[redacted]

Q1: 2021 Security Assessment Retest Report Prepared For

Report Issued: 10 January 2021

Confidentiality Notice

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to NGPEW or facilitate attacks against NGPEW. Finals[redacted] shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

Disclaimer

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a "point-in-time" assessment made on NGPEW's environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

Finals-[redacted] Consulting performed a security assessment of three NGPEW computer networks from 8 January 2021 to 9 January 2021. The test is a follow-up to a previous assessment performed on 7 November 2020. Finals-[redacted] Consulting tested NGPEW's internal corporate network, customer services network, and power utility network. Finals-[redacted]'s penetration test simulated an attack from an external threat actor attempting to gain access to internal systems within NGPEW, in order to identify vulnerabilities and suggest remediations.

Overall, Finals-[redacted] identifies low remaining risk to business functions due to successful remediation efforts. Network segmentation severely limits the movement of an attacker within the network, and new lockout policies increase the difficulty of obtaining valid credentials.

Finals-[redacted] identified a total of 11 remaining vulnerabilities within the scope of the engagement, which are broken down by severity in the table below:

CRITICAL	HIGH	MEDIUM	LOW
0	1	4	6

Concerningly, Finals-[redacted] identified the industrial control system interface does not require any login. This allows an attacker to gain full control of NGPEW's dam and power distribution systems. Attackers can use the vulnerability to sabotage the dams or power stations and cause loss of life. NGPEW may be held responsible for damages resulting from these attacks.

However, most of the identified vulnerabilities can only be exploited once the attacker has gained a set of valid user credentials or system access within NGPEW's internal network. Without valid user credentials or system access, attackers pose a limited threat. NGPEW's recently-implemented network controls were very effective at limiting the number of available attack options. NGPEW successfully implemented these controls in a limited timeframe since the previous engagement.

2. HIGH LEVEL ASSESSMENT OVERVIEW

I. Observed Security Strengths

Finals-[redacted] identified the following strengths with NGPEW's network, and recommends continuing to maintain the existing high level of security in the following areas

a. Network Segmentation

- Network access-controls blocked traffic from unauthorized sources from communicating with portions of the NGPEW network.

b. Account Lockout Policies

- Strong account lockout policies prevent attackers from successfully performing brute-force attacks and obtaining credentials.

c. Authentication Requirements

- Most services are now only accessible by authenticated users which prevents unauthorized access. Additionally, no working default credentials were found during testing.

d. Updated Service Versions

- Most software versions were up to date and included security patches that prevent attackers from exploiting well-known vulnerabilities.

e. Proper Service Configuration

- Default pages for websites were removed, some services used non-default ports, and avoided exposing sensitive debug interfaces.

These security strengths are discussed in detail in Section *5: Security Strengths Analysis.*

II. Recommendations

Finals-[redacted] recommends NGPEW take the following actions as soon as possible to minimize business risk.

a. Require Encryption

- Web servers like RocketChat are using insecure protocols. This may allow attackers to intercept traffic and steal credentials or sensitive information, or inject malware into web traffic.
- The domain controller allows plain-text authentication which may allow attackers to intercept traffic and steal credentials or sensitive information.

b. Disable Weak Encryption

- All Windows machines allow older, less secure encryption standards which may result in attackers being able to break the encryption and intercept communications.

c. Enforce Message Signing

- Windows machines do not require signed authentication messages, which allows messages to be intercepted or even modified. This also may allow the attacker to impersonate a valid user and gain their level of access.

3. SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

I. Networks

Network	Note
10.0.1.0/24	Primary Corporate Network
10.0.5.0/24	Customer Services (e.g. payments & support)
10.0.10.0/24	Power grid control network (e.g. industrial control systems & sensor monitoring)

II. Provided Systems

NGPEW provided Finals-[redacted] with the following systems to perform the security assessment.

Host	Note
172.16.213.129	Windows Test System 1
172.16.213.64	Windows Test System 2
172.16.213.128	Windows Test System 3
172.16.213.130	Windows Test System 4
172.16.213.65	Windows Test System 5
172.16.213.131	Windows Test System 6
10.0.254.201-206	Kali Linux Test Systems
10.0.1.60	Additional Internal Linux Test System - Provided on Jan. 9

III. Provided Credentials

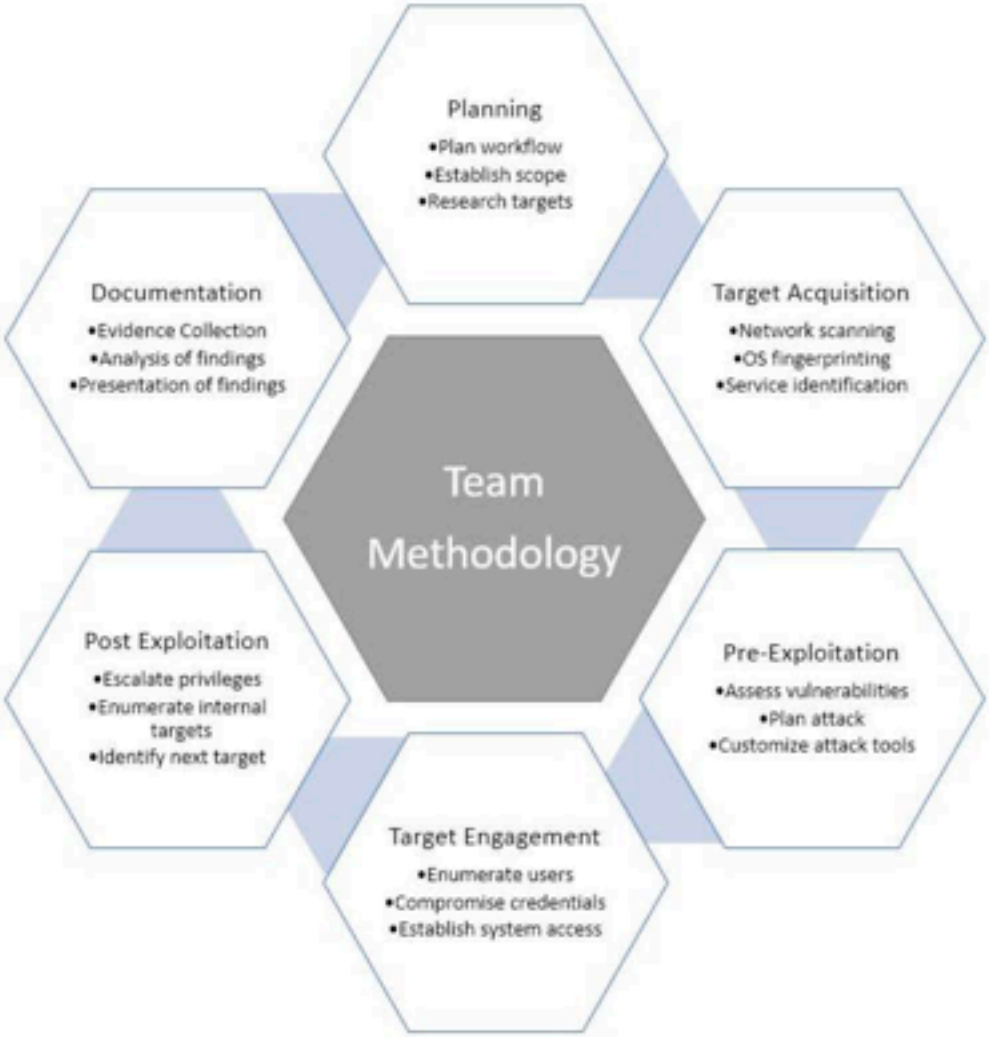
NGPEW provided Finals-[redacted] with the following credentials during the security assessment. These credentials provided sudo access to the security host at 10.0.1.60.

Username	Password
pentest	Cr******y

4. TESTING METHODOLOGY

Finals-[redacted]'s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about NGPEW's network systems. Finals-[redacted] used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. Finals-[redacted] simulated an attacker exploiting vulnerabilities in the NGPEW network. Finals-[redacted] gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.



5. SECURITY STRENGTHS ANALYSIS

I. Network Segmentation

During initial stages of testing, Finals-[redacted] was able to port scan hosts on the *10.0.1.0/24* subnet, but was unable to scan or or otherwise reach hosts on subnets *10.0.5.10/24* and *10.0.10.0/24*, despite using nmap techniques such as source routing, FIN scans, and fragmentation.

```
COMMAND $> nmap -n -sn -PE -T4 10.0.5.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 21:53 UTC
Nmap done: 256 IP addresses (0 hosts up) scanned in 26.13 seconds

COMMAND $>  nmap -n -sn -PE -T4 10.0.10.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 21:57 UTC
Nmap done: 256 IP addresses (0 hosts up) scanned in 26.24 seconds
```

Raw Data 5.I.1: *Port scans unable to reach hosts on 10.0.5.0/24 and 10.0.10.0/24.*

Given the amount of endpoint monitoring by *LaForge* as discussed in pre-engagement communication between NGPEW and Finals-[redacted] we believe that this would have effectively hindered the progress of an attacker, potentially enough for an internal Incident Response team to notice the attempts to gain access to the network before being able to compromise a host.

II. Account Lockout Policies

While attempting to brute-force login credentials, Finals-[redacted] became aware of lockout policies.

```
COMMAND $>  ./kerbrute bruteuser --dc 10.0.1.1000  -d corp.millenialpower.us --safe

2021/01/08 18:22:27 >
[!] tiny.glover@corp.millenialpower.us:****** - USER LOCKED OUT and safe mode on! Aborting...
```

Raw Data 5.II.1: *Error message indicating account tiny.glover is locked out.*

In order to avoid impact to business operations, brute-forcing logins was discontinued for the duration of the engagement. Furthermore, this prevented Finals-[redacted] from validating username and password combinations, despite being able to enumerate probable owners/users of the devices. Not only did this policy prove effective during Finals-[redacted]'s engagement with the client, but would also help to prevent possible account compromise during real cyberattacks.

III. Authentication Requirements

Finals-[redacted] then shifted focus to various services on the *10.0.1.0/24* subnet, such as RPC, SSH, LDAP and SMB. While testing these services, the team attempted null logins (not providing credentials), anonymous binds, and common default credentials such as *admin/password*.

```
COMMAND $> enum4linux -U 10.0.1.11
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri
Jan  8 16:40:30 2021

==========================
|    Target Information    |
==========================
Target ..... 10.0.1.11
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


================================================
|    Enumerating Workgroup/Domain on 10.0.1.11    |
================================================
[E] Can't find workgroup/domain


==================================
|    Session Check on 10.0.1.11  |
==================================
[E] Server doesn't allow session using username '', password ''.  Aborting
remainder of tests.
Use of uninitialized value $global_workgroup in concatenation (.) or string at
./enum4linux.pl line 437.
```

***Raw Data 5.III.1**: enum4linux reporting that a null session is not allowed*

Finals-[redacted] confirmed that null logins/sessions and anonymous access were disabled for SMB, RPC and LDAP(s). In addition, SSH required public key authentication, preventing user enumeration and password spraying attacks. The authentication requirement for these services prevented further enumeration of the environment as well as lateral movement from the subnet.

IV. Updated Service Versions

As part of application & service testing, Finals-[redacted] checked if any applications or services were versions with known vulnerabilities.

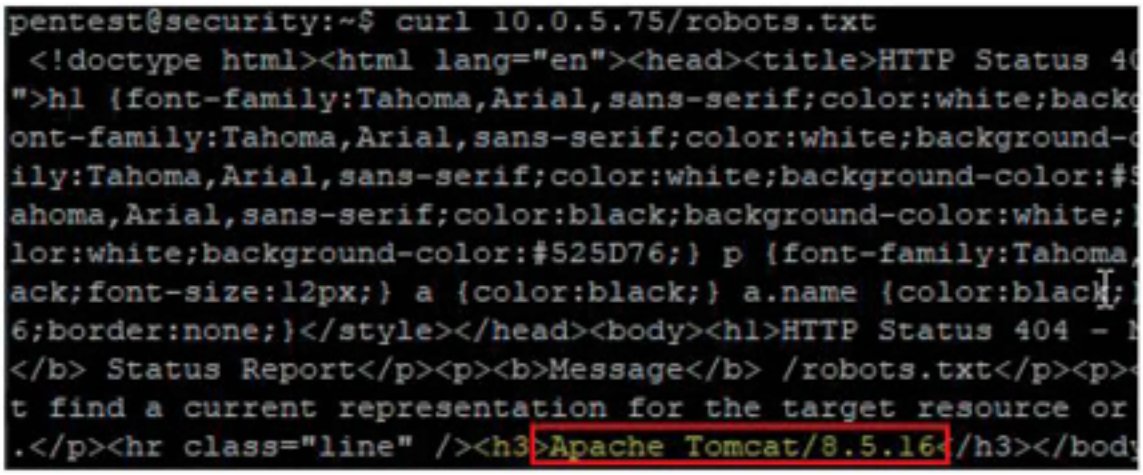


Figure 5.IV.1: *Response from host 10.0.5.75 indicating Apache Tomcat is up-to-date (8.5.16)*

Most services on the network were updated to mitigate recently announced vulnerabilities. The good update policies prevented Finals-[redacted] from gaining a foothold on segmented portions of the network using well-known exploits.

V. Proper Service Configuration

Throughout the test Finals-[redacted] found various examples of services configured in a secure, non-default manner. During testing, RocketChat had a non-default configuration that disabled the ability to register new user accounts and did not allow for guests to register to the LiveChat service. As Finals-[redacted] progressed further using the security host, we noted other services such as Redis, MySQL, and the Microgrid Controller (Werkzeug) had more secure configurations than the previous engagement. Redis previously had the default password. During this retest, that password was no longer valid. MySQL was hardened by only allowing connections from specific hosts. The

Microgrid controller's debug interface was also closed which prevented Finals-[redacted] from obtaining remote code execution.

6. CLASSIFICATION DEFINITIONS

I. Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization and exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization. Recovery from impacts of exploitation may be difficult. Remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

II. Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

III. Business Impact Classifications

Impact	Description
Severe	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Mild	Successful exploitation may affect few users, without causing much disruption to routine business functions.

IV. Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Medium	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

7. ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	VNC Without Authentication	8	High	16
2	Unsafe HTTP Methods	6	Medium	18
3	Login Over HTTP	6	Medium	21
4	SMB Message Signing Disabled	5	Medium	23
5	Firewall Rule Misconfiguration	4	Medium	25
6	Supported Outdated SMB Version 1.0	3	Low	27
7	Weak SSL Ciphers	3	Low	29
8	Exposed Sensor Data	2	Low	33
9	DNS Enumeration	2	Low	35
10	Information Disclosure	2	Low	36
11	End of Life Software	2	Low	40

1 - VNC Without Authentication

HIGH RISK (8/10)	
Exploitation Likelihood	Likely
Business Impact	Severe
Remediation Difficulty	Easy

Security Implications

Not requiring authentication allows attackers to gain full control of the Administrator account of the industrial control system interface without credentials. Attackers can use this access to control NGPEW's dam and energy systems and could potentially cause damage to the infrastructure and loss of life.

Analysis

Finals-[redacted] performed a network scan from the security host at 10.0.1.60 and identified that VNC was running on the target server. Finals-[redacted] then connected to the server using RealVNC Viewer without providing any credentials. This gave Finals-[redacted] access to the Administrator user's desktop without being prompted for credentials. The NGPEW's Industrial control system (ICS) interface was open on the desktop and did not require any secondary authentication. NGPEW's ICS interface also allowed interaction with ModBus values and thresholds.

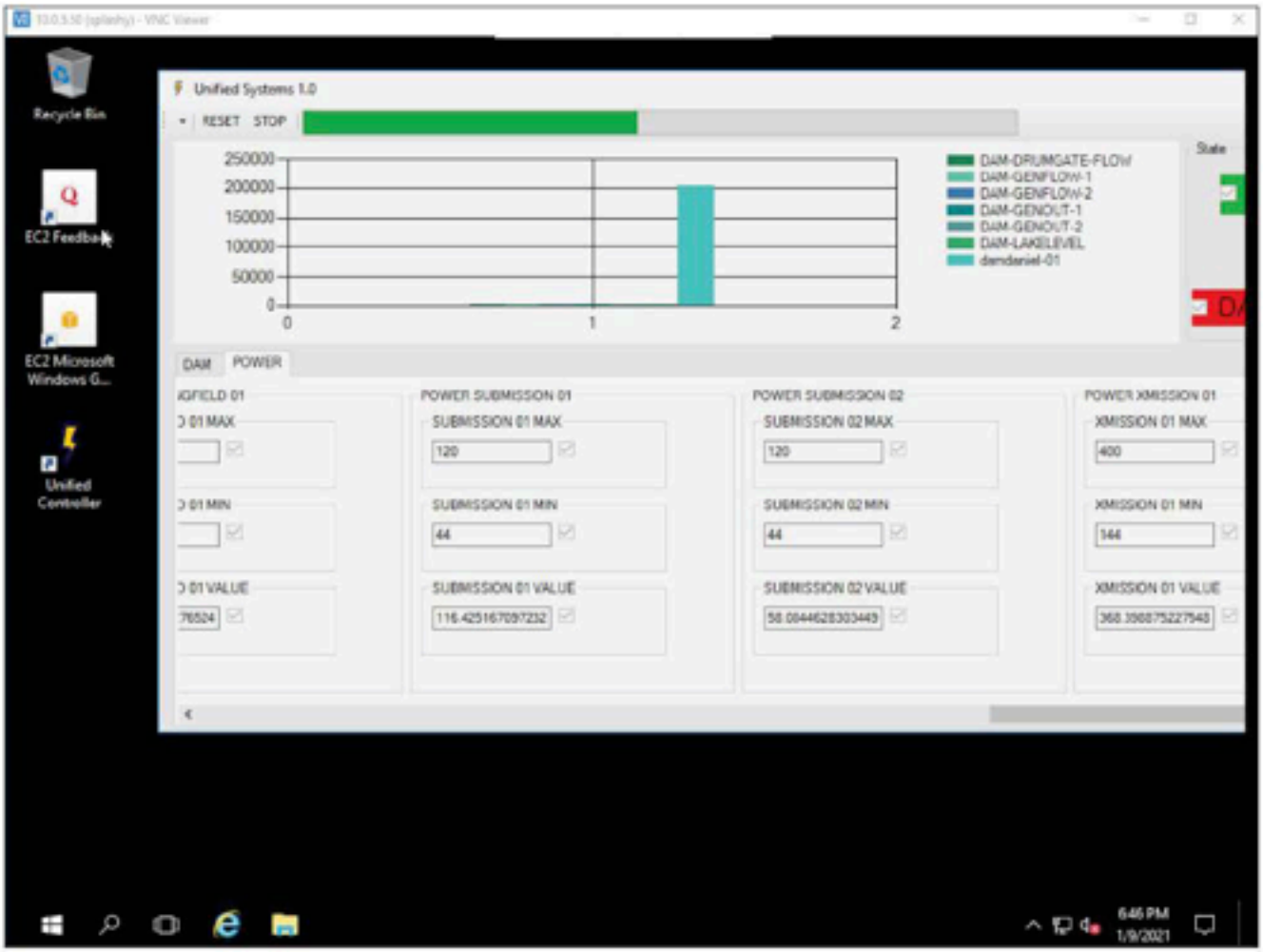


***Figure 1.2**: VNC desktop access allowing control of many dam systems*

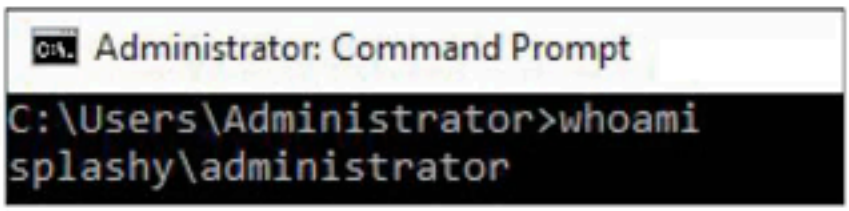


***Figure 1.2**: Default user is the local system administrator account*

Affected Host:

- 10.0.5.50

Recommendations

- Require authentication for VNC connections
- Restrict VNC connections to non-administrative user accounts

2 - Unsafe HTTP Methods

MEDIUM RISK (6/10)	
Exploitation Likelihood	**Possible**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

Security Implications

Insecure HTTP methods are enabled on the web server at http://10.0.1.152. These methods provide additional control of the web server, which an attacker can use to conduct attacks against the application and its users. An attacker can use these methods to cause reputational harm to NGPEW by adding unauthorized content to the website.

Analysis

Although most HTTP methods provide the web application with additional functionality, unauthenticated attackers can leverage these methods to control and exploit the application. Unsafe HTTP methods can provide attackers with additional information or control of the web application.

The following unsafe HTTP methods are allowed on the web server:

- PUT
- TRACE/TRACK

The HTTP PUT method allows attackers to upload arbitrary files including malware and webshells to the server. Any file an attacker uploads using the PUT command is publicly accessible and hosted by the application. For a proof of concept, Finals-[redacted] uploaded a simple webpage to demonstrate the functionality of this method.

```
PUT /canary.html HTTP/1.1
Host: 10.0.5.152
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Connection: close
Referer: http://10.0.5.152/contactUs.html
Upgrade-Insecure-Requests: 1
Content-type: text/html
Content-Length: 15

<p>Hello </p>

HTTP/1.1 100 Continue
Server: Microsoft-IIS/4.0
Date: Sat, 09 Jan 2021 19:20:03 GMT
PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" l by "easteregg@jrwr.io" on
"2020.09.04T03:21--100" exp "2021.09.04T12:00--100" r (v 0 s 0 n 0 l 4))

HTTP/1.1 201 Created
Server: Microsoft-IIS/4.0
Date: Sat, 09 Jan 2021 19:20:03 GMT
PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" l by "easteregg@jrwr.io" on
"2020.09.04T03:21--100" exp "2021.09.04T12:00--100" r (v 0 s 0 n 0 l 4))
Connection: close
Location: http://10.0.5.152/canary.html
Content-Type: text/html
Content-Length: 60
Allow: OPTIONS, TRACE, GET, HEAD, PUT, DELETE

<body><h1>/canary.html was created successfully.</h1></body>
```

***Raw Data 2.1**: Using an HTTP PUT request to create a test page*

***Figure 2.2:** Verifying the uploaded webpage is hosted by the application*

The HTTP TRACE/TRACK method is normally used to return the full HTTP request to the requesting client for proxy and debugging purposes. This behavior is usually harmless, but can lead to disclosure of sensitive information such as internal authentication headers. Attackers

can also create a webpage tricking a victim into issuing a TRACE request and enabling the attacker to capture the victim's cookies. This was not attempted by Finals-[redacted]

Finals-[redacted] tested the HTTP DELETE method which was enabled during the previous assessment. NGPEW has successfully remediated this vulnerability by requiring Request-header field preconditions to be met before deleting the request webresource.

Affected Host:

- 10.0.5.152

Recommendations

- Disable PUT and TRACE/TRACK in IIS Manager to limit HTTP methods to required functions
- Implement Request-header field preconditions on PUT and TRACE/TRACK methods

3 - Login Over HTTP

MEDIUM RISK (6/10)	
Exploitation Likelihood	**Possible**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

Security Implications

Logging into a web service or HTTP application allows for attackers to intercept the traffic or modify packets without detection. Attackers can exploit this to intercept valid credentials or inject malware into client traffic.

Analysis

Finals-[redacted] located a RocketChat web server running on 10.0.1.154 over port 3000. The home page had a login form where a user can enter credentials to gain access to the service. Finals-[redacted] identified that the service was being run over HTTP instead of HTTPS which allows man in the middle attacks to occur. An attacker could intercept RocketChat's traffic and wait for a user to login using their credentials and steal them. Furthermore, the attacker could use these credentials to gain access to other parts of the network if the user has the same username and password.

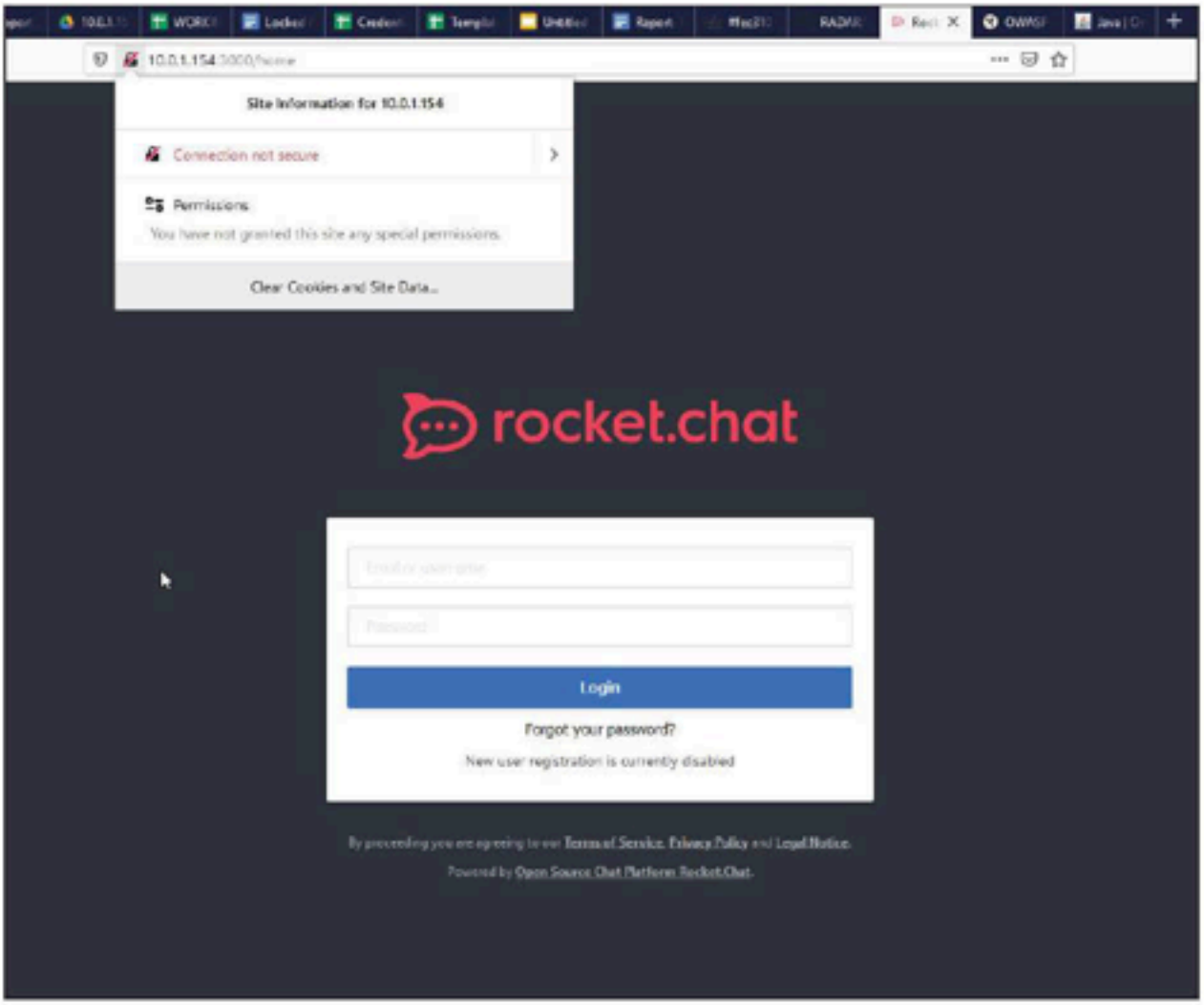


***Figure 3.1**: RocketChat using HTTP instead of HTTPS*

Affected Host

- 10.0.1.154

Recommendation

- Secure the application by running it over HTTPS

4 - SMB Message Signing Disabled

MEDIUM RISK (5/10)	
Exploitation Likelihood	**Possible**
Business Impact	**Medium**
Remediation Difficulty	**Easy**

Security Implications

If a man-in-the-middle (MITM) attack is performed on SMB connections that do not have message signing, the attacker will be able to execute arbitrary code on the affected hosts.

Analysis

If an attacker is able to access the same network as the target SMB host system, they would be able to perform a MITM attack on the target system. An attacker could perform a relay attack using the link-layer multicast name resolution (LLMNR), NetBIOS (NBNS), and WINS requests sent to the SMB host.

A relay attack is done by responding to the name resolutions requests faster than the connecting, and authorized, system. If the attacker responds to the previously mentioned requests faster than the authorized system, they are able to gain the same privileges as the user that is connecting to the SMB Host, leading to potential full compromise of systems running SMB without message signing. By enabling SMB message signing, the SMB service host can verify LLMN, NBNS, and WINS responses came from an authorized source, preventing the attack.

Finals-[redacted] verified that SMB Message Signing is disabled by using the smb-security-mode NMAP script. The smb-security-mode script verified SMB user-level authentication, share-level authentication, and message signing.

```
# Nmap 7.91 scan initiated Fri Jan  8 16:04:28 2021 as: nmap -sC -oN scripts.txt 10.0.1.0/24
Nmap scan report for ip-10-0-1-10.ec2.internal (10.0.1.10)
Host is up (0.00054s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
```

```
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: GRACE
|   NetBIOS_Domain_Name: GRACE
|   NetBIOS_Computer_Name: GRACE
|   DNS_Domain_Name: grace
|   DNS_Computer_Name: grace
|   Product_Version: 10.0.14393
|_  System_Time: 2021-01-08T16:05:29+00:00
| ssl-cert: Subject: commonName=grace
| Not valid before: 2021-01-06T22:40:18
|_Not valid after:  2021-07-08T22:40:18
|_ssl-date: 2021-01-08T16:05:29+00:00; 0s from scanner time.

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-08T16:05:39
|_  start_date: 2021-01-07T23:09:02
```

***Raw Data 4.1**: Result of smb-security-mode NMAP script*

Affected Hosts

- 10.0.1.10
- 10.0.1.11
- 10.0.1.12
- 10.0.1.13

Recommendations

- Enable SMB Message Signing in Domain and Local Group Policy

References

- https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing
- https://nmap.org/nsedoc/scripts/smb-security-mode.html

5 - Firewall Rule Misconfiguration

MEDIUM RISK (4/10)	
Exploitation Likelihood	**Unlikely**
Business Impact	**Moderate**
Remediation Difficulty	**Easy**

Security Implications

NGPEW's Internet facing firewall allows traffic on ports that are not currently running any services. This may allow an attacker to set up an unauthorized service and the firewall would allow the traffic through.

Analysis

The firewall rule set in use protecting NGPEW's Internet-facing systems is not configured in accordance with observed security best practices. Best industry practice for firewalls should include a master DENY ALL policy, whereby only specific ports on specific hosts are individually authorized to be open. Only ports that are necessary should be allowed open. No hosts on the network should appear to have any CLOSED ports. A CLOSED port appears when the firewall lets a packet through to a certain host, but the host is not listening on that port.

The following shows port scanning tool raw output. Any port that is listed as 'closed' needs to be firewalled as explained above.

```
Nmap scan report for ip-10-0-1-60.ec2.internal (10.0.1.60)
Host is up (0.00059s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  closed http
443/tcp closed https

Nmap scan report for ip-10-0-1-154.ec2.internal (10.0.1.154)
Host is up (0.00082s latency).
Not shown: 65531 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
```

```
80/tcp   closed http
443/tcp  closed https
3000/tcp open   ppp

Nmap scan report for killbill.services.millenialpower.us (10.0.5.75)
Host is up (0.0011s latency).
Not shown: 65528 filtered ports
PORT     STATE  SERVICE
80/tcp   open   http
443/tcp  closed https
3306/tcp open   mysql?
8000/tcp open   java-rmi
8080/tcp open   http-proxy
9090/tcp closed zeus-admin
12345/tcp open  jdwp
```

Raw Data 5.1: *Nmap output showing closed ports*

Affected Hosts

- 10.0.1.60
- 10.0.1.154
- 10.0.5.75

Recommendations

- Immediately DENY all 'CLOSED' ports listed above
- Implement a DENY ALL policy on the Internet-facing firewall. Only allow ports explicitly authorized by NGPEW network security policy.
- Periodically audit firewall years (e.g., twice a year) to make sure no rules were added without proper authorization and a stated individual is responsible for each allowed port.

6 - Supported Outdated SMB Version 1.0

LOW RISK (3/10)	
Exploitation Likelihood	Possible
Business Impact	Mild
Remediation Difficulty	Easy

Security Implications

SMB Version 1 does not support encryption. An attacker can sniff SMBv1 streams for sensitive information, credentials, or even modify the streams to send commands to the target machine.

Analysis

Although SMB Version 3 is preferred by the machines, outdated SMBv1 communications might still be used across the network, leading to compromise of credentials, and potential remote code execution on the SMB server if the insecure stream is sniffed using a man-in-the-middle attack. Finals[redacted] tested supported SMB versions using the smb_version metasploit module which revealed that SMBv1 was still supported.

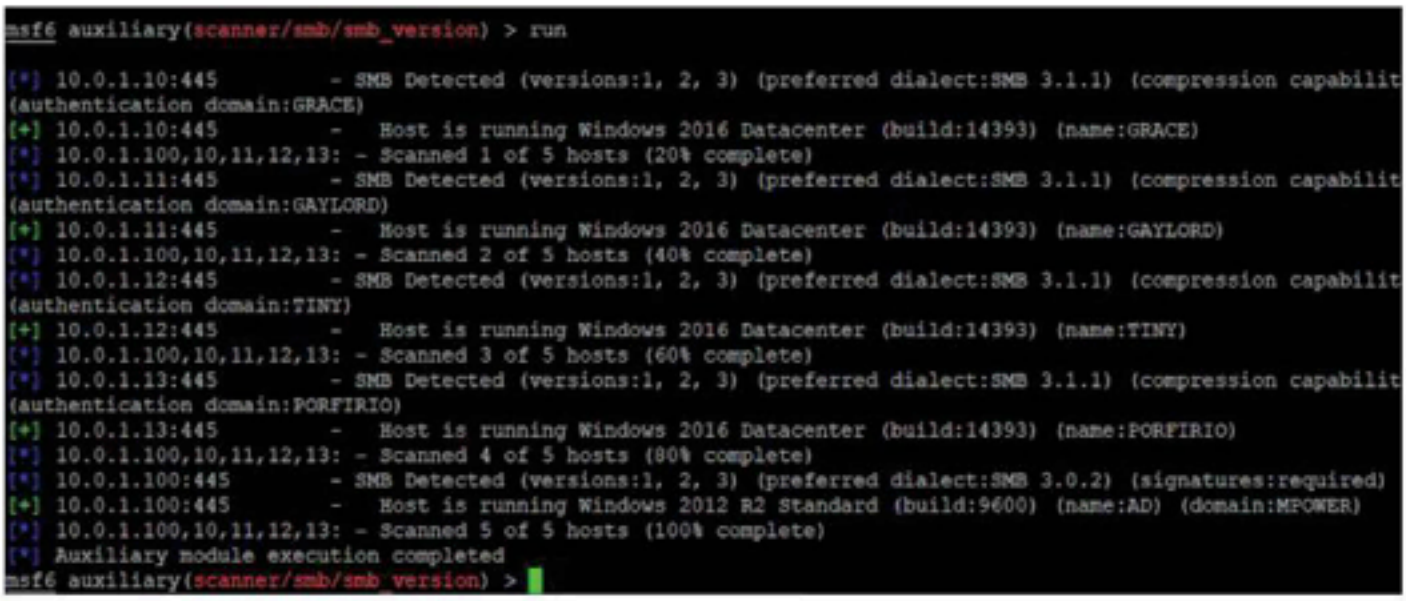


***Figure 6.1**: Metasploit SMB version scanner determining running SMB versions*

Affected Hosts

- 10.0.1.10
- 10.0.1.11
- 10.0.1.12
- 10.0.1.13
- 10.0.1.100

Recommendation

- Disable SMB version 1 in Domain Group Policy and on individual machines

References

- https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

7 - Weak SSL Ciphers

LOW RISK (3/10)	
Exploitation Likelihood	**Unlikely**
Business Impact	**Moderate**
Remediation Difficulty	**Medium**

Security Implications

Weakness in encryption configurations can threaten the integrity of encrypted sessions and the confidentiality of encrypted data. Although cryptographic attacks generally require a high degree of expertise to perform, automated tools are available to simplify some attacks.

Analysis

The web servers that support the application are "self-signed" (i.e., signed by an untrusted certificate authority). The certificate was generated by NGPEW. Use of this certificate can make it hard for users to distinguish between a valid session and a "main in the middle" attack.

The web servers also support session negotiation with RC4 cipher suites, which are known to be vulnerable to cryptographic attacks such as "Bar Mitzvah" (CVE-2015-2808) due to a flaw in random number generation. Successful attacks against RC4 can derive the original plaintext from the encrypted traffic.

Lastly, the web servers support session negotiation with "Early TLS" (TLS 1.0) which is known to be vulnerable to cryptographic attacks, mostly when used in conjunction with RC4 cipher suites.

The following table lists servers in which encryption is not optimally configured.

IP Address	Relevant Port	Comments
10.0.1.10	3389	TLS 1.0 and 1.1 enabled
10.0.1.10	3389	Supports 128 bit RC4-SHA and 128 bit RC4-MD5
10.0.1.10	3389	Certificate self signed by grace

10.0.1.11	3389	TLS 1.0 and 1.1 enabled
10.0.1.11	3389	Supports 128 bit RC4-SHA and 128 bit RC4-MD5
10.0.1.11	3389	Certificate self signed by gaylord
10.0.1.12	3389	TLS 1.0 and 1.1 enabled
10.0.1.12	3389	Supports 128 bit RC4-SHA and 128 bit RC4-MD5
10.0.1.12	3389	Certificate self signed by tiny
10.0.1.100	3389	TLS 1.0 and 1.1 enabled
10.0.1.100	3389	Supports 128 bit RC4-SHA and 128 bit RC4-MD5
10.0.1.100	3389	Certificate self signed by ad.corp.millenialpower.us

***Table 7.1**: List of hosts with weak ssl/tls encryption*

The following example illustrates the configuration of the 10.0.1.100 server:

```
Testing SSL server 10.0.1.100 on port 3389 using SNI name 10.0.1.100

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
TLSv1.1 not vulnerable to heartbleed
TLSv1.0 not vulnerable to heartbleed
```

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384      Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256      Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA         Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384    DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256    DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Accepted  TLSv1.2  128 bits  RC4-SHA
Accepted  TLSv1.2  128 bits  RC4-MD5
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA         Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Accepted  TLSv1.1  128 bits  RC4-SHA
Accepted  TLSv1.1  128 bits  RC4-MD5
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA         Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5

  Server Signature Algorithm(s):
TLSv1.2  rsa_pkcs1_sha256

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048
```

```
Subject:  ad.corp.millenialpower.us
Issuer:   ad.corp.millenialpower.us

Not valid before: Jan  6 22:59:50 2021 GMT
Not valid after:  Jul  8 22:59:50 2021 GMT
```

Raw Data 7.2: *SSLScan Output of Domain Controller*

Affected Hosts

- 10.0.1.10
- 10.0.1.11
- 10.0.1.12
- 10.0.1.100

Recommendations

- Web servers and other services that utilize TLS encryption should be configured to only allow encryption negotiation with TLS version 1.2. Earlier versions of TLS may be used but only if vulnerable cipher suites and cipher strengths of lower than 128-bit are disabled.

References

- https://nvd.nist.gov/vuln/detail/CVE-2015-2808
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

8 - Exposed Sensor Data

LOW RISK (2/10)	
Exploitation Likelihood	Likely
Business Impact	Mild
Remediation Difficulty	Easy

Security Implications

Accessible sensor data provides attackers with information about the status of NGPEW infrastructure which can entice attacks on NGPEW systems. The sensor data can allow attackers to monitor if their attacks are successfully controlling NGPEW systems.

Analysis

Finals-[redacted] identified a python web server that was accessible from 10.0.1.60. Finals-[redacted] setup a socks5 proxy to forward web traffic from 10.0.1.60 and then connected to the web server using Firefox. Upon connecting to the web server, Finals-[redacted] received JSON data that included current readings, health status, and configured alert thresholds without requiring any authentication. Attackers could use this information to identify if an attack is successfully controlling NGPEW infrastructure.

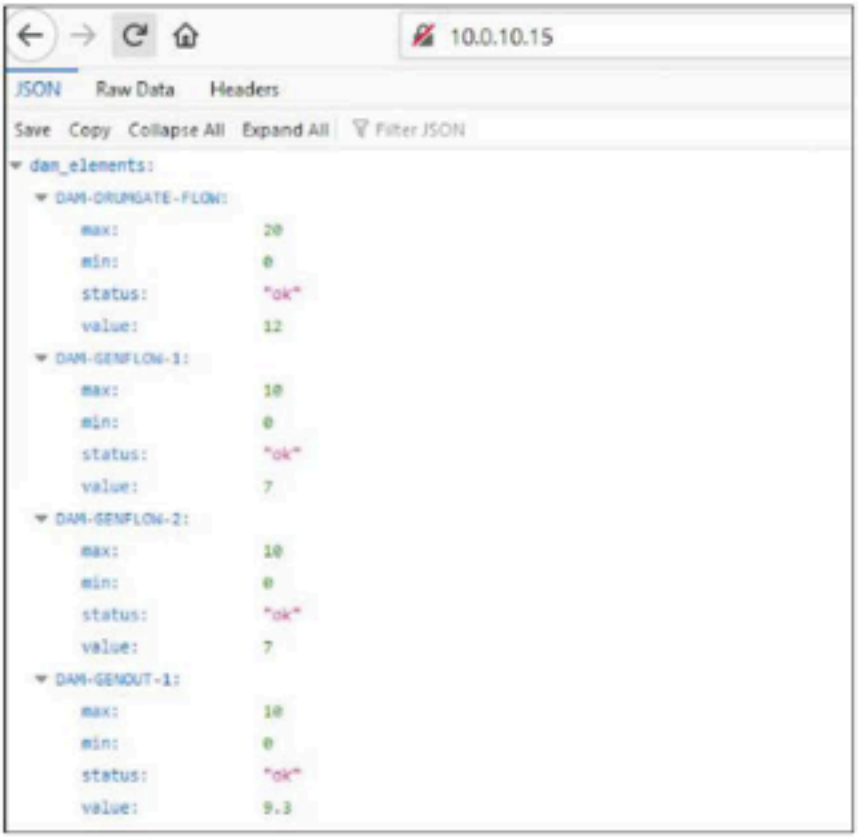


***Figure 8.1**: The API endpoint showing current readings from dam sensors*

Affected Host

- 10.0.10.15

Recommendation

- Restrict access to only devices and users which must access the data

9 - DNS Enumeration

LOW RISK (2/10)	
Exploitation Likelihood	**Likely**
Business Impact	**Mild**
Remediation Difficulty	**Easy**

Security Implications

DNS enumeration allows attackers to query the DNS server to retrieve information about the hosts in the network. Attackers can use this information to plan attacks on NGPEW and facilitate future attacks.

Analysis

Finals-[redacted] identified the domain controller was running a DNS server. By using the nslookup command, Finals-[redacted] was able to perform reverse-ip lookups and find the internal DNS names for a given IP address. The DNS name may provide information about the services the host is running. This allows an attacker to get information about potential targets without directly accessing target systems.

```
COMMAND $> nslookup 10.0.5.151 10.0.1.100
151.5.0.10.in-addr.arpa        name = db.services.millenialpower.us.

Authoritative answers can be found from:
```

***Raw Data 9.1**: Using nslookup to identify that 10.0.5.151 is actually a database server*

Affected Host

- 10.0.1.100

Recommendations

- Block DNS queries from external sources

10 - Information Disclosure

LOW RISK (2/10)	
Exploitation Likelihood	Likely
Business Impact	Mild
Remediation Difficulty	Easy

Security Implications

Exposed debug information allows attackers to gather information about the web server's configuration which entices an attacker to probe the web server further and find other vulnerabilities.

Analysis

Finals-[redacted] setup a socks5 proxy on 10.0.1.60 to forward web traffic. Finals-[redacted] used the proxy to access the "killbill" web server at 10.0.5.75. Upon clicking the buttons on the webpage, Finals-[redacted] was brought to web pages that showed the current state of the Java application and debug information.

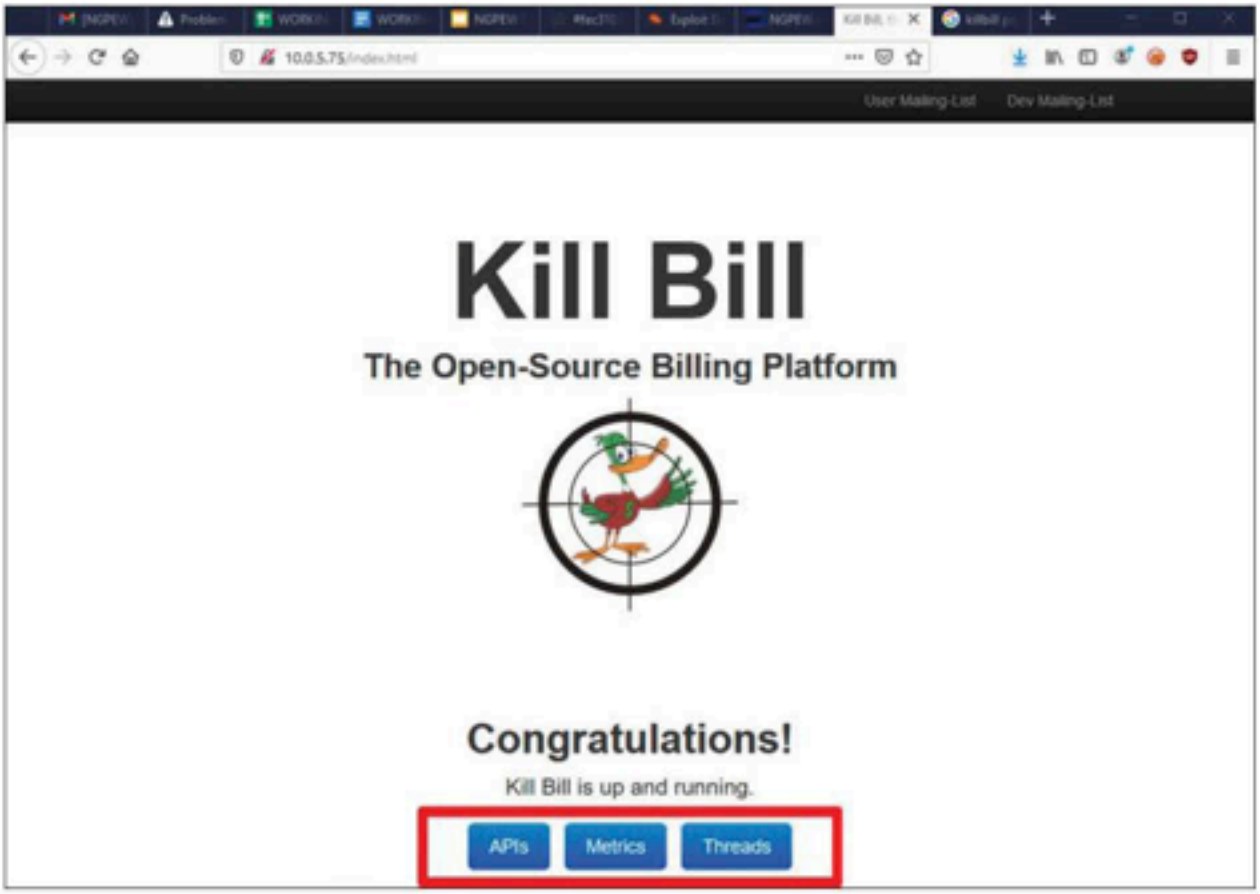


***Figure 10.1**: Kill Bill advertising various debug views on the home page.*

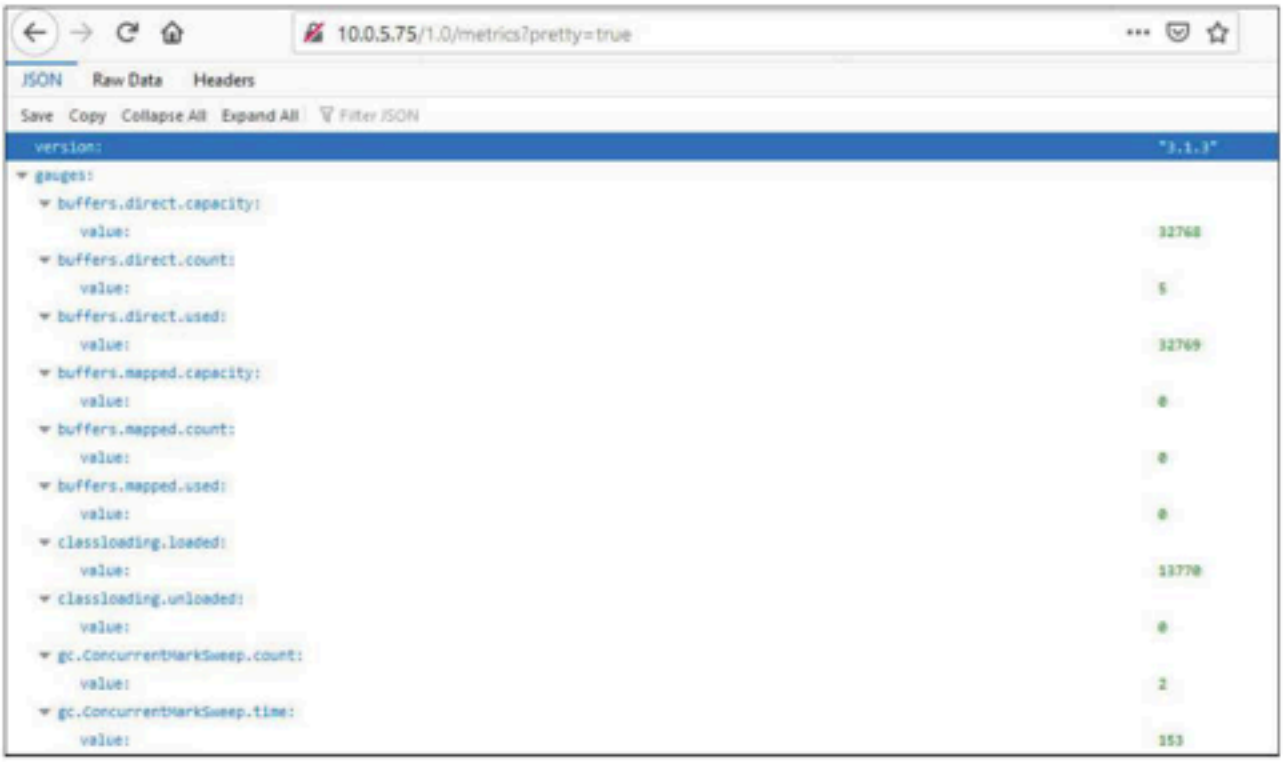


***Figure 10.2**: Debug views show detailed information about the program.*

During testing, Finals[redacted] identified that the web server would return verbose error messages. The verbose error messages show the webserver is running Apache Tomcat version 8.5.16. This information can be used by attackers to craft exploits for the specific version of the platform.

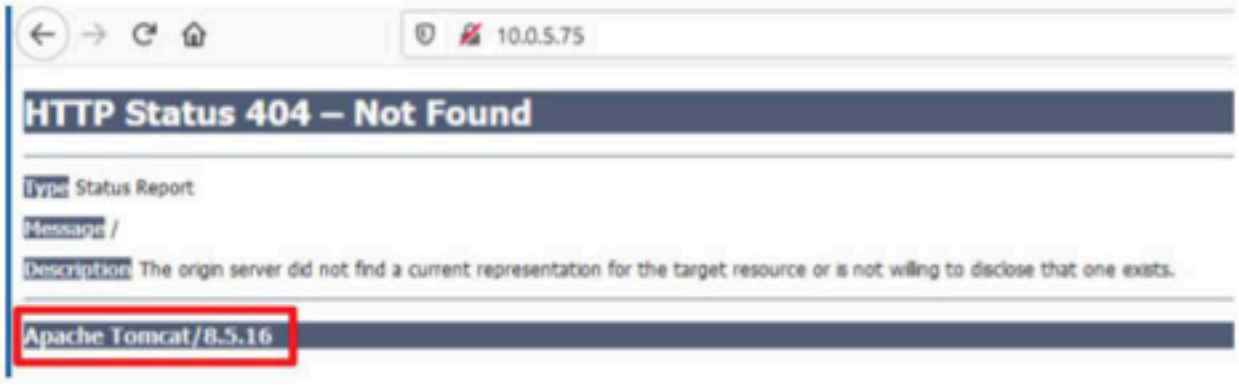


***Figure 10.3**: Error message shows detailed server information*

Affected Host

- 10.0.5.75

Recommendations

- Configure Tomcat to restrict access to debug views
- Change Tomcat's default error page to not include the server version

References

- https://www.computerworld.com/article/2769025/how-to-restrict-access-to-web-applications-in-tomcat.html

11 - End of Life Software

LOW RISK (2/10)	
Exploitation Likelihood	**Unlikely**
Business Impact	**Mild**
Remediation Difficulty	**Medium**

Security Implications

The web server 10.0.5.152 runs Microsoft IIS 4.0. Microsoft IIS 4.0 is no longer supported. Also located on 10.0.5.75 is a MySQL database version 5.5.5. This is also end of life and unsupported. Any new vulnerabilities will not be patched, meaning these vulnerabilities will remain on systems, and will be at risk of being exploited.

Analysis

Testing of the web server revealed Microsoft IIS 4.0 is being run. Further research found that this version of Microsoft IIS is an end of life software. Microsoft is no longer supporting IIS 4.0, and is not making new vulnerability patches. This leaves the web server vulnerable to attackers who discover new vulnerabilities on this web server. This also for the MySQL 5.5.5 database. Attackers who exploit these might have the ability to achieve privilege escalation, exfiltrate confidential data, or gain remote code execution.

```
GET / HTTP/1.1
Host: 10.0.5.152
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sat, 09 Jan 2021 19:20:03 GMT
If-None-Match: "8042286ebce6d61:b0e"
Cache-Control: max-age=0


HTTP/1.1 304 Not Modified
```

```
Server: Microsoft-IIS/4.0
Date: Sat, 09 Jan 2021 19:44:23 GMT
PICS-Label: (PICS-1.0 "http://www.rsac.org/ratingsv01.html" l by "easteregg@jrwr.io" on
"2020.09.04T03:21--100" exp "2021.09.04T12:00--100" r (v 0 s 0 n 0 l 4))
Cache-Control: max-age=1800
Expires: Sat, 09 Jan 2021 20:14:23 GMT
Connection: close
Content-Location: http://10.0.5.152/index.html
ETag: "0f3de674f94d61:b0e"
```

***Figure 11.1**: HTTP response output from the web server*

```
msf6 auxiliary(scanner/mysql/mysql_version) > set rhosts 10.0.5.75
rhosts => 10.0.5.75
msf6 auxiliary(scanner/mysql/mysql_version) > exploit

[+] 10.0.5.75:3306        - 10.0.5.75:3306 is running MySQL 5.5.5-10.3.14-MariaDB-
)
[*] 10.0.5.75:3306        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

***Figure 11.2**: Metasploit response showing MySQL version*

Affected Hosts

- 10.0.5.152
- 10.0.5.75

Recommendations

- Update Microsoft IIS to the latest version, currently IIS 10.0
- Update MySQL to the latest version, currently 8.0

APPENDIX A - LIMITATIONS

The following limitations affected the assessment performed by Finals-[redacted] Consulting and the content included in the report.

Access to 10.0.5.0/24 and 10.0.10.0/24 subnets

Finals-[redacted] Consulting received credentials from client to the security.corp.millenialpower.us host (10.0.1.60) at 1:07pm on 9 January 2021. Prior to receiving access to this additional testing machine, Finals-[redacted] Consulting did not have network access to the 10.0.5.0/24 "support" network nor the 10.0.10.0/24 "power" network. Limited time with access to these networks may have resulted in an incomplete assessment of these networks' security.

Limitations on PLC Modbus Tests

Finals-[redacted] Consulting was unable to test write permissions on the PLCs (10.0.10.50-65) as the control systems were connected to critical infrastructure that was already unstable. Testing these systems could result in loss-of-life if the systems are overloaded.

APPENDIX B - TOOLS USED

TOOL	DESCRIPTION
RADAR	Program for distributed command execution and automation.
BurpSuite Community Edition	Used for testing of web applications.
Zed Attack Proxy	Used for testing of web applications.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
Greenbone Security Assistant	Used to scan the networks for vulnerabilities.
SSLScan	Used to determine SSL configuration of hosts
dirb	Used to discover web directories via brute-force
nikto	Web application vulnerability scanner

Table B.1: *Tools used during assessment*

APPENDIX C - ENGAGEMENT INFORMATION

Client Information

Client	Next-Generation Power, Electric & Water
Primary Contact	Gaylord Schaefer, Director of Information Technology
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement • Gaylord Schaefer

Deliverables

Filename	Date	Description
NGPEW_2021Q1_Retest_PentestReport.pdf	10 Jan 2021	Final report
NGPEW_2021Q1_Retest_Fi[redacted]_Presentation.pptx	10 Jan 2021	Executive Presentation

Contact Information

Name	Finals-[redacted] Consulting
Address	1001 Fake Street, Gotham, NY 11201
Phone	[redacted]
Email	[redacted]