NEXT GEN

Next Generation
Power, Electric, & Water

Penetration Test
Q1. 2021
[redacted]

Table of Contents

Table of Contents 2

Executive Summary 4

Scope 4

Terminology 5

Key Strengths 5

Areas of Improvement 5

Methodology 6

Attack Narrative 6

Phase Testing and Timeline 6

Open Source Intelligence Gathering (OSINT) 6

Network Reconnaissance 7

Threat Modeling 8

Exploitation 9

Findings 10

Risk Classification 10

Employees posting passwords in Rocketchat 10

Sensitive files on organization's Github page 10

Critical 11

VNC unauthenticated administrator access on 10.0.5.50 11

High 13

Weak password complexity and password reuse 13

Outdated IIS Server 14

Medium 16

Employees posting passwords in Rocketchat 20

Low 22

Sensitive files on organization's Github page 22

Website's security tips 24

Note 25

Open Source Intelligence Notes 25

Open Source Intelligence Gathering (OSINT) 25

Information From Unsuccessful Attacks 26

Windows 26

SMB Protocol 26

SMB Relay Attack 27

Anonymous SMB and LDAP 28

Workstation Access 29

Web Chat 30

Breached Passwords (Rocket.Chat) 30

Rocket.Chat Configuration 30

Rocket.Chat Bruteforce 31

SSH Attempts 32

Conclusion 33

Appendix 34

Provided Nessus Scan Results 34

Executive Summary

[redacted] was contracted by NGPEW to conduct a second penetration test to determine their infrastructure vulnerability, assess risk levels, and provide remediation methods. The engagement began January 8th, 2021 and concluded January 9th, 2021. The infrastructure is in production during the time of testing and in use by customers.

On January 8th, NGPEW provided [redacted] with three subnets. NGPEW provided [redacted] with a vulnerability scan report and one user account on January 9th.
The objectives of this test include the following:

- Identify publicly exposed ports and services which have documented vulnerabilities that can be exploited to bypass existing perimeter defenses
- Identify the presence of any vulnerabilities in the infrastructure which can be exploited to provide unauthorized access to data stored in workstations
- Gain access to dam and electrical plants' controller interfaces to either view or disrupt them

[redacted] discovered 8 vulnerabilities in the production environment, of which only one is critical. NGPEW is highly encouraged to remediate these technical findings within 5 days due to their high potential for exploit which can result in a downtime for customers and immediate monetary impact. NGPEW is also highly encouraged to train their employees and staff on safe security practices, like creating strong passwords that are not reused. This training is to take place once a year with all employees of all seniority. Overall, the external corporate network is well-secured, preventing initial footholds from gaining traction; however, the internal network has a few concerning exploits to watch out for.

Scope

The scope of this assessment covers NGPEW's production infrastructure. This includes three subnets, which comprises of a Corporate Local Area Network (LAN) and Supervisory Control and Data Acquisition (SCADA) Network. [redacted] did not test outside of the provided scope, as shown in Figure 1.

Network Ranges
10.0.1.0/24
10.0.5.0/24
10.0.10.0/24

Figure 1: Network Ranges.

Terminology

Internal Network
The 10.0.1.0/24 network that allows access to other machines on the 10.0.1.0/24, 10.0.5.0/25, and 10.0.10.0/24 networks.

We consider our initial Kali machines (10.0.254.201-6) to be not part of the internal network, but the security (10.0.1.60) machine to be part of it as we were given access on day two.

Key Strengths

[redacted] has found that NGPEW is doing a great job remediating vulnerabilities from [redacted]s previous engagement. Some specific details include:

- Keeping running services up-to-date
- Disabling remote connection to workstations outside the network
- Disallowing unauthorized users to create profiles on Rocket.Chat
- Locking accounts after brute force attempts in their Active Directory (AD) environment

Areas of Improvement

[redacted] has found NGPEW can improve on the following:

Findings	Remediation
Network Segmentation	Reevaluate privileged and non privileged users and create firewall rules to block unauthorized Internet Protocol (IP) addresses.
Weak Passwords & Password Reuse	Improve the current password policy to be at least 8 letters, have one uppercase and one lowercase, one number and one special character. Disallow password reuse between workstations and chat applications.
Lack of Authentication	Require authentication on all machines within NGPEW's network. Specifically, all VNC sessions need to be authenticated with credentials.

Methodology

Attack Narrative

[redacted] began the penetration test with reconnaissance and Open Source Intelligence (OSINT) on January 8th. For this, [redacted] used both off-the-shelf tools for scanning the network as well as manually visiting NGPEW's website to find employee and company information that is publicly available to everyone.

During the engagement period, [redacted] was provided with subnets and company background needed for gray box testing. Once the network was mapped, [redacted] began targeting machines with specific scanners to find more details. For example, when a Windows machine was found running the Kerberos authentication protocol, they scanned the machine with a tool geared towards Windows with Kerberos.

Once the network was enumerated and each host was scanned, [redacted] moved onto the exploit stage. [redacted] found it to be well-guarded and was impressed by NGPEW's quick response to the first test and its increased security.

After being provided a Nessus scan and an insider box on January 9th, [redacted] was able to compromise the entire internal network, the 10.0.1.0/24 subnet. On top of this, [redacted] found several other vulnerabilities on both the 10.0.5.0/24 and 10.0.10.0/24 subnets.

Phase Testing and Timeline

Open Source Intelligence Gathering (OSINT)

As part of the penetration test, [redacted] scoured the internet for information related to NGPEW. The findings include information from the online websites Twitter, Github, Facebook, and LinkedIn. Individual user accounts are accounts held by specific users within the NGPEW company. Company accounts are accounts that represent the company on various platforms. Specifics can be found in the findings section.

Network Reconnaissance

10.0.1.0/24 Corporate LAN

IP	Hostname	Role	Services
10.0.1.10	GRACE	Workstation Windows 2016 Datacenter (build:14393)	MSRPC, NetBIOS, Windows Server 2008, Windows Terminal Services
10.0.1.11	GAYLORD	Workstation Windows 2016 Datacenter (build:14393)	MSPRC, NetBIOS, Windows Server 2008, Windows Terminal Services
10.0.1.12	TINY	Workstation Windows 2016 Datacenter (build:14393)	MSPRC, NetBIOS, Windows Server 2008, Windows Terminal Services
10.0.1.13	PORFIRIO	Windows 2016 Datacenter (build:14393)	MSPRC, NetBIOS, Windows Server 2008, Windows Terminal Services, HTTP
10.0.1.60	Security	Provided machine in internal network	SSH
10.0.1.100	MPOWER	Windows AD Windows 2012 R2 Standard (build:9600)	Kerberos, LDAP, RPC
10.0.1.154	RocketChat	Chat Services	SSH, HTTP (port 3000)
10.0.1.198	N/A	N/A	LANDESK

10.0.5.0/24 SCADA Network

IP	Hostname	Role	Services
10.0.5.50	N/A	Programmable Logic Controller (PLC)	VNC
10.0.5.75	killbill.services.millenialpower.us	Services	Web Server, MySQL, KillBill
10.0.5.151	N/A		MySQL, PostgreSQL, SSH, ldap
10.0.5.152	N/A		Domain Controller, VNC, Web Server, Kerberos, SSH
10.0.5.153	support.millenialpower.us	Web Server	SSH, Web Server

10.0.10.0/24 SCADA Network

IP	Hostname	Role	Services
10.0.10.15	microgrid-controller.power.millenialpower.us	Microgrid Controller	HTTP

Threat Modeling

[redacted] identified dam and electric SCADA control interfaces as high-value assets to NGPEW and their up time.

Originally, from outside the network it was difficult to gain initial access. Once given the account to access the 10.0.1.60 box, [redacted] then had access to the other subnets where most of the vulnerabilities were found. Without VNC authentication, [redacted] was able to access the microgrid controller (10.0.10.15), which has access to interact with the dam and electric SCADA systems. If not secured, this can lead to down time as well as extremely dangerous situations.

An attacker would need to compromise a machine on the 10.0.1.0/24 subnet in order to cause serious damage. Given the Active Directory (AD) policies and network rules put in place, it would be hard to compromise a machine on the 10.0.1.0/24 subnet from outside the network. But depending on how well trained staff are with proper cyber security practices, a social engineer and/or phishing attempt can easily lead to your network being compromised.

Exploitation

After identifying the targets and their running services, [redacted] attempted to find vulnerabilities for the exposed services. Once a set of potential vulnerabilities is found, [redacted] attempts to exploit said vulnerabilities to gain access to private information or remote access to various machines on the network.

Post Exploitation

After gaining access to machines, [redacted] succeeded in privilege escalation and laterally moved across the network to other machines. Once [redacted] gained access to domain admin credentials, this led to further dumps of password hashes from other domain controllers and compromised more user accounts and services.

Findings

Risk Classification

Risk is modeled using: **Risk = Likelihood * Impact**
(https://owasp.org/www-community/OWASP_Risk_Rating_Methodology).
Likelihood is how easy the vulnerability can be exploited.
Impact is how damaging the vulnerability is to NGPEW, be it financial and/or technical.

The following table shows [redacted]s findings organized into the following categories:

CRITICAL	VNC unauthenticated administrator access
HIGH	Weak password complexity
HIGH	Outdated IIS Server
MEDIUM	Dumping passwords from memory (RAM)
MEDIUM	Reading passwords from SYSTEM and ntds.dit (Hard Drive)
MEDIUM	Employees posting passwords in Rocketchat
LOW	Sensitive files on organization's Github page
LOW	NGPEW's website security tips
NOTE	Individual Accounts

Critical

Finding #	Risk Rating	Findings
1	**CRITICAL**	VNC unauthenticated administrator access on 10.0.5.50

Description

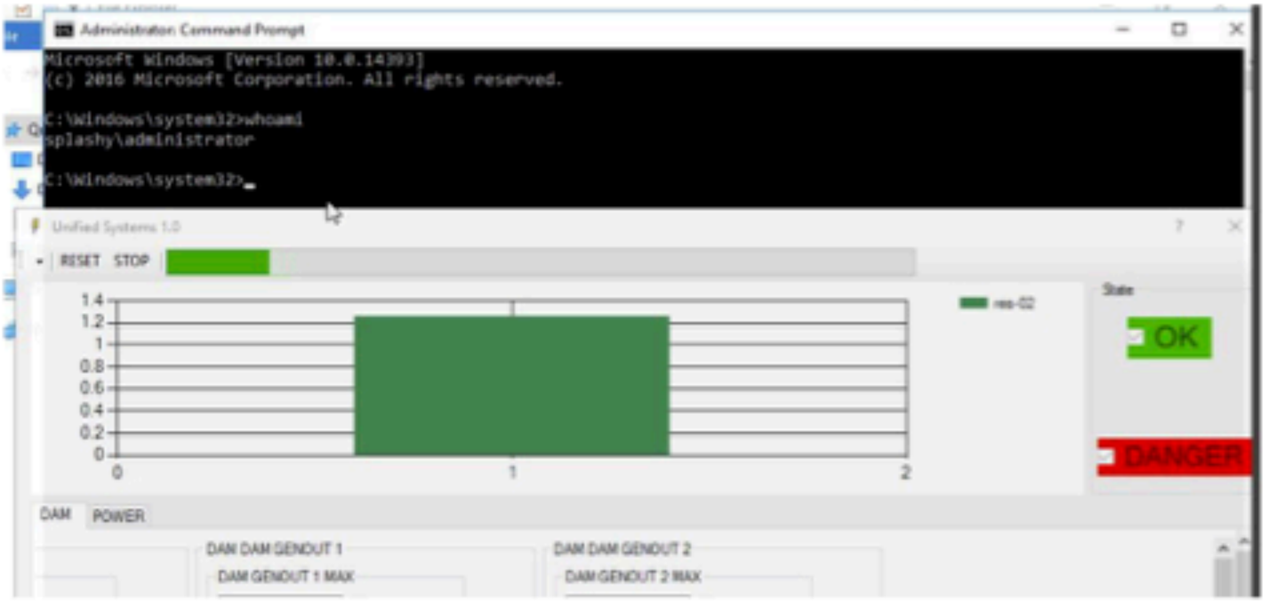
VNC is a technology that allows users to remotely access a machine. On the machine responsible for the monitoring services for the dams, [redacted] was able to use VNC to connect to the machine without supplying a password. Additionally, the unauthenticated VNC gave access to a local Administrator account on the Windows machine.

Steps to Reproduce

1. Download and install the TightVNC Desktop Client Software
2. Open the software.
3. Fill in the remote host box with the following line: 10.0.5.50:5900
4. Click ‘Connect’
5. You are logged in as Administrator

Impact and Details

As an administrator, the attacker has full control of the software running on the machine.



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
splashy\administrator

C:\Windows\system32>_
```

This includes the ability to “Reset” and “Stop” the software. Additionally, the attacker is able to further enumerate the machine. This leads to findings #2 and #3.

Affected Assets

10.0.5.50, PLC

Recommendations

Require a complex password in order to login with VNC. Run the software on a local account that only has the required permissions required to run the software.

References

N/A

High

Finding #	Risk Rating	Findings
2	HIGH	Weak password complexity and password reuse

Description

Reusing Windows Domain Administrator password on multiple machines with weak password complexity.

Steps to Reproduce

1. Get Domain Administrator password from Finding 4's exploit
2. Apply Administrator username and password onto different Windows workstations

Impact and Details

Reusing passwords allows the attacker to laterally move between different machines. The attacker is more likely to uncover sensitive company data.

Affected Assets

10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.100

Recommendations

Ensure employees fulfill password complexity.and prevent reusing passwords between different accounts and machines. For example, WestThompsonDam31 is significantly harder to bruteforce compared to WestThompsonDam. Both passwords are made up to obscure the actual recovered passwords.
Here is a password complexity recommendation from Sophos[1]:

- Password must be eight or more characters long.
- Password must contain characters from two of the following four categories:
  - Uppercase characters A-Z (Latin alphabet)
  - Lowercase characters a-z (Latin alphabet)
  - Digits 0-9
  - Special characters (!, $, #, %, etc.)

References

[1] https://docs.sophos.com/central/Mobile/help/en-us/esg/Sophos-Mobile/concepts/WDPasswordComplexityRules.html

Finding #	Risk Rating	Findings
3	HIGH	Outdated IIS Server

Description

The IIS server (version 4.0) running the NGPEW website is very outdated and subject to several exploits.

Password Bypass

This version of IIS exposes administrative password management via:
http://10.0.5.152/iisadmnpwd/achg.htr
http://10.0.5.152/iisadmnpwd/aexp.htr
http://10.0.5.152/iisadmnpwd/aexp2.htr
http://10.0.5.152/iisadmnpwd/aexp2b.htr
http://10.0.5.152/iisadmpwd/aexp3.htr
http://10.0.5.152/iisadmpwd/aexp4.htr
http://10.0.5.152/iisadmpwd/aexp4b.htr
http://10.0.5.152/iisadmpwd/anot.htr
http://10.0.5.152/iisadmpwd/anot3.htr

This allows unauthenticated users to brute force users and passwords on the machine. It also allows them to bypass the lockout policy.

Remote Command Execution (2)

IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, aka the "Web Server Folder Traversal" vulnerability.[2]

A vulnerability that could enable an attacker to run operating system commands on an affected server.[3] This vulnerability also leads to a denial of service attack by overloading allocated memory.

Outdated Host OS

OS detection scans revealed that the host OS is Windows NT 4.0. This version is no longer supported by Microsoft and should be updated to keep up with security patches.

Steps to Reproduce

Password Bypass

1. Navigating to the web pages listed above allows brute forcing of users and passwords without any authentication.

Unicode Remote Command Execution

1. [redacted] did not have time to verify this exploit. However, there is a metasploit module available for this vulnerability.

Outdated Host OS

N/A

Impact and Details

The outdated IIS allows an unauthenticated attacker to brute force usernames and passwords on the machine. Additionally, it may allow an attacker to execute commands on the machine.

Affected Assets

10.0.1.152

Recommendations

Update both the host OS and IIS server.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0421
[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0884
[3] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2001/ms01-026

Medium

Finding #	Risk Rating	Findings
4	MEDIUM	Reading passwords from memory

Description
By having access to a Windows machine, attackers were able to read passwords stored in memory via the lsass.exe program.

Steps to Reproduce

1. Gain access to a Windows machine
2. Download procdump from the Sysinternals Suite[1]
3. Execute procdump against lsass.exe
4. Exfiltrate the dump file created to an attacking machine
5. Execute mimikatz to extract passwords from the dump file

Impact and Details
This allows an attacker to compromise accounts and move laterally throughout the network, as well as potentially compromising a domain admin account. This can give an attacker full access to the AD environment where changes can be made or more accounts/services becoming compromised.

Affected Assets
10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.100
10.0.5.50

Recommendations
If the window's OS is Windows 10 or Windows Server 2016, we suggest using Windows Defender Credential Guard[2] to protect the passwords from attacks like these.

If the OS is older than Windows 10 or Windows Server 2016, we suggest enabling protection mode on lsass. This can be done by updating the registry in windows.

In the references you can find links referencing these mitigation tactics and more.

References

[1] https://docs.microsoft.com/en-us/sysinternals/
[2] https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard
[3] https://www.reliaquest.com/blog/credential-dumping-part-2-how-to-mitigate-windows-credential-stealing/

Finding #	Risk Rating	Findings
5	MEDIUM	Reading passwords from SYSTEM and ntds.dit

Description

By having Administrator access to the Domain Controller machine, the password hashes for all the users in the domain could be dumped using the SYSTEM and ntds.dit file.

Steps to Reproduce

1. Copy the SYSTEM and ntds.dit file using the following commands
   a. Ntdsutil
   b. activate instance ntds
   c. create full C:\foldername
2. Once the SYSTEM and ntds.dit file have been copied, tools such as Mimikatz will be able to extract the hashes from the file.
3. The hashes can then be cracked using online tools such as CrackStation, or offline tools such as Hashcat, revealing the password in plaintext.

Impact and Details

While this requires for there to have already been administrative access to the Domain Controller, this allows for the rest of the accounts and passwords in the system to be compromised.

All passwords of existing users on the system are affected.

[redacted]

Affected Assets

10.0.1.100

Recommendations

Ensure the domain admin accounts and domain controllers are secure, as there is no way to stop a user with administrator privileges from doing this attack.

References

[1] https://attack.mitre.org/techniques/T1003/

Finding #	Risk Rating	Findings
6	MEDIUM	Employees posting passwords in Rocketchat

Description

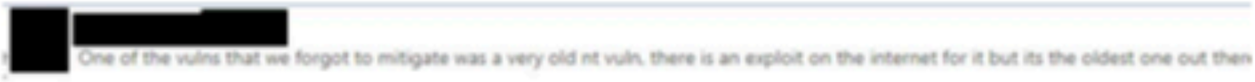
- NGPEW utilizes RocketChat for intra-company communication. Each employee has a RocketChat account that they can use in order to communicate with others in the organization. Some employees share important details about their security posture, such as sharing info about vulnerable systems, files of interest, and sending plaintext passwords.
- The RocketChat platform was accessed as a result of findings 3 and 4. Using the credentials from finding 4, we were able to login as any user. This includes CEO Grace Grantham's account and IT Director Gaylord Schaefer.

Steps to Reproduce

1. Choose a pair of credentials from finding 3.
2. Navigate to http://10.0.1.154:3000
3. Login with the credentials.
4. Read all the messages in the general channel.

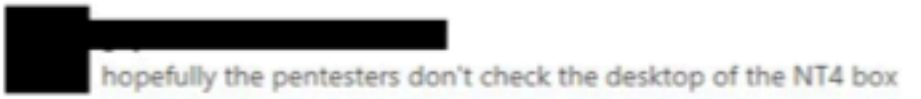
Impact and Details

[redacted] was able to learn of several vulnerabilities and passwords within the NGPEW infrastructure as a result of the available RocketChat messages. Here are a few notable findings:



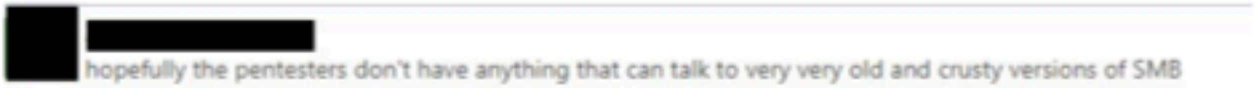
[redacted] [redacted]

One of the vulns that we forgot to mitigate was a very old nt vuln. there is an exploit on the internet for it but its the oldest one out ther



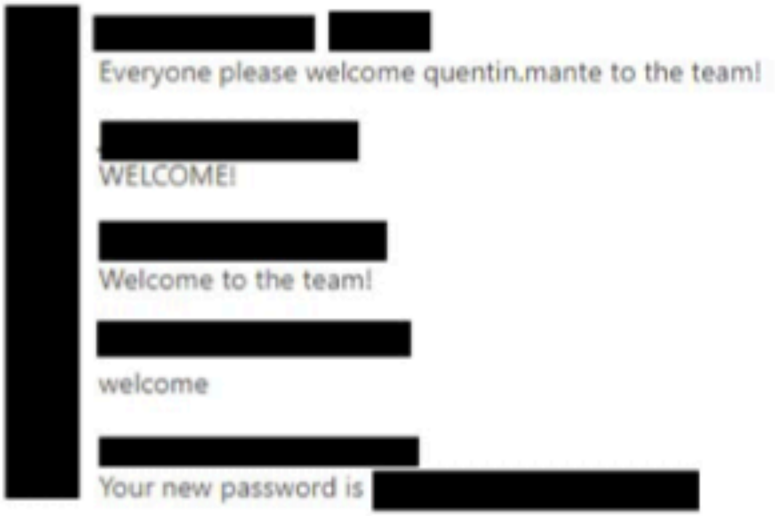
[redacted] [redacted]

hopefully the pentesters don't check the desktop of the NT4 box



[redacted] [redacted]

hopefully the pentesters don't have anything that can talk to very very old and crusty versions of SMB



[redacted]

[redacted] [redacted]
Everyone please welcome quentin.mante to the team!

[redacted]
WELCOME!

[redacted]
Welcome to the team!

[redacted]
welcome

[redacted]
Your new password is [redacted]

Affected Assets

The account of the employee whose password was posted publicly to the company is compromised. Given that passwords are re-used throughout the company's infrastructure, the account can be utilized to access several systems and services.
Not to mention possible insider threats using this to frame others or hide their tracks.

Recommendations

Refrain from posting personally identifiable information on channels public to all employees. Use complex passwords so that they cannot be easily brute-forced. Refrain from posting important details about the security of company infrastructure in a channel public to several employees. The practice of least privilege should be practiced, those should only have access to what they need to see. Multiple channels have already been created for this purpose although they are not being used.

References

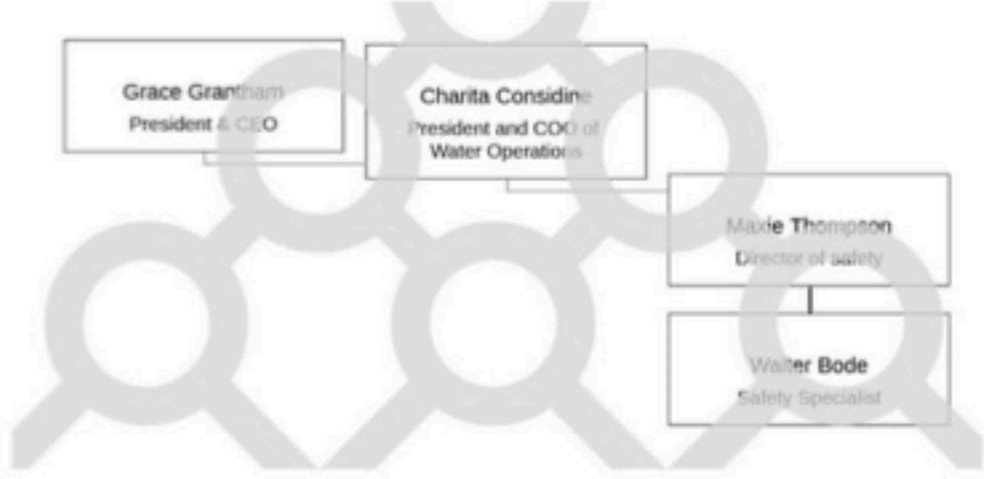
N/A

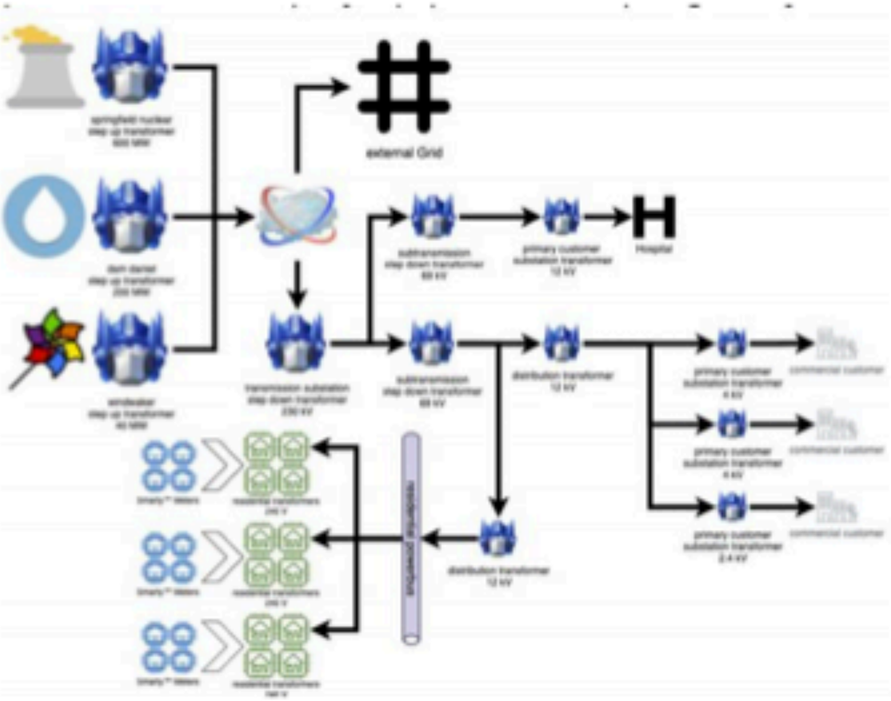
Low

Finding #	Risk Rating	Findings
7	LOW	Sensitive files on organization's Github page

Description

There are sensitive documents in the Github Repo's "docs" folder. By navigating to the commit history, click "commits", one would be able to see and download two PDF documents containing sensitive company information.




springfield nuclear step up transformer
external Grid
step up transformer
subtransmission step down transformer 69 kV
primary customer substation transformer 12 kV
Hospital
windwaker step up transformer
transmission substation step down transformer 230 kV
subtransmission step down transformer 69 kV
distribution transformer 12 kV
primary customer substation transformer
commercial customer
primary customer substation transformer
commercial customer
primary customer substation transformer 2.4 kV
commercial customer
Smarty™ Meters
residential transformers 240 V
Smarty™ Meters
residential transformers 240 V
distribution transformer 12 kV
Smarty™ Meters
residential transformers 240 V

Steps to Reproduce

1. Refer to the links in the Affected Assets Section.
2. Click on the GitHub links
3. You can now see the “deleted” documents.

Impact and Details

A file with convenient information about the company’s important employees is easily accessible for anyone to see over the internet. Additionally, another document containing the specifications and topological layout of company equipment is also easily accessible.

Affected Assets

Organization Chart highlighting employee hierarchy with title:
https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/Demo_Organization_Import_09_03_2020.pdf
Infrastructure Topology:
https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/PowerBus-Overview.png

Recommendations

In order to fix this issue, the Github Repo must be deleted and a new one must be created. There is no way to fully scrub the commit history where the files can be found. NGPEW must remove the entire repository and start a new one. [redacted] suggests the use of a private repository, so that even accidentally uploaded sensitive files will not be publicly accessible.

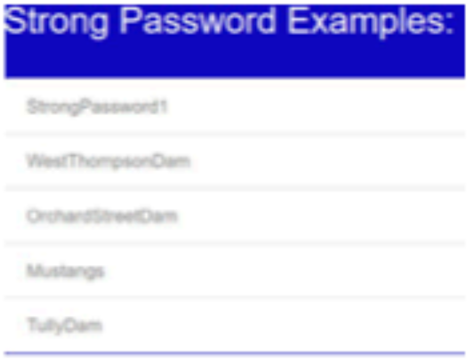
References

[1]https://github.com/Next-Generation-Power-and-Water/docs

Finding #	Risk Rating	Findings
8	LOW	Website’s security tips

Description

The official NGPEW website contains a page titled "Security Tips"[1] where sample passwords are given. The passwords given on the website have a format consistent with passwords discovered throughout the penetration test.



Strong Password Examples:

StrongPassword1

WestThompsonDam

OrchardStreetDam

Mustangs

TullyDam

Steps to Reproduce

N/A

Impact and Details

Since the passwords were simple, they were easy to guess. As a result, [redacted] had access to a majority of the users with domain access. These credentials could then be used throughout the NGPEW infrastructure, such as on the RocketChat platform.

Affected Assets

All Employee Accounts

Recommendations

While it is admirable that NGPEW is concerned about security and is willing to share security tips on their website, [redacted] suggests that they remove this information as it can be used to gain some kind of reference to the structure of passwords used by NGPEW employees.

References

[1] http://www.ngpew.com/securityTips.html

Note

Finding #	Risk Rating	Findings
9	**NOTE**	Open Source Intelligence Notes

Description
Open Source Intelligence Gathering (OSINT)

As part of the penetration test, [redacted] scoured the internet for information related to NGPEW. The findings include information from the online websites Twitter, Github, Facebook, and LinkedIn. Individual user accounts are accounts held by specific users within the NGPEW company.

Individual User Accounts:

a) https://twitter.com/kingshields6
b) https://twitter.com/HrLeuschke
c) https://twitter.com/GraceGrantham14
e) https://www.linkedin.com/in/grace-grantham-2a66001b6/
f) https://www.linkedin.com/in/king-shields-34ba461b7/
g) https://www.linkedin.com/in/tiny-glover-99550b1b6/
h) https://www.linkedin.com/in/gaylord-schaefer-4a18381b7/
i) https://www.linkedin.com/in/barbara-leuschke-88a9651b7/

Impact and Details.
Actors looking to attack NGPEW would view these accounts in order to gain information regarding the company. The majority of these accounts yield no significant information; however, given that they are owned by employees they must be constantly monitored for sensitive information.

Information From Unsuccessful Attacks

The following findings are exploit attempts that have been safeguarded by NGPEW's system configurations. The findings should nevertheless be brought to attention as they can still be potentially exploited.

Windows

SMB Protocol

Description
Running a version scan on the smb servers revealed the workstations support the following smb versions: NT LM 0.12, 2.02, 2.10, 3.00, 3.02, 3.11.

Steps of Attempt

1. Investigate the following RCE exploits against the service:
    a. **CVE-2017-0144 (EternalBlue)**
        i. The machines were not vulnerable to this exploit.
        ii. Initial scans showed the machine was.
    b. **CVE-2020-0796 (SMBGhost)**
        i. Vulnerability detection was run, revealing the machines are not vulnerable.
2. None of the above exploits worked, indicating an up to date configuration.

Intended Impact
Potential attacker access to Windows workstations.

Potentially Affected Assets
10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13

References
N/A

SMB Relay Attack

Description

A scan on the smb server showed that message signing was not required. This opens up the server to a SMB relay attack where our machine intercepts victim NTLM hashes and relays it to the SMB server as authentication. The attacking machine was unable to intercept any NTLM hashes from the network, and therefore were not able to perform this attack.

Steps of Attempt

1. On the interception machines, Responder[1] was used to intercept AD broadcast messages.
2. The intercepted messages were sent to impacket[2], which attempted to use the victim provided hashes to authenticate with the Domain Controller.

This attack failed because no AD broadcast messages were intercepted. However, message signing should still be enabled on the potentially affected assets listed below.

Intended Impact

Potential attacker access to Windows workstations.

Potentially Affected Assets

10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.50
10.0.1.100

Interception Machines:
10.0.254.202
10.0.1.60

References

[1] https://github.com/lgandx/Responder
[2] https://github.com/SecureAuthCorp/impacket

Anonymous SMB and LDAP

Description

Anonymous users in SMB and LDAP were disabled. This prevents potentially leaking sensitive information to unauthorized users.

Steps of Attempt

1. Attempt to anonymously connect to SMB and LDAP servers. Commands attempted include:
   ```
   smbclient <HOST_IP>
   smbclient -U "" <HOST_IP>
   ldapsearch -H <HOST_IP>
   ```
2. Both SMB and LDAP revealed anonymous authentication was disabled.

Intended Impact

Potential attacker access to Windows workstations or leakage of information.

Potentially Affected Assets

10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.100

References

N/A

Workstation Access

Description

Network access to the workstations 10.0.1.10 through 10.0.1.13 as well as Active Directory 10.0.1.100 is denied through a group policy setting. Therefore, [redacted] was not able to remotely access any local accounts through these machines. **However, this policy did not prevent the logon of domain accounts.**

Through attempting brute force of accounts with common passwords, [redacted] noticed that an account lockout policy was enforced. Repeated login attempts result in user lockout after 10 attempts. This policy is a great way of preventing brute force password attacks on system accounts because it restricts the amount of failed login attempts. Guest account logins were also restricted which limits unauthorized access to any of the system resources.

Steps of Attempt

1. Create a list of usernames or get a list of usernames that exist within the AD environment
2. Obtain a list of potential passwords
3. Use a tool like hydra, metasploit, kerbrute, or a script that has bruteforce capabilities with your lists

Intended Impact

Potential attacker access to Windows workstations.

Potentially Affected Assets

10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13
10.0.1.100

References

N/A

Web Chat

Breached Passwords (Rocket.Chat)

Description
Several username/password combinations previously breached were retried again. The old credentials did not work. Forcing employees to rectify password breaches prevents further outside access.

Steps of Attempt

1. Previously leaked passwords were used to attempt to log back in to Rocket.Chat.

Intended Impact
Potential attacker access to Rocket.Chat.

Potentially Affected Assets
10.0.1.154:3000

References
N/A

Rocket.Chat Configuration

Description
Rocket.Chat was found to have new user registration disabled on both the website and Application Programming Interface (API). Disabling new user registration prevents unauthorized users from viewing internal conversations, which can potentially leak sensitive information and cause monetary damage.

Steps of Attempt

1. [redacted] used the Rocket.Chat REST API to attempt to make a user. This led to an error signifying user creation was disabled.

Intended Impact
Potential attacker access to Rocket.Chat.

Potentially Affected Assets
10.0.1.154:3000

References
N/A

Rocket.Chat Bruteforce

Description

Login was protected from a bruteforce attack by rate limiting the rate of login attempts. [redacted] attempted a bruteforce attack with the following usernames:

grace.grantham
king.shields
tiny.glover
gaylord.schaefer
maxie.thompson
barbara.leuschke

Following the password policy available on the public website (https://ngpew.com), [redacted] compiled a wordlist by scraping https://en.wikipedia.org/wiki/List_of_dams_and_reservoirs_in_the_United_States. The result was a password list consisting of 242 entries.

No combination of these usernames/passwords allowed access into Rocket.Chat. A larger word list could have been made and tried, but due to time constraints [redacted] opted to look into other vulnerabilities.

Once access to Rocket.Chat was obtained through finding 123, it is revealed that quentin.mante's password follows the simple dam name format. If more time was spent attempting to brute force with a larger username and password list, this most likely would have been found.

Steps of Attempt

1. Obtain list of usernames from the NGPEW website.
2. Scrape the linked Wikipedia article to create a wordlist of dams following the company password policy.
3. Attempt to login through the Rocket.Chat API with all combinations of usernames and passwords.

Intended Impact

Potential attacker access to Rocket.Chat.

Potentially Affected Assets

10.0.1.154:3000

References

N/A

SSH Attempts

Description
All of the machines that [redacted] were able to interact with enforced "key-based authentication". A key is a file used by a person to identify themselves when connecting to a system. In this case, authorized users would need their own, specially generated private key in order to login to any machine. This protection denies all unauthorized users from logging in within the network, given that authorized users do not share their private keys.

Steps of Attempt

1. [redacted] utilized the tool Hydra to attempt to brute force SSH for Gaylord's account.

Intended Impact
Attempt to obtain Gaylord's password in order to authenticate to machines with elevated privileges.

Potentially Affected Assets
10.0.1.10
10.0.1.11
10.0.1.12
10.0.1.13

References
N/A

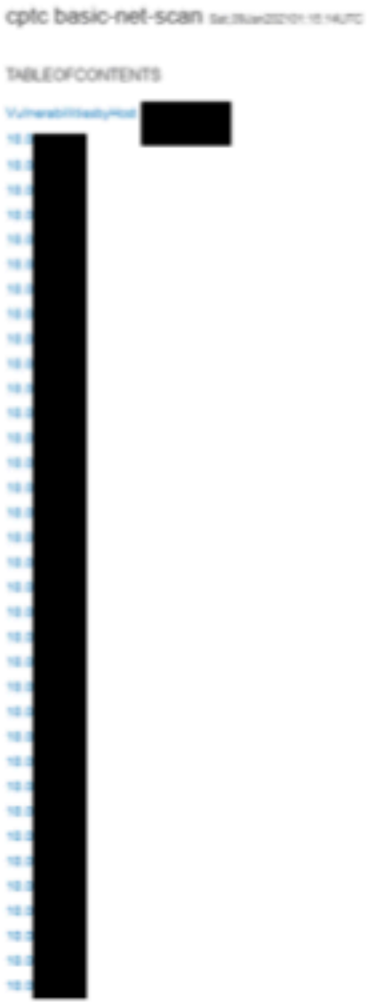
Conclusion

The provided network was much more secure than our first pentest with NGPEW. The only concerning issues existed within the internal network and not from external access. Had [redacted] not been given access to the Security Host (10.0.1.60), [redacted] would not have found several of the vulnerabilities mentioned in this report. NGPEW did a great job mitigating brute force attacks, segmenting the network, and removing a lot of the critical vulnerabilities we found in our first pentest.

Following these recommendations, [redacted] encourages NGPEW to invest in security awareness training for all employees. There are fantastic security measures in place, however these can easily be bypassed if employees fall victim to social engineering attacks.

Appendix

Provided Nessus Scan Results



cptc basic-net-scan Sat,29Jan202201:15:14UTC

TABLEOFCONTENTS

VulnerabilitiesbyHost [redacted]

[redacted]