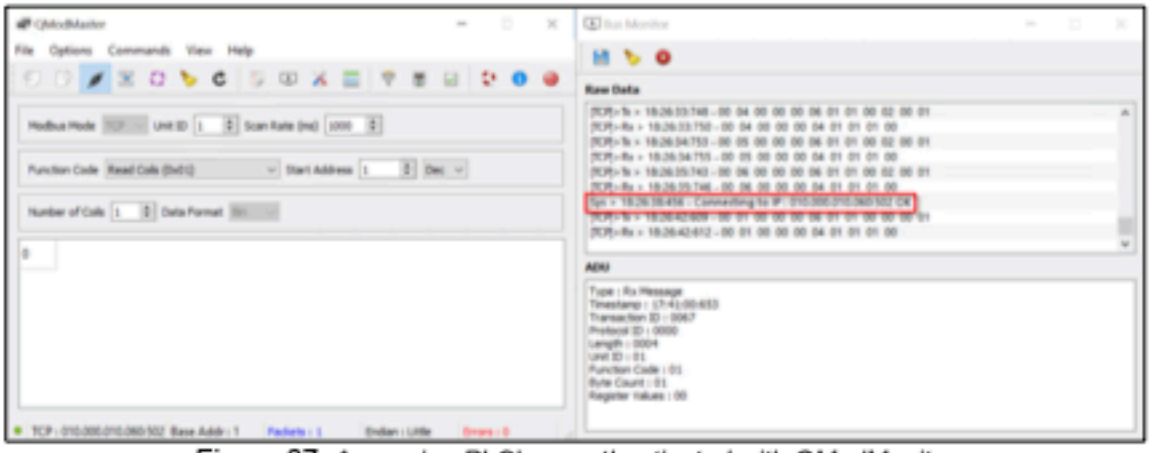


Figure 27: Accessing PLC's unauthenticated with QModMonitor

Remediation	[redacted] recommends NGPEW implement a form of industry accepted authentication[24] on each PLC in order to reduce the risk of unwanted access to business critical machines. The implemented form of authentication should provide secure sessions, session expiry, and require strong passwords. [redacted] also strongly encourages NGPEW to implement an air gapped environment specifically for the PLC devices. These environments should be completely disconnected or segmented from any network that does not need access to the PLCs. This can be accomplished by creating a bastion host, a server whose purpose is to provide access to a private network from an external network, with the sole purpose of managing business critical devices.
Compliance Violations	NERC CIP 5 R2.2 Interactive remote access sessions are not encrypted NERC CIP 5 R2.3 Multi factor authentication is no required for remote sessions More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf[25]

[24] https://us-cert.cisa.gov/sites/default/files/recommended_practices/RP_Managing_Remote_Access_S508NC.pdf
[25] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf

Critical - 06	Default MySQL Credentials for Billing Database	
Risk Assessment	**Impact: High**	**Likelihood: High**
Description	[redacted] discovered NGPEW's internal billing server to have an externally accessible MySQL database that authenticates with default database credentials. Root access credentials for the database can be found in the installation documentation of Kill Bill, an open-source billing application programming interface ("API") running on the system.	

Affected Scope	• MySQL (TCP/3306)
	  ○ 10.0.5.75 (KILLBILL)
	  ■ Account Affected
	  • root	

Business Impact	The database root account has ultimate control over the database, including the addition, modification, and deletion permissions. An attacker with such access would be able to view, edit and delete confidential billing information of NGPEW's vendors and residential clients. A compromise of NGPEW's billing database would cause catastrophic financial and reputational damage, as well as risk invoking laws and regulations governing financial records.	
Exploitation Likelihood	No exploit code is necessary for the successful exploitation of this vulnerability and the required credentials are listed in the vendor's documentation, making the exploitation of this vulnerability trivial.	

Exploitation Details	[redacted] identified an externally accessible MySQL database running on NGPEW's billing server and went on to research the documentation of the API being hosted on it. The Kill Bill API Getting Started" documentation page[26] lists the default credentials among its environment variables:
	`environment:`
	`  - KILLBILL_DAO_URL=jdbc:mysql://db:3306/killbill`
	`  - KILLBILL_DAO_USER=root`
	`  - KILLBILL_DAO_PASSWORD=[redacted]`
	`  - KILLBILL_CATALOG_URI=SpyCarAdvanced.xml`
	Figure 28: Kill Bill MySQL credentials listed in the documentation
	Figure 28 exhibits [redacted] connecting to the MySQL database, validating the vulnerability.	

[26] https://docs.killbill.io/latest/getting_started.html

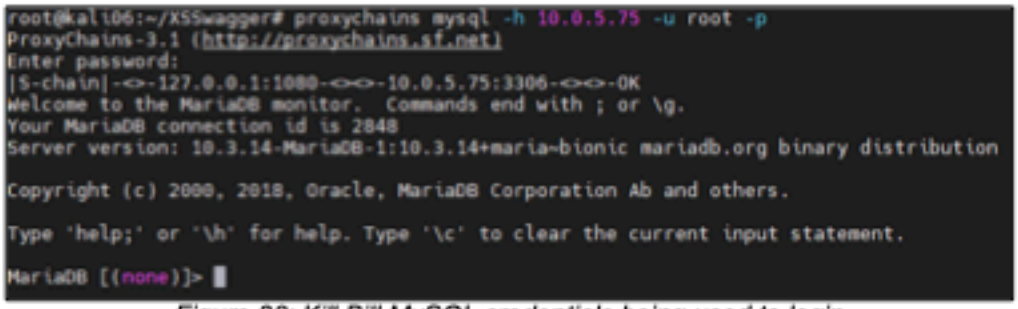


Figure 28: Kill Bill MySQL credentials being used to login

[redacted] confirmed full access to the billing database and tables designed to contain sensitive financial records and credit cards demonstrated below in Figure 29.

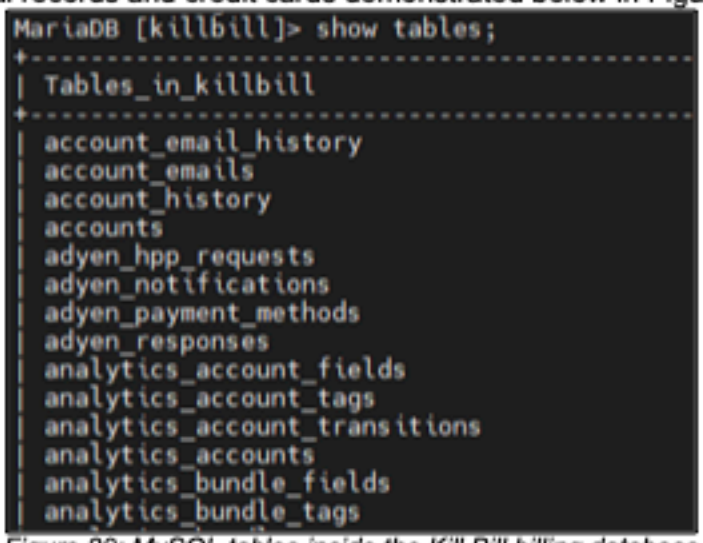
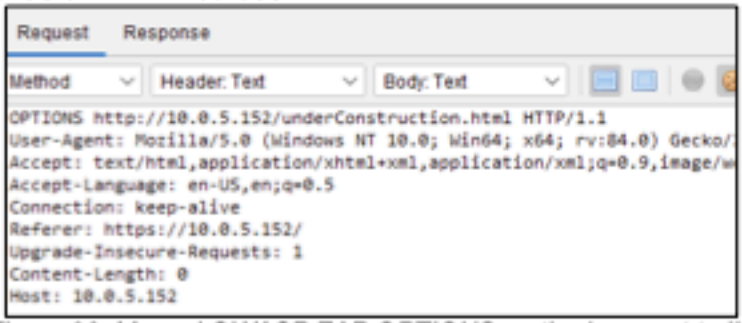


Figure 29: MySQL tables inside the Kill Bill billing database

Remediation	[redacted] recommends NGPEW to configure host-based firewall rules to deny connections to the MySQL database from systems that do not have a legitimate business need for it. In additio, database users need to be configured to have strong passwords and to be limited by the hosts they are allowed to connect from. External connections to the database as the root user are considered to be a bad security practice, therefore [redacted] recommends for external root logins to be disabled[27] and for the principle of least privilege to be applied. An API database user should only have the privileges necessary for its operation.
Compliance Violations	NERC CIP 7 R5.5 All known default passwords must be changed More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[28]

[27] https://www.networkinghowtos.com/howto/disable-remote-root-logins-into-mysql/
[28] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

HIGH FINDINGS

High - 01	Arbitrary File Deletion via DELETE HTTP Method	
Risk Assessment	**Impact: Medium**	**Likelihood: High**
Description	After recommending remediation during the first penetration testing engagement, [redacted] sought to verify that the previously outlined vulnerabilities have been mitigated. Upon gaining a foothold in the network, [redacted] discovered NGPEW's public-facing web server, which is being developed to include billing functionality, to still have the DELETE HTTP method publicly accessible. Its availability allows an attacker to arbitrarily remove files on the web server without authentication, jeopardizing its integrity.	
Affected Scope	• Internet Information Services (TCP/80) ○ 10.0.5.152 (WEBSERVER)	
Business Impact	The vulnerable website is currently under construction and is being developed to include billing functionality for NGPEW's residential customers and vendors. The vulnerability allows an attacker to remove arbitrary files on the server, leading to significant loss of integrity and availability. The potential destruction of billing functionality can have a significant adverse impact on NGPEW's operations.	
Exploitation Likelihood	The vulnerability is easily discoverable with common web application vulnerability scanners such as Nikto and doesn't require any exploit code, making its exploitation highly likely.	
Exploitation Details	[redacted] made an OPTIONS request to IIS with OWASP ZAP's manual request function to verify the available HTTP methods:  *Figure 30: Manual OWASP ZAP OPTIONS method request to IIS* The vulnerability was validated in the OPTIONS response body from IIS, showing the DELETE method to still be accessible.	

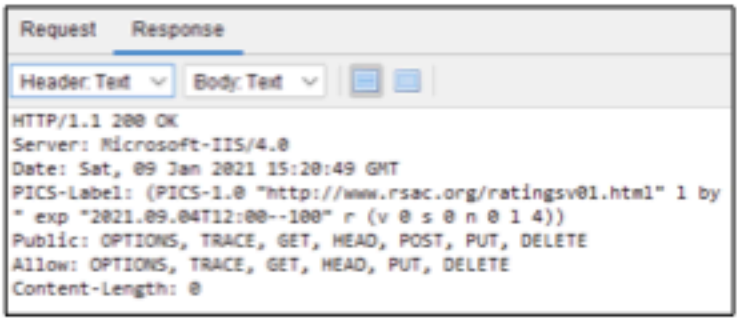


Figure 31: Manual OWASP ZAP OPTIONS method response from IIS

[redacted] created an empty test file on the web server with the PUT method and issued a manual DELETE HTTP request to its url with OWASP ZAP.

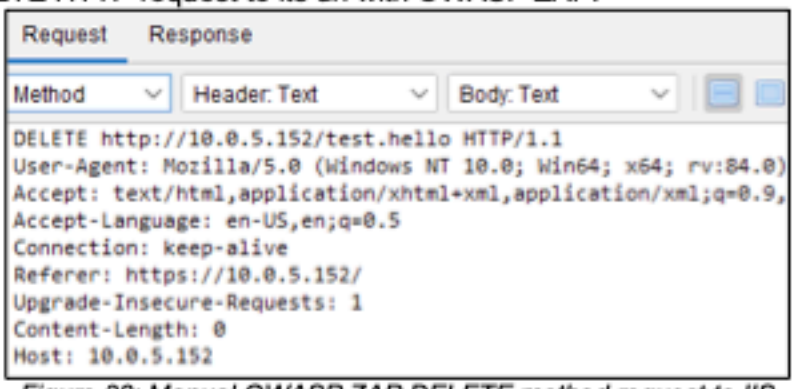


Figure 32: Manual OWASP ZAP DELETE method request to IIS

The vulnerability was validated with the IIS response confirming test file deletion.

Figure 33: Manual OWASP ZAP OPTIONS method response from IIS

Remediation

[redacted] recommends NGPEW to deploy a more up-to-date version of Windows and IIS. Until an update is made, HTTP methods that allow modifications to the web server should be restricted. IIS versions older than 7.0 do not include request filtering functionality by default, therefore the UrlScan IIS tool should be used. UrlScan[29] allows for HTTP requests to be rejected based on file extensions and HTTP methods on older versions of the IIS web server, such as the one running on 10.0.5.152.

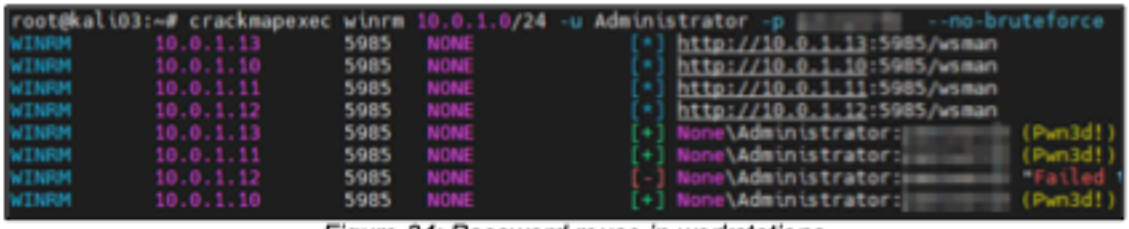
[29] https://docs.microsoft.com/en-us/iis/extensions/working-with-urlscan/urlscan-overview

Compliance Violations	CIP 7 R3.1 No method to deter, detect, or prevent malicious code More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[30]

[30] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

High - 02	Local Administrator Credential Reuse	
Risk Assessment	**Impact: Medium**	**Likelihood: High**
Description	Local administrator credentials were reused on workstations belonging to executives. This means that an attacker with knowledge of the reused password would be able to exploit multiple systems in NGPEW's network.	

Affected Scope	• Active Directory
	  ○ 10.0.1.10 (GRACE)
	  ○ 10.0.1.11 (GAYLORD)
	  ○ 10.0.1.13 (PORFIRIO)
	  ■ Account Affected
	  • Local Administrator	

Business Impact	Credential reuse allows an attacker to take over multiple systems on NGPEW's network with a single piece of credential information. After discovery of a credential, an attacker could password spray[31] and exploit similar vulnerable workstations across the network.	
Exploitation Likelihood	An attacker must discover the credential in use and workstations in NGPEW's infrastructure for this attack. An attack would be likely to retry credentials across NGPEW systems in an attempt to gain further access.	
Exploitation Details	This vulnerability as demonstrated in Figure 34 shows [redacted] security analysts using a discovered password across NGPEW hosts. This figure shows [redacted] successfully gained access to local administrative accounts running on these systems.  *Figure 34: Password reuse in workstations*	
Remediation	In order to improve password security posture, [redacted] recommends NGPEW to utilize Microsoft's Local Administrator Password Solution (LAPS)[32] to prevent local passwords from being duplicated on workstations. Local Administrator Password Solution a way to manage local administrative accounts and has the ability to change such passwords to a unique value, preventing reuse.	
Compliance Violations	N/A	

[31] https://www.coalfire.com/the-coalfire-blog/march-2019/password-spraying-what-to-do-and-how-to-avoid-it
[32] https://support.microsoft.com/en-us/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps

High - 03	Weak VNC Credentials on Web Server	
Risk Assessment	**Impact: High**	**Likelihood: Medium**
Description	After logging in with weak Local Administrator credentials, [redacted] enumerated the workstations and discovered an email conversation that contained credentials to a system hosting VNC. [redacted] was able to connect to the VNC session and gain access to the web server hosting NGPEW's public facing website.	

Affected Scope	• ThunderBird
	  ○ 10.0.1.12 (TINY)
	  ○ 10.0.1.13 (PORFIRIO)
	• VNC (TCP/5900)
	  ○ 10.0.1.152 (WEBSERVER)	

Business Impact	This vulnerability would allow an attacker to gain control over the system hosting the NGPEW public site. With this access, an attacker could deface or remove the site, which could lead to reputational damage, loss of public trust, and related loss of profits.	
Exploitation Likelihood	In order to conduct this attack, a threat actor would need to be on the same network as the web server in order to authenticate over VNC. Due to the weak VNC password, an attacker could brute force with a password list.	
Exploitation Details	[redacted] enumerated the Windows workstations and discovered emails listed under `%appdata%/roaming/Thunderbird/Profiles/aapxwams.default-release/Mail/Local Folders`.	

```
width=            =3D"100%" height=3D"100%" style=3D"min-width: 348px;" border=3D"0"
cellspacing=3D"0" cellpadding=3D"0" lang=3D"en">Hey Tiny I found a VNC server listening
internally that I think belongs to you? My team was able to bruteforce the VNC password being
"[redacted]" and got admin access to the system with the same password</body></html>
```

Figure 35: Email containing exposed plaintext credentials

The credential entered was a slight deviation from the password provided in the email. [redacted] used VNC Viewer to authenticate to the VNC Server.

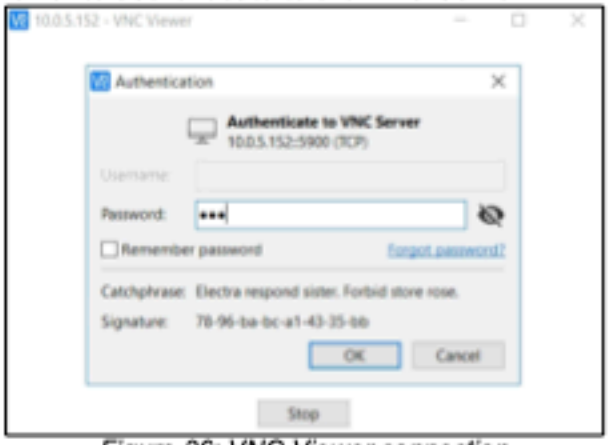


Figure 36: VNC Viewer connection

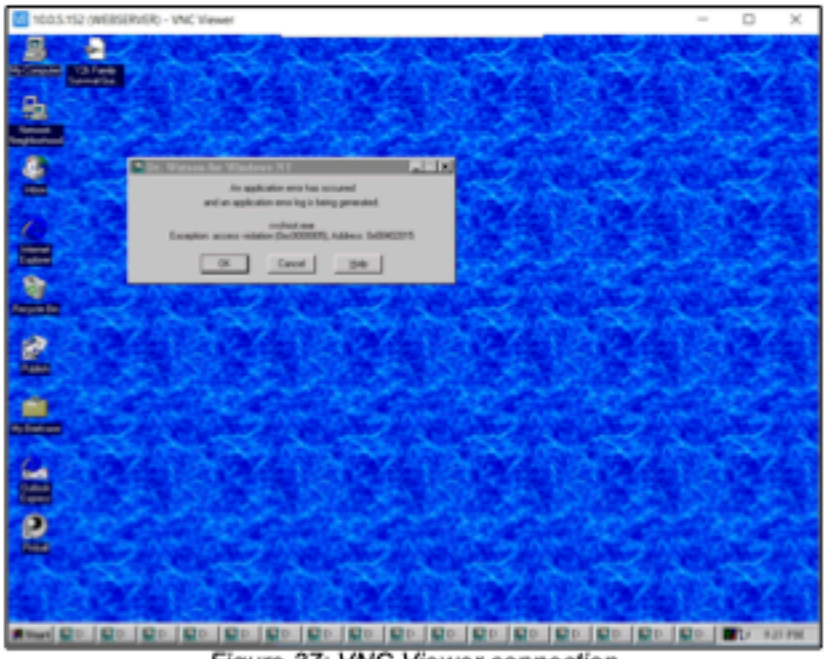


Figure 37: VNC Viewer connection

After authenticating, [redacted] had a graphical user interface on the web server.

Remediation	[redacted] recommends employees NGPEW mail servers to support IMAP and have employee inboxes set up to not synchronize subscribed folders. This fixes the issue of plaintext credentials stored on the system as well as ensure that ThunderBird does not store email contents by default. In addition, it is recommended that the web server does not run a VNC Server, but is instead remotely accessible only by Remote Desktop with Network Level Authentication enabled. Combined with an enforced password policy, this remediation will ensure that passwords are less vulnerable to brute forcing and overall improve NGPEW's security posture.
Compliance Violations	N/A

High - 04	Weak Root Credentials Leading to Database Compromise	
Risk Assessment	**Impact: High**	**Likelihood: Medium**
Description	[redacted] discovered weak root user credentials and password reuse amongst multiple networks within NGPEW. The root user was able to be accessed through port 22 which was running SSH. With access to the root user through SSH, [redacted] security analysts were able to gain access to the MySQL server within the `10.0.5.151` system. The MySQL server contained information disclosure which contained usernames, legal names, emails, and passwords of NGPEW employees.	

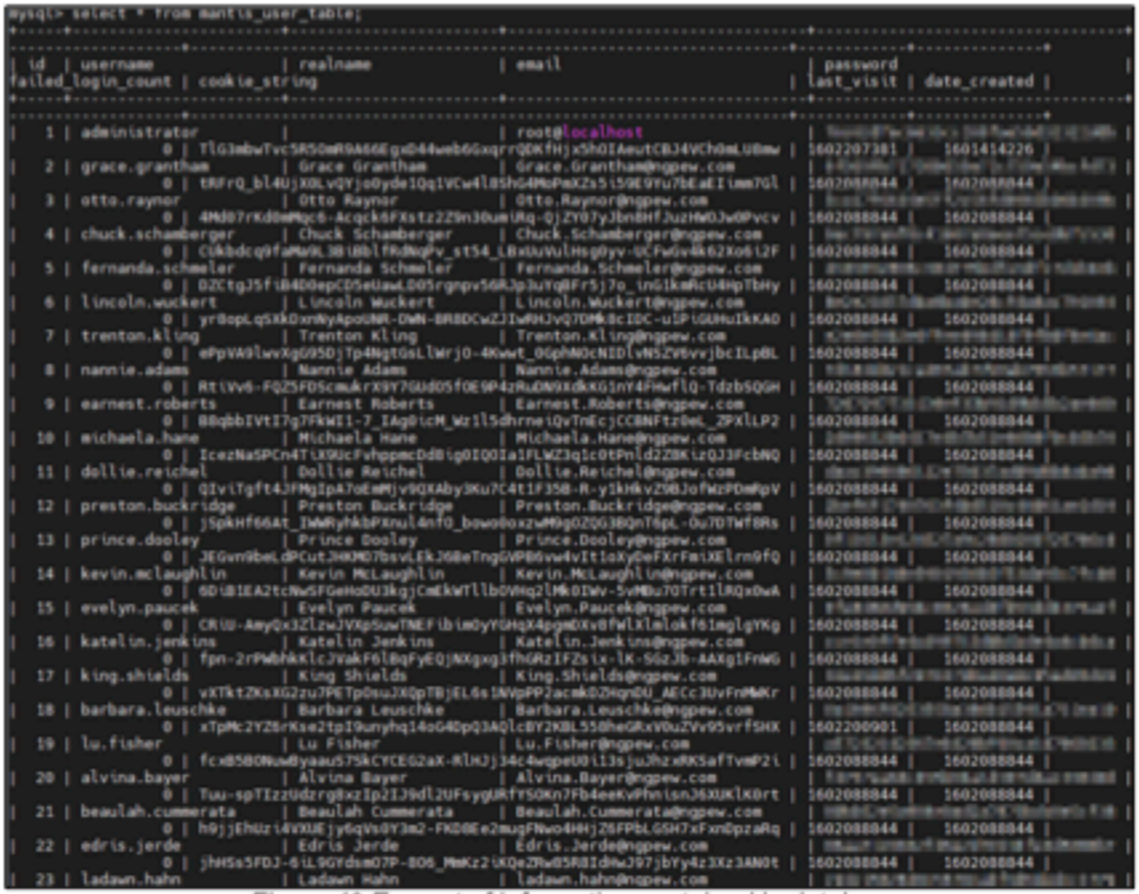
Affected Scope	• MySQL (TCP/3306)
	  ○ 10.0.5.151 (DB)
	• SSH (TCP/22)
	  ○ 10.0.5.151 (DB)
	  ▪ Account Affected
	  • root	

Business Impact	NGPEW's database which previously hosted Mantis Bug Tracker ("MantisBT") continued to maintain information regarding their employees despite MantisBT being offline during the time of [redacted] engagement. [redacted] gained the ability to fully compromise the MySQL database which withheld data from MantisBT and disclosed employee information such as usernames, emails, and passwords used for MantisBT. With such information disclosure, an attacker can use these usernames and passwords to attempt password reuse amongst NGPEW's network and gain further persistence. Moreover, since the password used to gain access into the system using SSH and MySQL does not meet NERC CIP password complexity requirements, NGPEW can face regulatory violations.	
Exploitation Likelihood	The password that was discovered by [redacted] is commonly found in weak password lists and should not be used anywhere within NGPEW's corporate network. Due to this, the likelihood of an attacker attempting weak password attempts amongst known usernames is fairly likely. Furthermore, with the `10.0.5.151` system acting as NGPEW's database, it may pose a bigger threat due to an attacker viewing a database as a high priority due to the possibility of obtaining information about employees and their credentials.	
Exploitation Details	[redacted] was able to utilize previously compromised passwords as seen in the High - 02 finding to gain access to MySQL and SSH on the `10.0.5.151` system. Within these findings, wordlists of common passwords were used amongst NGPEW employee accounts which led to successful login of accounts. Figures 38, 39, and 40, demonstrate initial access to SSH and MySQL, as well as information disclosure of NGPEW employees due to root MySQL access.	

Figure 38:Successful SSH access to NGPEW

```
root@db:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Figure 39: Access to mySQL database as root user

	 *Figure 40:Excerpt of information contained in database*
Remediation	The root password for the system as well as the MySQL database should meet complexity requirements. Since the `10.0.5.151` system was accessed using SSH, NGPEW can utilize SSH keys which provide a more secure way of logging into SSH than a password would. NGPEW can also utilize Pluggable Authentication Modules ("PAM")[33] and install additional modules, such as `libpam-cracklib` to enforce a specific password complexity amongst all users. Additionally, MySQL can utilize the `validate_password` plugin[34], which enforces all MySQL accounts to abide by a specific password policy put into place which can aid in strengthening MySQL accounts.
Compliance Violations	NERC CIP 7 R5.5.1 Password-only authentication length requirements are not met NERC CIP 7 R5.5.2 Password-only authentication complexity requirements are not met More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[35]

[33] https://www.techrepublic.com/article/how-to-force-users-to-create-secure-passwords-on-linux/
[34] https://dev.mysql.com/doc/refman/5.6/en/validate-password.html
[35] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

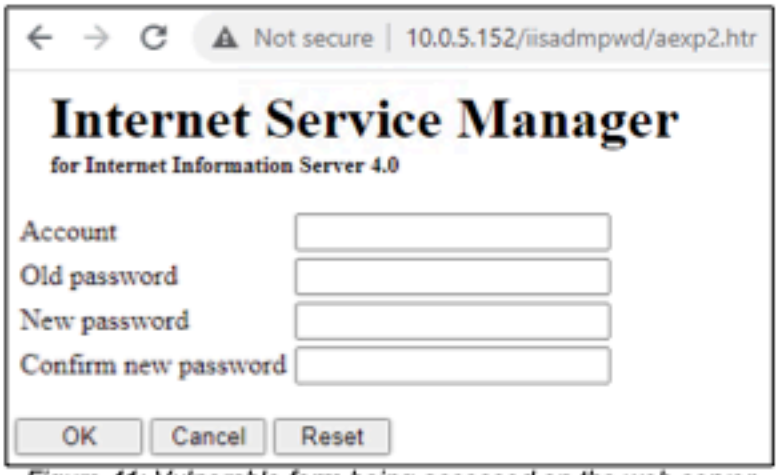
High - 05	Deprecated Password Reset Functionality	
Risk Assessment	**Impact: Medium**	**Likelihood: High**
Description	[redacted] discovered NGPEW's public-facing website to have sensitive deprecated IIS functionality accessible externally. This vulnerability provides external attackers with an ability to enumerate valid usernames and bruteforce passwords of local users on the web server. An attacker with valid credentials can use it to bypass local security policies that prevent a user from changing their own password, such as the case with locked accounts.	
Affected Scope	• Internet Information Services (TCP/80) ○ 10.0.5.152 (WEBSERVER)	
Business Impact	NGPEW's public-facing website is being developed to contain billing functionality for its vendors and residential customers. If thoroughly exploited, the vulnerability may lead to an attacker acquiring valid credentials to access the web server remotely, compromising the confidentiality, integrity and possibly availability of its sensitive business-critical system, causing financial and reputational damage.	
Exploitation Likelihood	The vulnerability requires no exploit code and plugins for major vulnerability scanners exist that detect it, making its exploitation highly likely.	
Exploitation Details	[redacted] was first alerted to the vulnerable file being accessible by a vulnerability scanner report shared by the NGPEW security team. [redacted] validated it by navigating to the file.  *Figure 41: Vulnerable form being accessed on the web server* [redacted] tested the available form with a non-existent account username and confirmed user enumeration to be possible due to the verbose error message:	

Figure 42: When an invalid username is submitted, a verbose error confirms it

When [redacted] gained access to the web server, it tested a valid username with a wrong password and confirmed password bruteforce to be possible due to the verbose error message and lack of rate limiting.

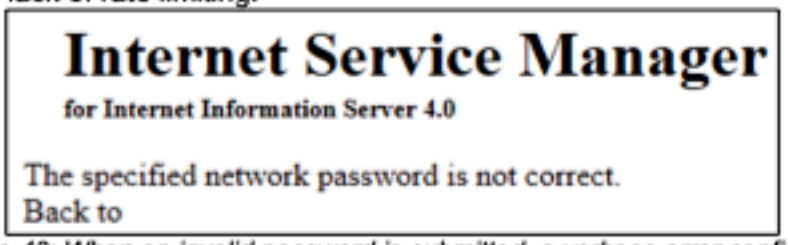


Figure 43: When an invalid password is submitted, a verbose error confirms it

Finally, valid credentials were tested against the form and the password was changed successfully.

Figure 44: When valid credentials are provided, the password is changed successfully

Remediation	[redacted] recommends NGPEW to deploy an up-to-date version of Windows and IIS, because the current versions running on 10.0.5.75 are end-of-life. Until an update is rolled out, the vulnerable files[36] "aexp2.htr", "aexp3.htr" and "aexp4.htr" should be removed from the "iisadmpwd" directory on the web server.
Compliance Violations	CIP 7 R3.1 No method to deter, detect, or prevent malicious code More Information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[37]

[36] https://securitytracker.com/id/1003756
[37] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

MEDIUM FINDINGS

Medium - 01	Weak SSH Server Configuration	
Risk Assessment	**Impact: High**	**Likelihood: Low**
Description	SSH is a network protocol that allows for remote login to a server. With the SSH server daemon ("SSHD") running on the system with weak security configurations, potential security issues can occur such as the ability for the root user to be logged into remotely through SSH, no account lockout policy which can lead to user accounts being brute forced, allow `X11Forwarding`, and not ignoring `Rhosts`.	
Affected Scope	• SSH (TCP/22) ○ 10.0.5.151 (DB)	
Business Impact	Weak SSH configuration can allow an attacker to attempt to log into any account on the system using passwords rather than SSH keys without the fear of accounts being locked out. If accounts are compromised due to weak SSH server configurations, user files and possible permissions to services may lead to information disclosure of employees / possible clients, as well as possible full system compromise if the root user is accessible.	
Exploitation Likelihood	The likelihood of an attacker exploiting a weak SSH server configuration is fairly low. Exploitation of a weak SSH server configuration heavily relies on poor password policy or previously compromised passwords.	
Exploitation Details	Weak SSH configurations can allow an attacker to attempt to log into any account on the system using only passwords as a source of authentication. Furthermore, weak configuration of SSH can allow the root user to be logged into remotely which can pose a security risk for the system. `PermitRootLogin` and `PasswordAuthentication` variables being enabled within the `sshd_config` file, an attacker can attempt to use a list of common passwords to gain access to the root user which would lead to a full compromise of the system. With the `PasswordAuthentication` variable, other user accounts on the system may be accessed through the same attack method of attempting to use common password lists to log in due to authentication being done through passwords rather than SSH keys. Figure 45 shows the `sshd_config` file found within the `10.0.5.151` system.	

Figure 45: sshd_config on 10.0.5.151 system

Remediation	[redacted] recommends implementing stronger SSH configurations within the sshd_config file by utilizing SSH key authentication, limiting the number of login attempts through the `MaxAuthTries` variable, disabling the root login by setting the `PermitRootLogin variable` to no, disabling `X11Forwarding`, and enabling `IgnoreRhosts`, NGPEW would have a highly secure SSH server and would greatly lower the attack surface of the SSH server.
Compliance Violations	NERC CIP 7 R5.5.1 Password-only authentication length requirements are not met

	NERC CIP 7 R5.5.2 Password-only authentication complexity requirements are not met More information: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf[38]

[38] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-007-5.pdf

Medium - 02	Unauthenticated Access to Dam API	
Risk Assessment	**Impact: High**	**Likelihood: Low**
Description	The API for the microgrid controller which can set and receive parameters for power generation systems was accessible from anywhere in the power and service networks without authentication.	
Affected Scope	• Werkzeug (TCP:80) ○ 10.0.10.15 (MICROGRID)	
Business Impact	Attackers could use the functionality to modify the expected metrics for power generation systems, triggering alarm systems or allowing power generation to exceed safe levels, endangering workers or causing damage to NGPEW equipment.	
Exploitation Likelihood	To exploit this vulnerability, an attacker would need to be on either the services or power network, making it less likely to be exploited.	
Exploitation Details	When navigating to the IP address in a web browser, a JSON object was returned that included metrics for all power systems, as shown in figure 46.  *Figure 46: JSON returned when visiting 10.0.10.15* A packet capture was taken from the HMI that revealed the format of the POST request.	

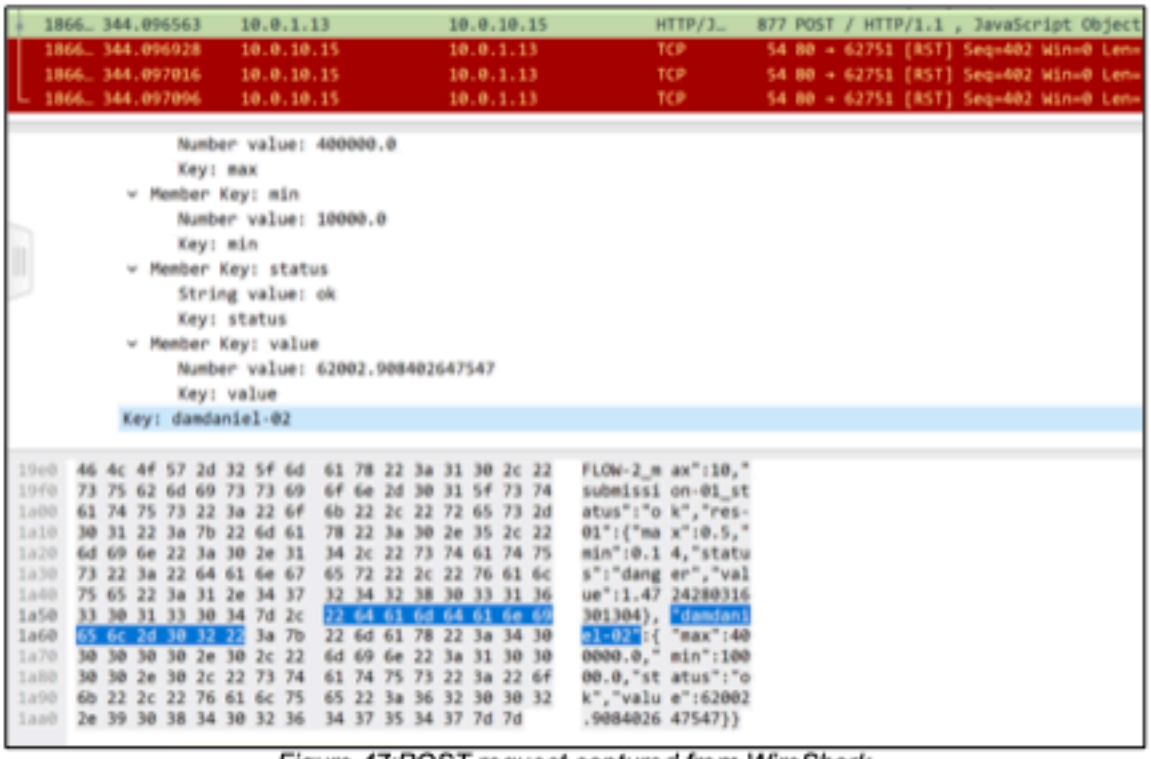


Figure 47:POST request captured from WireShark

Figure 48: TCP stream captured by WireShark

Remediation	API requests should be secured with API tokens and HTTPS. Network access to the API endpoint could be restricted to only authorized IP addresses for additional security.
Compliance Violations	N/A

LOW FINDINGS

Low - 01	Unencrypted Authentication on Rocket.Chat	
Risk Assessment	**Impact: Low**	**Likelihood: Low**
Description	[redacted]s security analyst visited the Rocket.Chat communication platform and upon connection discovered it was not using Hypertext Transfer Protocol Secure ("HTTPS") to secure its login page.	

Affected Scope	• Rocket.Chat (TCP/80)
	  ○ 10.0.1.154 (MAXWELL)
	  ■ Affected Users
	  • Rocket.Chat Users	

Business Impact	Due to this platform requiring employees to login over an unencrypted HTTP connection, it's possible for an attacker to steal that plaintext traffic. The unencrypted HTTP traffic could contain usernames and passwords which could be leveraged to further compromise the NGPEW network. Further, it could also be possible for an attacker to view unencrypted messages or transcripts that could contain sensitive information and intellectual property.	
Exploitation Likelihood	The exploitation of this vulnerability would require a threat actor to maintain prolonged access to the network while performing man in the middle attacks on HTTP traffic. Due to the complex setup of man in the middle attacks and the need to maintain anonymous access on the network, this vulnerability is considered unlikely to be exploited.	
Exploitation Details	[redacted]isited Rocket.Chat at `http://10.0.1.154:3000/home`, as seen in Figure 49, and encountered a login page without HTTPS support.  *Figure 49: Login page without HTTPS*	

Remediation	Enable support for HTTPS connections using secure cipher suites and disable support for HTTP. If the server is internet facing, an SSL certificate can be obtained using CertBot[39] from the EFF, and if not, one can be created using a local certificate authority.
Compliance Violations	N/A

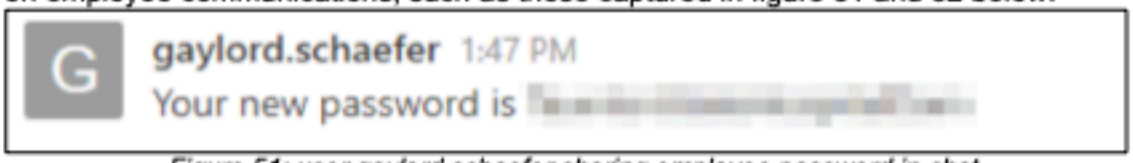
[39] https://certbot.eff.org/

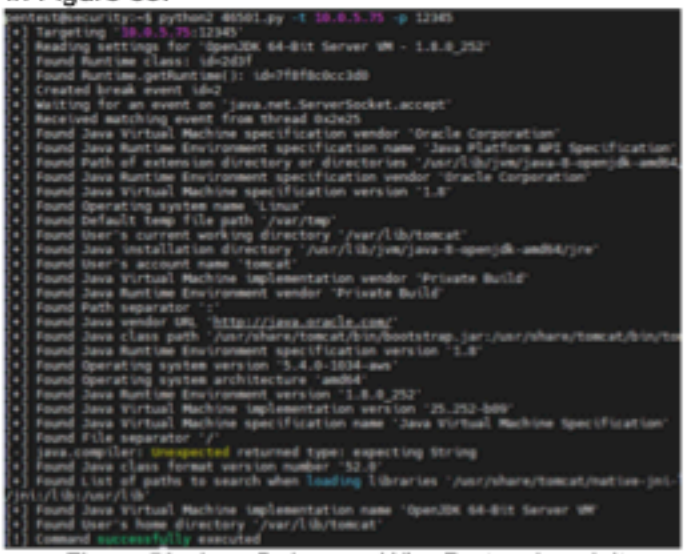
Low - 02	Insecure Server Message Block Service	
Risk Assessment	**Impact: Low**	**Likelihood: Low**
Description	SMB version 1 is a protocol that has been deprecated since 2014 and is considered to be obsolete and insecure. [redacted] security analysts identified instances of systems running with SMBv1 as well as SMB signing disabled. The lack of signing leaves SMB communications vulnerable to man-in-the-middle attacks, as well as an NTLM relay attack[40].	
Affected Scope	• SMBv1/v2 (TCP/139) ○ 10.0.1.10 (GRACE) ○ 10.0.1.11 (GAYLORD) ○ 10.0.1.12 (TINY) ○ 10.0.1.13 (PORFIRIO) ○ 10.0.1.100 (AD)	
Business Impact	An NTLM relay attack could be used to aid an attacker in compromising user hashes and potentially allow for lateral movement. With this access, an attacker could view sensitive information on NGPEW workstations.	
Exploitation Likelihood	To exploit this vulnerability, an attacker would need to be on the local network and to have redirected the traffic in a way that can be intercepted. It is unlikely that this would be executed without the attacker first gaining a significant foothold in the network.	
Exploitation Details	[redacted]s security analysts ran CrackMapExec[41] and discovered that NGPEW systems were utilizing SMBv1 and had signing disabled. Figure 50 contains the output showing NGPEW's SMB settings.  *Figure 50: SMB responses from CrackMapExec*	
Remediation	SMB signing can be enabled through group policy, and SMBv1/2 can be disabled[42] via a registry change through group policy. If SMB is a required service for NGPEW, [redacted] recommends that the servers run the latest version of SMB where possible.	
Compliance Violations	N/A	

[40] https://www.qomplx.com/qomplx-knowledge-ntlm-relay-attacks-explained/
[41] https://github.com/byt3bl33d3r/CrackMapExec
[42] https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

Low - 03	Password Disclosure on Rocket.Chat	
Risk Assessment	**Impact: Low**	**Likelihood: Low**
Description	Plaintext passwords were disclosed on public employee channels in Rocket.Chat	

Affected Scope	• Rocket.Chat (TCP/80)
	  ○ 10.0.1.154 (MAXWELL)
	  ■ Affected Users
	  • marcelino.pacocha	

Business Impact	Leaked passwords could allow access to company email and user accounts, leading to the disclosure of business documents or compromised access to workstations.	
Exploitation Likelihood	The likelihood of exploitation is low, as access to the internal Rocket.Chat server is required to see the communications and new registrations are currently disabled.	
Exploitation Details	[redacted] security analysts discovered that NGPEW Rocket Chat registration was disabled following the recommendations of the first penetration testing engagement. [redacted] analysts obtained domain credentials with Critical-2 and logged in to eavesdrop on employee communications, such as those captured in figure 51 and 52 below.  *Figure 51: user gaylord.schaefer sharing employee password in chat*  *Figure 52:user gaylord.schaefer sharing user marcelino.pacocha's password*	
Remediation	A clear standard should be put into place for issuing credentials to new users. One time use passwords should be distributed to new users by an automated system and through a secure channel, such as encrypted email.	
Compliance Violations	N/A	

Low - 04	Exposed Java Debugger Wire Protocol	
Risk Assessment	**Impact: Low**	**Likelihood: Medium**
Description	[redacted] discovered an exposed Java Debug Wire Protocol ("JDWG") port which a persistent attacker can utilize to gather intelligence on the underlying system.	
Affected Scope	• Java Debug Wire Protocol (TCP/12345) ○ 10.0.5.75 (KILLBILL)	
Business Impact	[redacted]s testing of JDWG yielded system information that can be found in Figure 53. A persistent attacker with additional time and better understanding of the application may be able to remotely execute commands on the affected system and affect the underlying billing system critical to NGPEW's operations.	
Exploitation Likelihood	Metasploit provides a trivial module that an attacker can use against JDWG for this exploit. However, the exploit is unreliable, therefore command execution is not guaranteed.	
Exploitation Details	[redacted] identified the affected server running Java Debug Wire Protocol and discovered public exploit code[43] to abuse this vulnerability. [redacted] was not able to gain full remote code execution but was still able to gather additional information about the system as shown in Figure 53.  *Figure 53: Java Debugger Wire Protocol exploit*	
Remediation	[redacted] recommends disabling access to debug functionality in production systems, as well as implementing host-based firewalls that limit external connectivity to only that which is business critical	
Compliance	NERC CIP 7 R3.1	

[43] https://www.exploit-db.com/exploits/46501

Violations	No method to deter, detect, or prevent malicious code

INFORMATIONAL FINDINGS

Info - 01	Enabled Guest Accounts	
Risk Assessment	**Impact: N/A**	**Likelihood: N/A**
Description	The built in Windows Guest account is enabled across all machines.	

Affected Scope	• Windows Machines
	  ○ 10.0.1.10 (GRACE)
	  ○ 10.0.1.11 (GAYLOAD)
	  ○ 10.0.1.12 (TINY)
	  ○ 10.0.1.13 (PORFIRIO)
	  ○ 10.0.1.100 (AD)
	  ○ 10.0.1.152 (WWW)	

Business Impact	Although the Guest account should have less privileges than a regular user, having the account enabled could increase the attack surface of all machines. If a Guest account is misconfigured or granted more privileges than needed then a potential vulnerability can be introduced into the environment.	
Exploitation Likelihood	N/A	
Exploitation Details	As Figure 54 shows, running the command `net user Guest` shows that the Guest account is currently active and allowed on the workstation.	

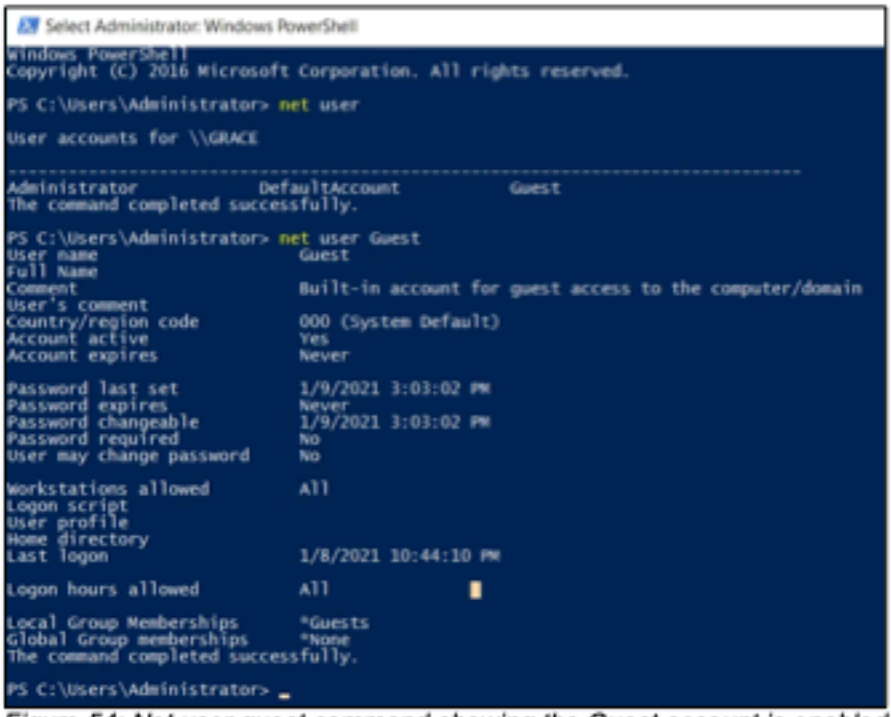


Figure 54: Net user guest command showing the Guest account is enabled

Remediation	Disable or restrict privileges for all Guest accounts. Privileges that should be restricted include installing software and changing networking permissions.
Compliance Violations	N/A

Info - 02	Exposed Rocket.Chat Version number	
Risk Assessment	**Impact: N/A**	**Likelihood: N/A**
Description	Querying the Rocket.Chat API as an unauthenticated user allows for version enumeration.	
Affected Scope	• Rocket.Chat (TCP/80) ○ 10.0.1.154 (MAXWELL)	
Business Impact	The exposed Rocket.Chat version makes it possible for an adversary to identify any publicly known exploits that the current version could be vulnerable to.	
Exploitation Likelihood	N/A	
Exploitation Details	Making an HTTP GET request against `http://10.0.1.154/api/info`, as seen in Figure 55, returns the software version number of the running Rocket.Chat service.  *Figure 55: Get request* returns Rocket.Chat version number	
Remediation	Remove the Rocket.Chat version from the source code or require authentication for request against the API endpoint.	
Compliance Violations	N/A	

APPENDIX A: OSINT ARTIFACTS

Prior to the engagement, [redacted] performed OSINT on the open internet for NGPEW as part of the Intelligence Gathering phase. [redacted] identified artifacts that included sensitive information on NGPEW systems and employees which have been detailed in this appendix. [redacted] has provided additional details with recommendations on steps ensuring NGPEW's online presence does not compromise its security posture.

Employee Information Disclosure

Figure 56: Employee Information Disclosure

Details

Information on an employee of NGPEW was discovered on an online site[44] for sharing private or identifiable information about individuals. This information includes the employee's title, address as well as credentials for both personal and work email addresses. This information could provide an adversary additional information about NGPEW's password policy and an employee to target. Although [redacted] was not able to find any instances of the employee's credentials on the NGPEW network, it is critical that NGPEW change employee passwords that have been exposed.

Recommendation

[redacted] recommends NGPEW to consult its legal team and request a takedown of the offending information. Additionally, [redacted] recommends that the employee is informed of the information disclosure and that the employee's accounts have password changes immediately.

[44] https://doxbin.org/upload/hoseaziemepowercompanydirector/

Exposed Internal Organization Chart

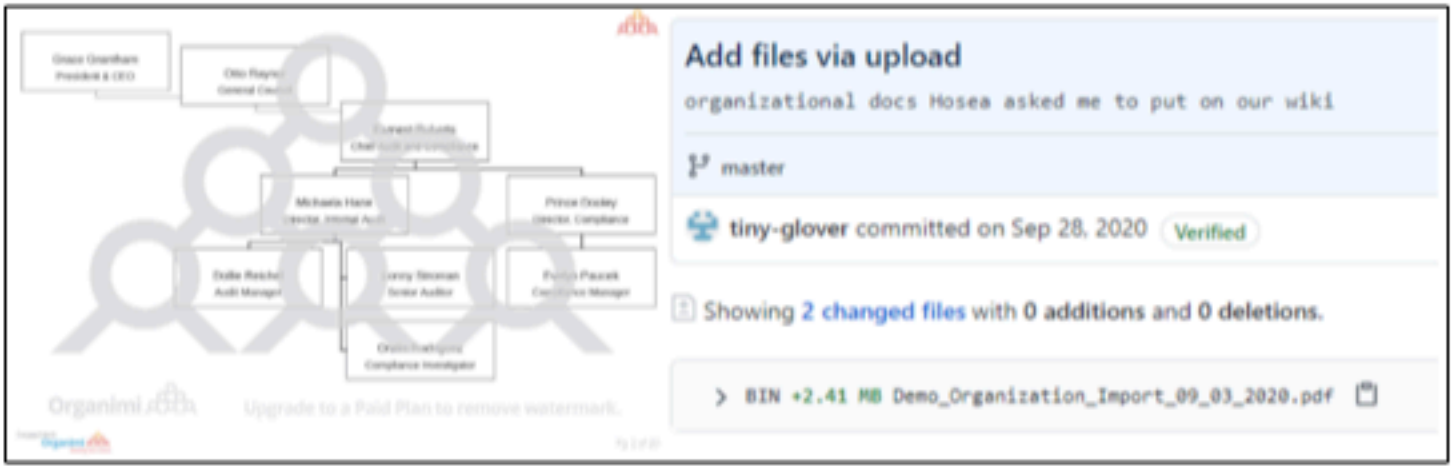


Figure 57: GitHub commit by tiny-glover containing NGPEW's organizational chart

Details

[redacted] discovered NGPEW's proprietary organizational structure containing full names and job titles of all its employees on the publicly available GitHub repository [45] during open source intelligence collection in October of 2020. GitHub commits indicate that the organizational chart was made public on September 28th, 2020. This proprietary document may provide attackers with unprecedented visibility into the organizational structure of NGPEW, which they can leverage to impersonate or target individuals within it. NGPEW was notified of this finding following [redacted]'s first penetration testing engagement and removed the files from the GitHub repository on December 22, 2020. Since GitHub provides version control by design, the documents are still accessible in the commit history, which is publicly available despite the files being removed.

Recommendation

[redacted] recommends NGPEW to consult GitHub documentation[46] on removing sensitive data from a repository. NGPEW may achieve that by using either built-in Git commands or the open-source BFG Repo-Cleaner[47] tool. Additionally, [redacted] recommends NGPEW to secure proprietary documents such as organizational charts within its intranet and apply the principle of least privilege, where only authorized employees can request and view the data.

[45] https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/Demo_Organization_Import_09_03_2020.pdf
[46] https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/removing-sensitive-data-from-a-repository
[47] https://github.com/rtyley/bfg-repo-cleaner

Exposed Grid Network Diagram

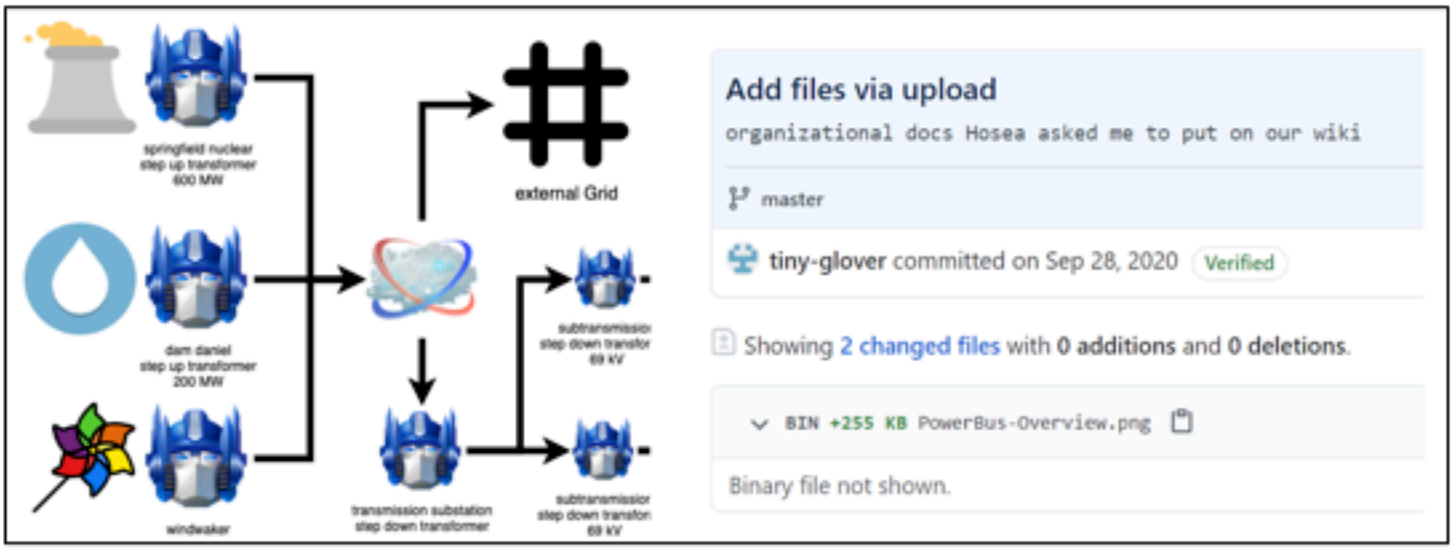


Figure 58: Internal Grid Diagram From a Public Employee Repository

Details

[redacted] identified that NGPEW's infrastructure diagrams are currently available publicly on the official NGPEW GitHub site[48]. These documents which are proprietary and confidential in nature provide an attacker vital insight into NGPEW's critical infrastructure. The diagram provided in Figure 58 can be leveraged by an attacker to discover vulnerabilities in NGPEW's grid network. NGPEW was notified of this finding following [redacted]'s first penetration testing engagement and removed the files from the GitHub repository on December 22, 2020. Since GitHub provides version control by design, the documents are still accessible in the commit history, which is publicly available despite the files being removed.

Recommendation

[redacted] recommends NGPEW to consult GitHub documentation[49] on removing sensitive data from a repository. NGPEW may achieve that by using either built-in Git commands or the open-source BFG Repo-Cleaner[50] tool. Additionally, [redacted] recommends NGPEW to secure proprietary documents such as grid network diagrams within its intranet and apply the principle of least privilege, where only authorized employees can request and view the data.

[48] https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/PowerBus-Overview.png
[49] https://docs.github.com/en/free-pro-team@latest/github/authenticating-to-github/removing-sensitive-data-from-a-repository
[50] https://github.com/rtyley/bfg-repo-cleaner

Improve GitHub Organization Approval Process

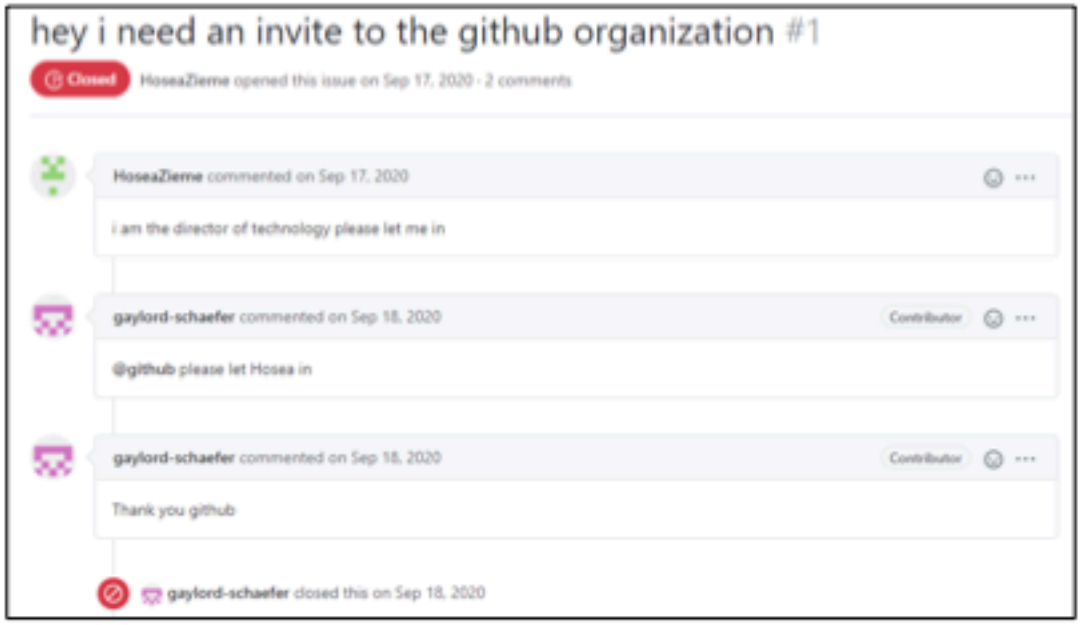


Figure 59: Comments requesting for invite on NGPEW GitHub Issue

Details

[redacted] identified a closed issue on the NGPEW GitHub site[51] under the home repository. In the Figure 59 listed above, user HoseaZieme is given an invite to the NGPEW GitHub organization after posting a comment stating his role as "director of technology". Without a formal process of approval, a threat actor could impersonate an employee and gain access to sensitive information stored on the internal GitHub organization.

Recommendation

[redacted] recommends NGPEW improve the approval process for gaining access into the internal GitHub organization. An employee must be authorized for access and confirmation of GitHub usernames should be verified through internal communication before an employee is given an invitation to the GitHub organization. With a fully documented process, NGPEW will be able to identify attempts of social engineering and improve security posture.

[51] https://github.com/Next-Generation-Power-and-Water/home/issues/1

APPENDIX B: Network Diagram

During the assessment, [redacted] identified the following hosts, services, and corresponding ports in the NGPEW internal network, as listed in the figures below:

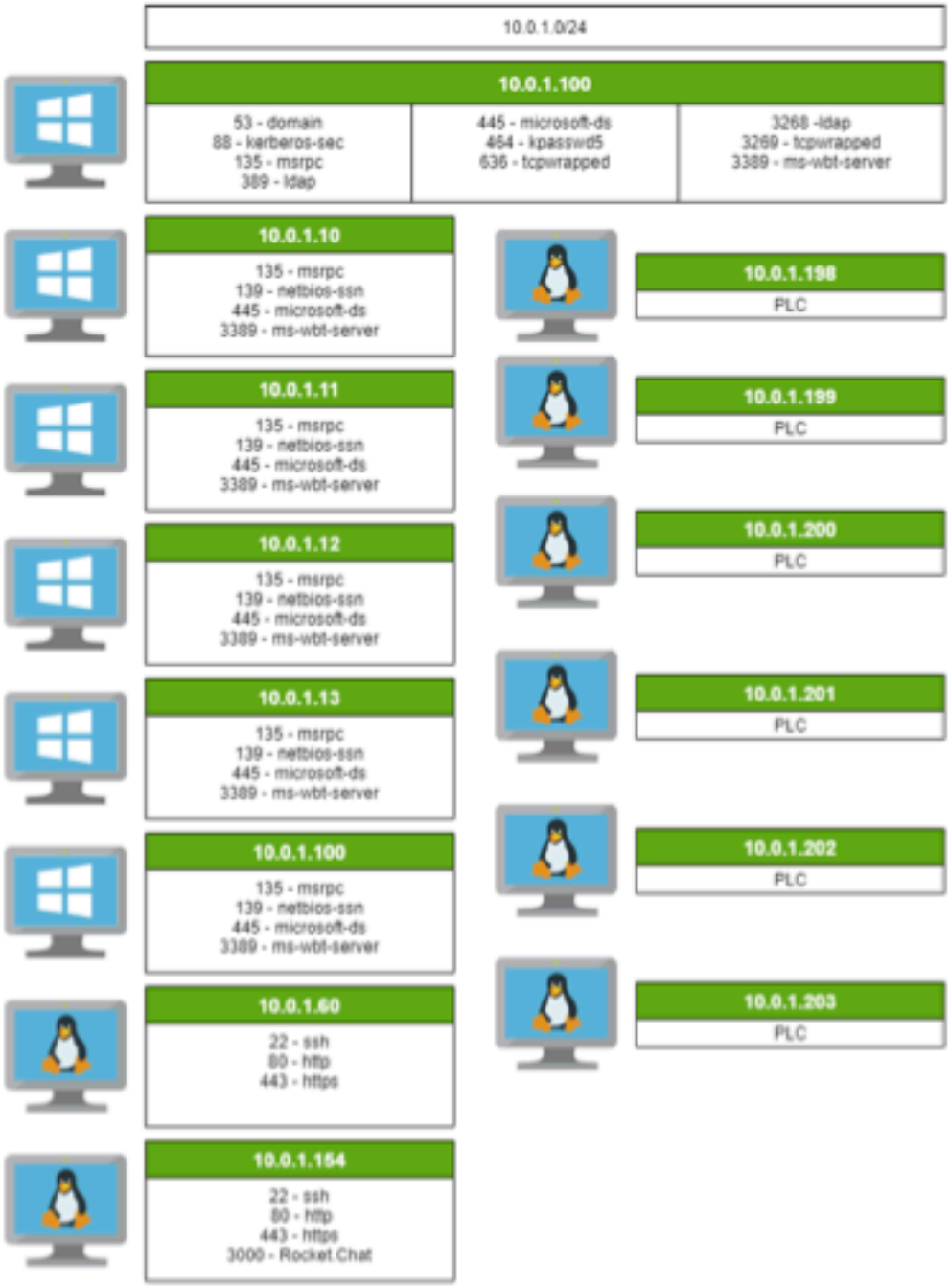


Figure 60: Visualized scan on ports on NGPEW 10.0.1.0/24 network

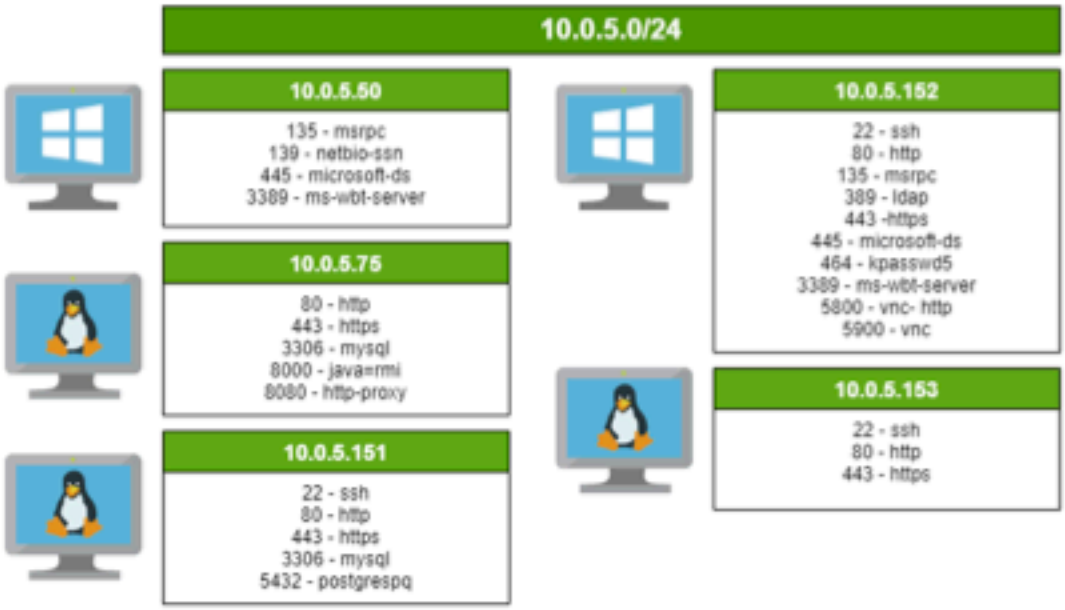


Figure 61: Visualized scan on ports on NGPEW 10.0.5.0/24 network

Figure 62: Visualized scan on ports on NGPEW 10.0.10.0/24 network

APPENDIX C: Tools

Although [redacted] uses a broad toolset, there are 3 main tools that [redacted] used to assist in this assessment.

nVis

A lightweight red teaming platform utilizing concurrent nmap scans to populate a collaborative web server. This tool was developed by [redacted] for the purposes of short term engagements or penetration testing competitions.

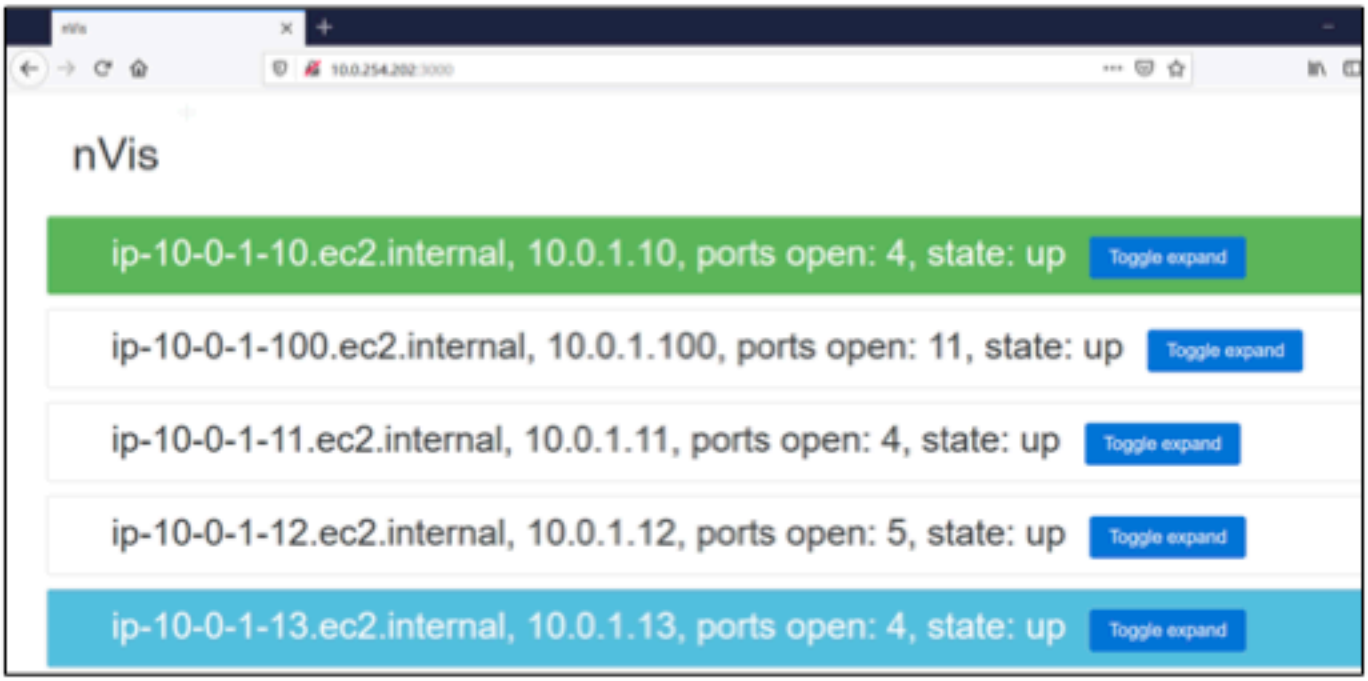


Figure 63: nVis showing number of hosts and number of ports open

Users are able to color code IP's according to the status of engagement (in progress, checked or compromised, and needs further investigation). Having these features allows quicker scans and helps reduce redundant work being done during the scanning and exploitation phases. The framework is available for download from on GitHub[52].

Burp Suite

Burp Suite ("Burp"[53]) is an integrated platform for performing security testing of web applications. Its platform allows for initial mapping and analysis of an application's attack surface.

[52] https://github.com/Menn1s/nVis
[53] https://portswigger.net/burp

OWASP ZAP

Open Web Application Security Project Zed Attack Proxy ("OWASP ZAP"[54]) is an open-source web application vulnerability scanner, which includes an intercepting proxy that allows its user to manipulate HTTP traffic.

APPENDIX D: NERC Penalty Financial Analysis

Through publicly available data[55] regarding enforcement actions taken by NERC[redacted]conducted a statistical analysis of fines issues in the years 2009 through 2019. For the purposes of this analysis, the dataset was restricted to enforcement actions that resulted in a financial penalty, and excludes enforcement actions that resulted in a financial penalty of zero dollars, financial penalties that were paid through a settlement, and financial penalties that were only available through the Notice of Penalty(NOP). The data was retrieved from the NERC website on October 23, 2020.

Average NERC Penalty

Average of All Penalties	$ 311,850.71
Average Penalty in 2019	$ 1,709,000.00
Average Penalty in 2018	$ 427,900.00
Average Penalty in 2017	$ 194,777.78
Average Penalty in 2016	$ 300,466.67
Average Penalty in 2015	$ 1,604,545.45
Average Penalty in 2014	$ 881,465.52
Average Penalty in 2013	$ 101,879.31
Average Penalty in 2012	$ 111,133.79
Average Penalty in 2011	$ 71,592.24
Average Penalty in 2010	$ 21,762.16
Average Penalty in 2009	$ 6,250.00

Figure 64: Average NERC penalty by year

Median NERC Penalty

Median of all penalties	$ 59,750.00
Median Penalty in 2019	$775,000.00
Median Penalty in 2018	$ 190,000.00
Median Penalty in 2017	$ 201,000.00
Median Penalty in 2016	$ 142,000.00
Median Penalty in 2015	$ 160,000.00
Median Penalty in 2014	$ 109,000.00
Median Penalty in 2013	$ 97,500.00

[54] https://owasp.org/www-project-zap/
[55] https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx

Median Penalty in 2012	$ 71,000.00
Median Penalty in 2011	$ 20,000.00
Median Penalty in 2010	$ 10,000.00
Median Penalty in 2009	$ 6,250.00

Figure 65: Median NERC penalty by year

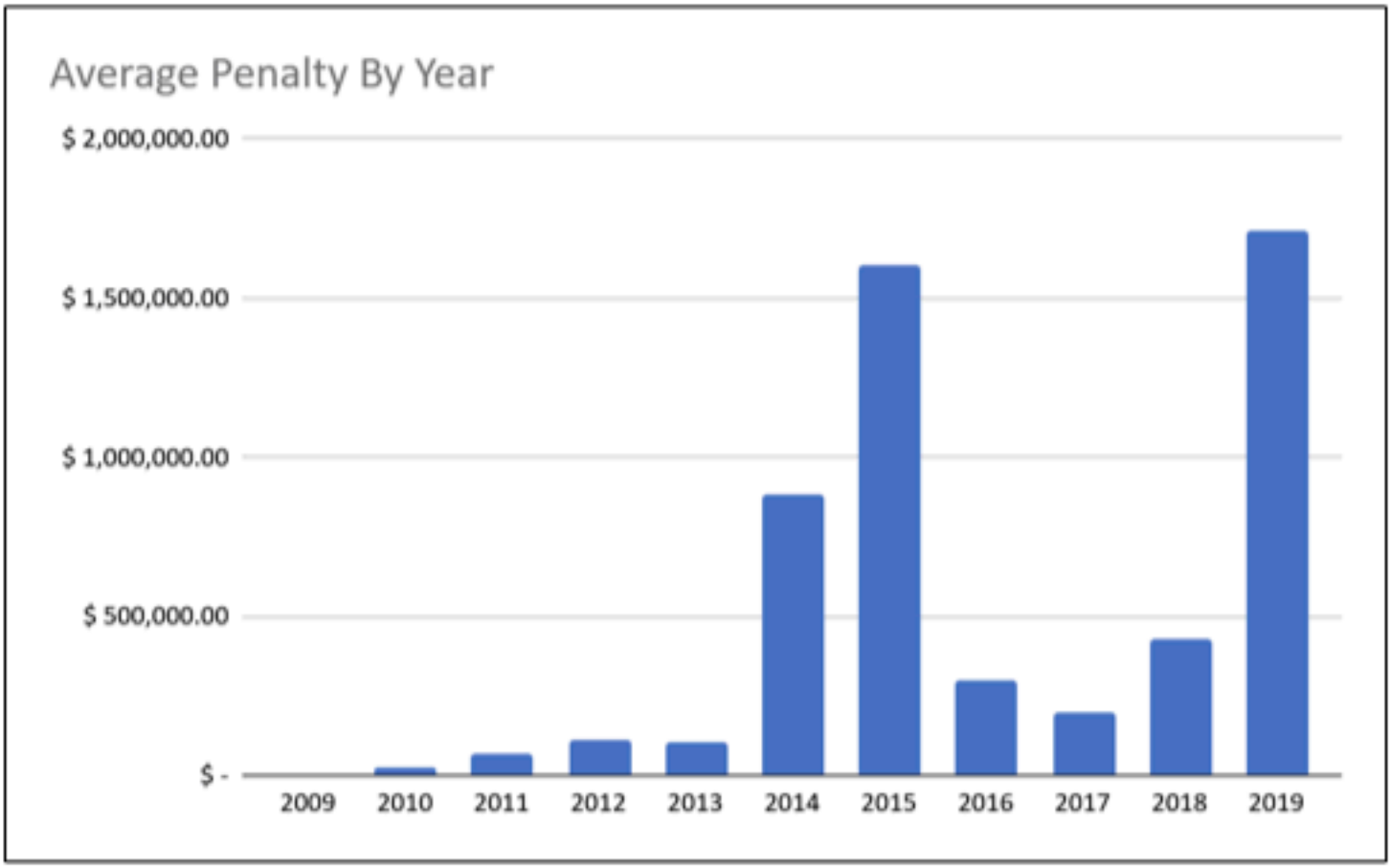


Figure 66: Average penalty for NERC CIP violations from 2009-2019 as gathered from https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx

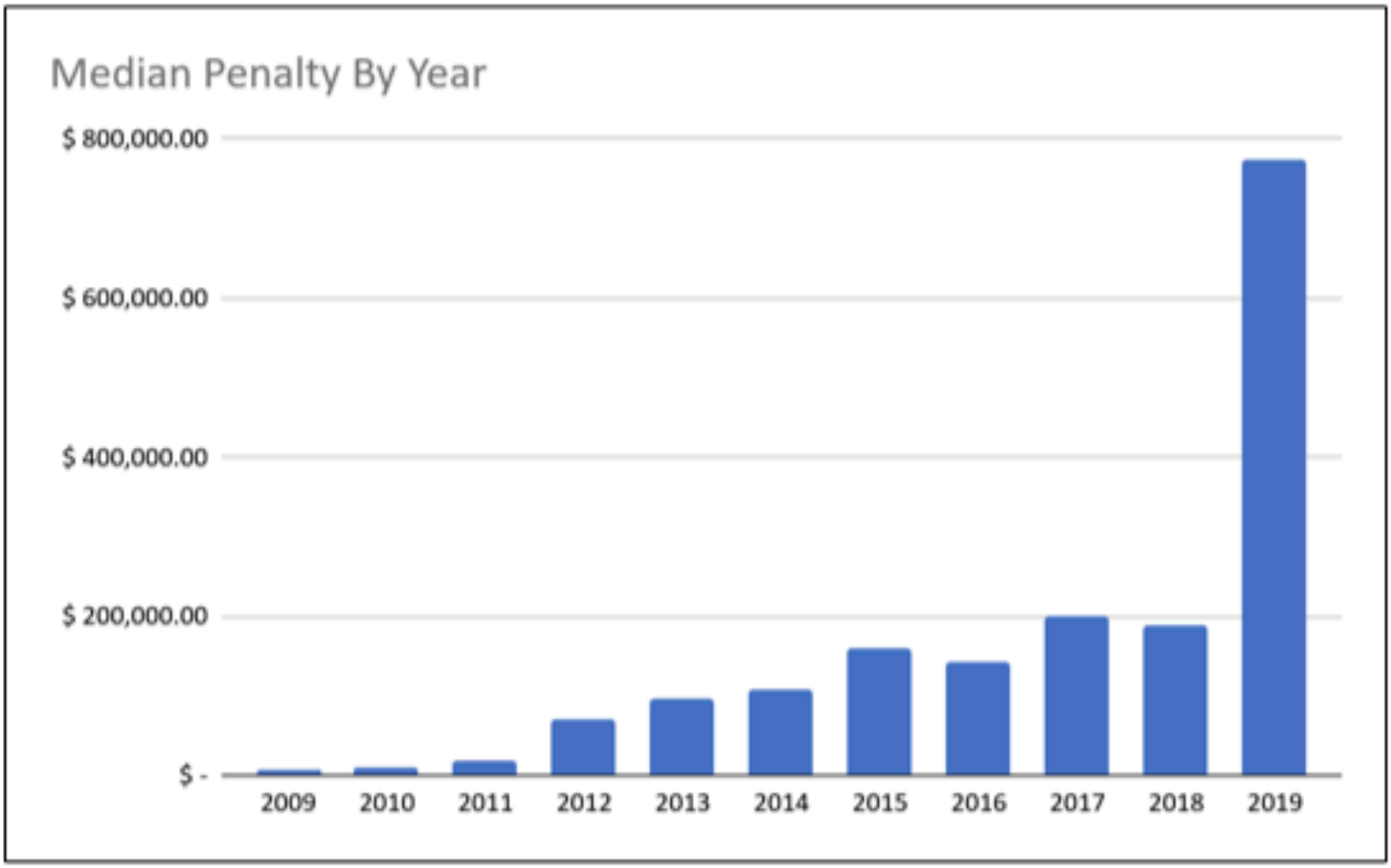


Figure 67: Median penalty for NERC CIP violations from 2009-2019 as gathered from https://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx

APPENDIX E: Rocket.Chat Operational Security

Throughout the engagement, [redacted] monitored NGPEW's Rocket.Chat general channel and noted several instances of possible security violations. Figure 68, 69, 70 are examples of instances where employees are failing to meet best security practices. Figures 71 shows a potential indicator of compromise, and figure 72 shows an employee potentially commiting fraud.

Figure 68: Employee storing physical unencrypted passwords

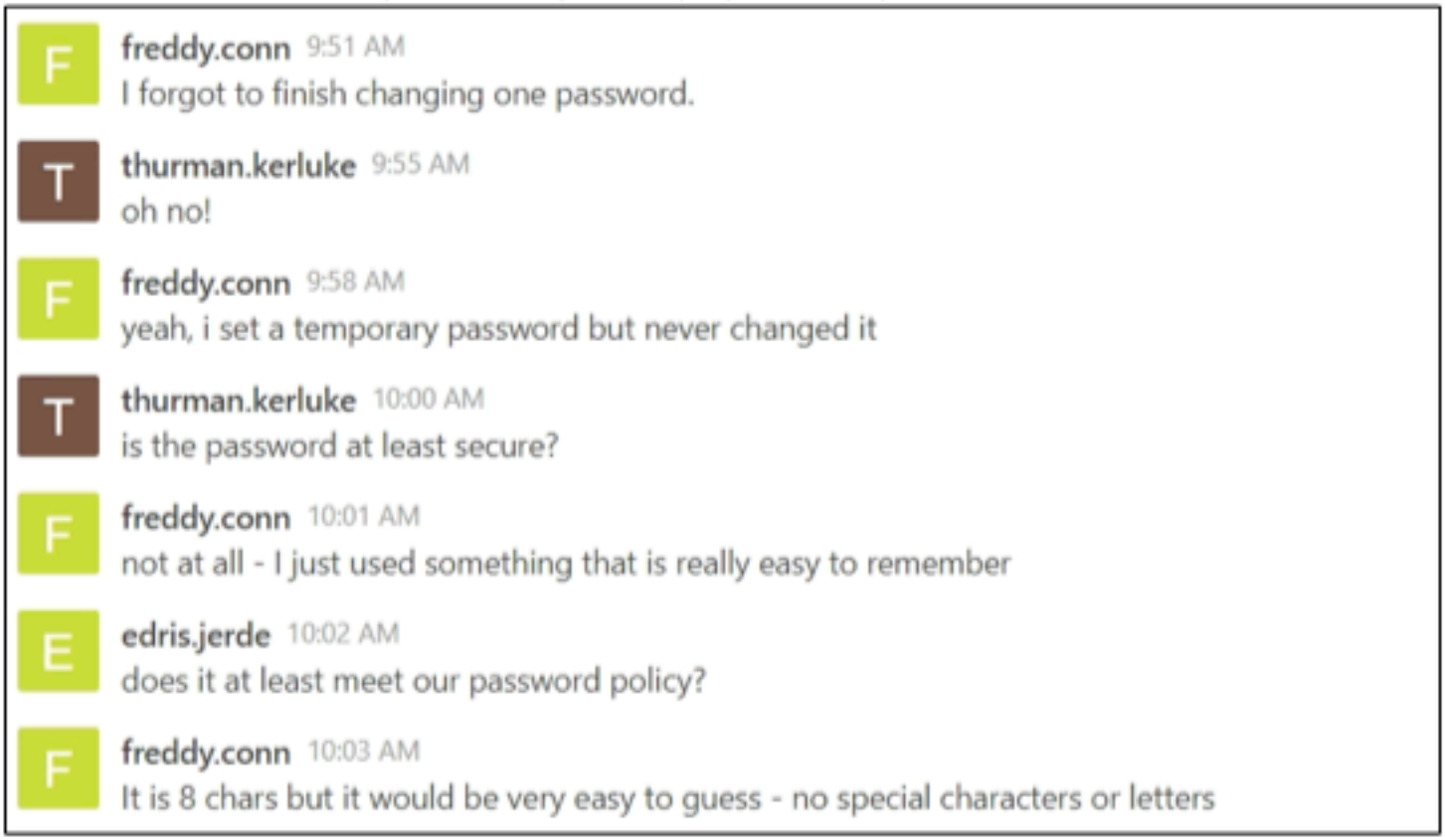


Figure 69: User stating that a password does not meet NGPEW security policy.

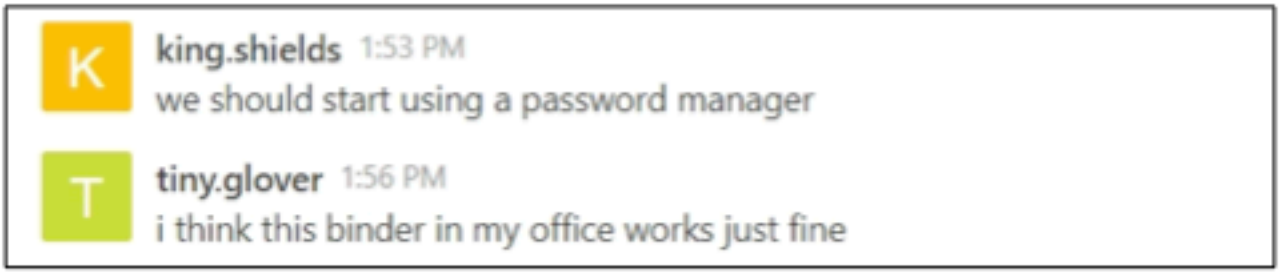


Figure 70: Employees storing physical passwords

Figure 71 indicates that an employee may have allowed an attacker onto their system. NGPEW should investigate into this situation and determine whether an incident has occurred or not.

Figure 71: Employee may have potentially been scammed

[redacted]oticed that an NGPEW employee mentioned that they may be outsourcing their work. If true, this can be a serious problem for NGPEW.

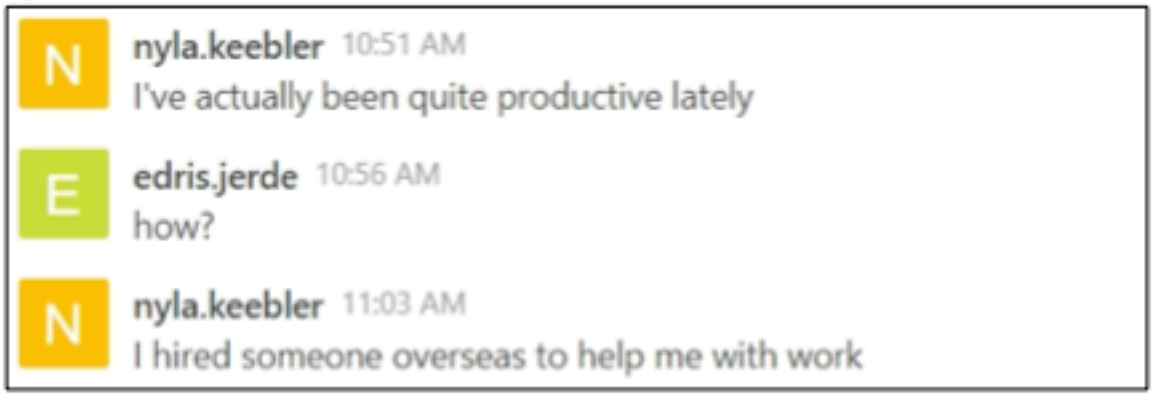


Figure 72: Employee potentially committing fraud by outsourcing work