

CyberApolis Water Breach Report

Reese Gerjekian

Department of Homeland Security

May 1, 2024

Table of Contents

Executive Summary.....3

Introduction.....3

 1. Reconnaissance.....4

 2. Scanning.....6

 3. Exploitation.....8

 4. Post-Exploitation.....13

 5. Summary and Mitigation..... 14

Executive Summary

In response to the imminent threat posed by Carbon Spector, the DHS Cyber Operations team successfully averted a potentially devastating attack at CyberApolis Water Company. Our strategic cybersecurity measures focused on securing the company's critical infrastructure, particularly by accessing the HMI controls on water.cyberapolis.gov and promptly shutting down the dam's floodgates. The team utilized acquired intelligence to identify and neutralize vulnerabilities through a systematic approach involving reconnaissance, scanning, and exploitation phases. Swift post-exploitation measures were implemented, demonstrating our commitment to collaboration with local authorities and adherence to established security protocols.

Introduction

The DHS Cyber Operations team was mobilized in response to a coordinated threat by Carbon Spector against the CyberApolis Water Company, aimed at causing a city-wide flood. This report details our cybersecurity intervention that mitigated the risks and protected the city. Intended for non-technical stakeholders such as the CEO, FBI Assistant Director, and the Mayor of CyberApolis, it highlights the team's proactive measures and the importance of strategic cybersecurity in protecting vital systems. The operations covered include reconnaissance, scanning, exploitation, and post-exploitation phases, emphasizing the effectiveness of our approach in securing the company's critical infrastructure.

1. Reconnaissance

In the reconnaissance phase, our primary goal was to pinpoint potential vulnerabilities within the CyberApolis Water Company's online infrastructure. We meticulously examined

critical areas of the company's website, such as the About Us, Careers, News, Pay Your Bill, and Employee Portal sections, to gather actionable intelligence.

- About Us Page:** This section disclosed essential documents like the annual report, which became a focal point for our analysis. The information contained within these documents provided insights into the website's administrative structure and highlighted potential security lapses.

CyberApolis Municipal Water

[ABOUT US](#) [CAREERS](#) [NEWS](#) [PAY YOUR BILL](#)

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?"


- Contacts Page:** This page lists details of several company employees, offering a deeper view of the organizational hierarchy and possible entry points for social engineering tactics.




JOHN BARNES
Senior Software Engineer
(505) 555-1234




JOHN BARNES
Senior Software Engineer
(505) 555-1234




JOHN BARNES
Senior Software Engineer
(505) 555-1234




JOHN BARNES
Senior Software Engineer
(505) 555-1234




JOHN BARNES
Senior Software Engineer
(505) 555-1234



JOHN BARNES
Senior Software Engineer
(505) 555-1234



JOHN BARNES
Senior Software Engineer
(505) 555-1234



JOHN BARNES
Senior Software Engineer
(505) 555-1234

- **Pay Your Bill Page:** This interface, crucial for transactions, includes fields for account number, last name, and zip code. These all present opportunities for injection attacks, prompting a thorough security review.

CyberApolis Municipal Water

Pay Your Bill

We welcome you to convenient pay your bills online using our new and improved system.

Account Number:

Last Name:

Zipcode:

[CONTINUE](#)

- **Employee Portal:** The portal's login interface, with username and password fields, was specifically scrutinized for vulnerabilities that could allow injection attacks, underscoring the need for enhanced security measures in these areas.

CyberWater [Log In](#)

Log in.

Username

Password

☐ Remember me?

[Log in](#)

Our reconnaissance was instrumental in mapping CyberApolis Water Company's digital landscape, highlighting potential breach points and laying the groundwork for the targeted scanning and exploitation phases. The analysis of various web interfaces provided a

comprehensive understanding of the security posture and helped identify critical areas requiring immediate attention.

2. Scanning

Building on the intelligence acquired during reconnaissance, the scanning phase was crucial in delving deeper into the CyberApolis Water Company's network infrastructure to identify and assess vulnerabilities.

- **IP Address Identification:** We began by pinpointing the IP address of the company's main site using a simple ping command in PowerShell, which revealed the address as 10.139.45.148.

```
(root@kali) - [/]
# ping -c 4 water.cyberapolis.gov
PING water.cyberapolis.gov (10.139.45.148) 56(84) bytes of data.
64 bytes from 10.139.45.148 (10.139.45.148): icmp_seq=1 ttl=64 time=0.967 ms
64 bytes from 10.139.45.148 (10.139.45.148): icmp_seq=2 ttl=64 time=0.545 ms
64 bytes from 10.139.45.148 (10.139.45.148): icmp_seq=3 ttl=64 time=0.581 ms
64 bytes from 10.139.45.148 (10.139.45.148): icmp_seq=4 ttl=64 time=0.529 ms

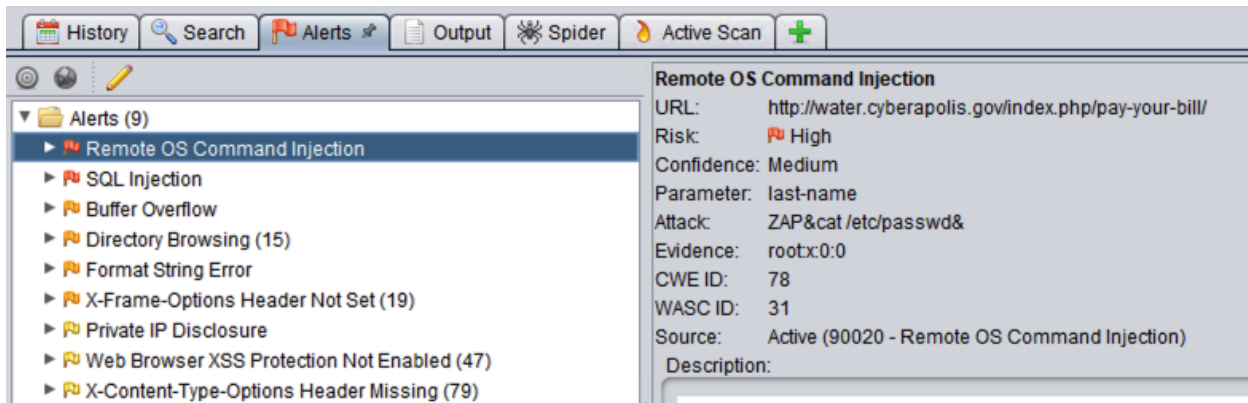
--- water.cyberapolis.gov ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.529/0.655/0.967/0.180 ms
```

- **Network Scan Using Nmap:** We conducted a scan of the network using Nmap to discover open ports. We identified several open ports (21/TCP, 22/TCP, 79/TCP, and 80/TCP) that could potentially be exploited.

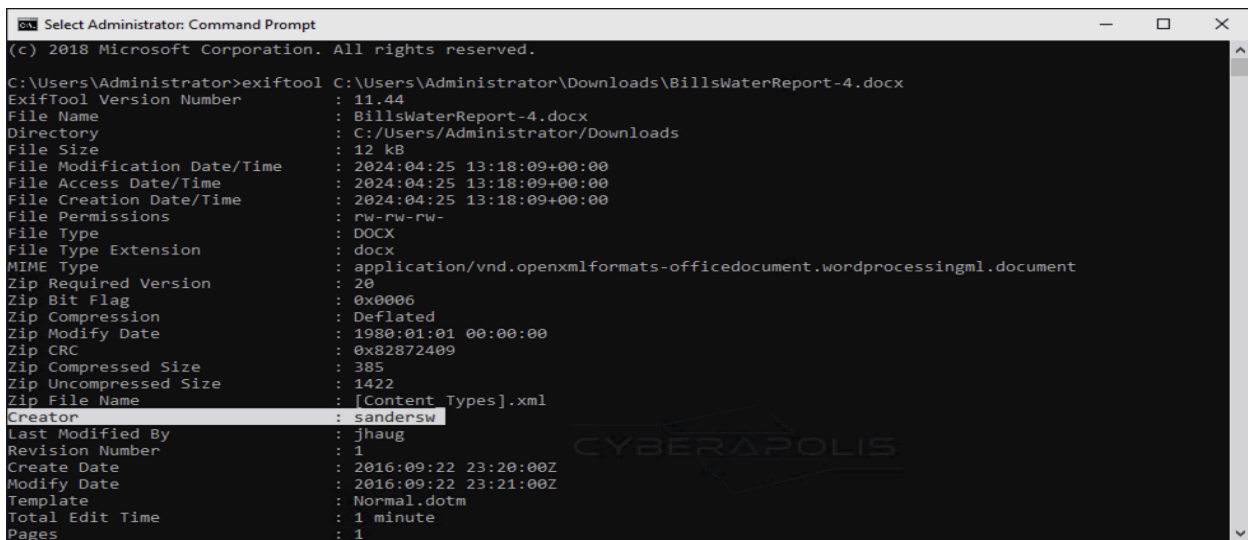
```
(root@kali) - [/]
# nmap 10.139.45.148
Starting Nmap 7.91 ( https://nmap.org ) at 2024-04-25 15:09 UTC
Nmap scan report for 10.139.45.148
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
79/tcp    open  finger
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

- Zap Analysis:** Using the OWASP ZAP tool, we launched simulated attacks on the "water.cyberapolis.gov" domain to identify vulnerabilities. Notably, a high-risk alert was triggered for a possible remote OS command injection vulnerability on the "Pay Your Bill" page, highlighting a significant security threat.



- Metadata Scanning Using Exiftool:** To confirm the depth of access potential attackers could achieve, we scanned the metadata of key documents using Exiftool. The analysis of the "BillsWaterReport-4.docx" file revealed the creator's username as "sandersw," linking it directly to employee portal access, thereby confirming a critical security concern.



The comprehensive data collected through network scans and vulnerability analysis tools like Zap provided pivotal insights into the company's defenses, pointing us toward specific vulnerabilities that must be addressed immediately in the exploitation phase. These findings were critical for planning precise and effective security interventions to safeguard the company's digital assets.

3. Exploitation

Having identified vulnerabilities during the scanning phase, our team moved into the exploitation phase with precision. The focus was primarily on the website's "Pay Your Bill" section, where a remote command injection vulnerability was discovered.

- **SQL Injection Analysis:** We initially tested the SQL injection vulnerability by inserting specialized commands into the input fields for account numbers, last names, and zip codes. These efforts revealed system information without triggering security alerts.

```
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$0skWE/17$f2WGrb2wqbX0ov3lbFKIZ0:17113:0:99999:7:::
dtomlinson:$1$BoIp//u1$XiGhxr12s4051AWB/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$MuMixwfUmX0Bnx5jppcYm.:17113:0:99999:7:::
mwilson:$1$mpu0S/Je$NWX57pcxT4Xu9ej/8ZxZI.:17113:0:99999:7:::
ghillman:$1$m7jQn/WV$Rdqfg0C35HX2xrHst81KX.:17113:0:99999:7:::
kwrotten:$1$37xt/Qs0$mdLeCS.MfqweuhnSP3cD31:17113:0:99999:7:::
phamm:$1$BtmNO3yS$OC0joLquOVbxqQuXgo1Fu0:17113:0:99999:7:::
srivera:$1$.0Jwb/b/$aHP6MFAc5ffq4V0tVz7dc/:17113:0:99999:7:::
jroberson:$1$cekti/23$UA7FGiVxTTIxDdoZabiyL1:17113:0:99999:7:::
```

Account Number:

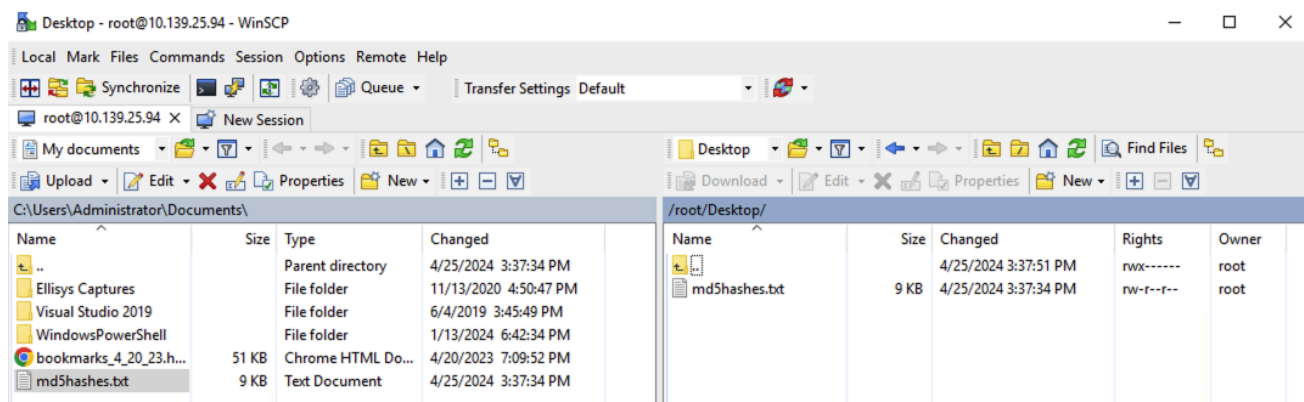
Last Name:

Zipcode:

- Successful SQL Injection:** After refining our techniques, we escalated our efforts with a more sophisticated SQL injection, targeting all three fields simultaneously. This maneuver successfully extracted critical data, including server IP addresses and hashed credentials, highlighting the extent of the vulnerability.



- File Transfer and Analysis:** Utilizing WinSCP, we securely transferred the extracted file containing hashed user credentials to our analysis environment on Kali Linux. This allowed us to proceed with decryption in a controlled setting.



- **Password Cracking:** We deployed 'John the Ripper,' a password-cracking tool, to decrypt the hashed credentials. The successful decryption provided us with direct access to the employee portal.

```
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)  
alb2c3d4         (dnewsome)  
4runner          (wsanders)  
1q2w3e4r         (kburkhardt)  
7dwarfs          (kmciver)  
57chevy          (jkeener)  
123go            (wgilbert)
```

- **Verification and Access Control:** Following decryption, we verified the integrity of the cracked passwords and utilized these credentials to access the employee portal, paving the way for mitigation actions and securing the HMI controls.

```
(rootkali) - [~/john]  
# cat john.pot  
$1$6k844/y4$q9d8qZm30oTfyuoug16MZ0:8675309  
$1$stPBi.qR$ljYMgKcPUaXK68l0Y95dJ/:alb2c3d4  
$1$2kMh5/cp$XAZKEUB/lpqkP7AQamVwS.:4runner  
$1$iqTazmxS$lgbQaQBwLrLDcDLlcac0E1:1q2w3e4r  
$1$.nlge/0S$HpQ8y2XeaVmLEUT8REBEB.:7dwarfs  
$1$MYLgsdvI$4JhSWoXCfLsxJ.fI/g4Yn.:57chevy  
$1$fXoRxjo0$Pl5LymzaHtCCRJkzyQvd0:123go
```

- **Employee Portal Access:** Utilizing the cracked credentials, we achieved unauthorized access to the employee portal. This breakthrough allowed us to control critical operational features from within the system. The confirmed usernames and passwords that we obtained and utilized are as follows:

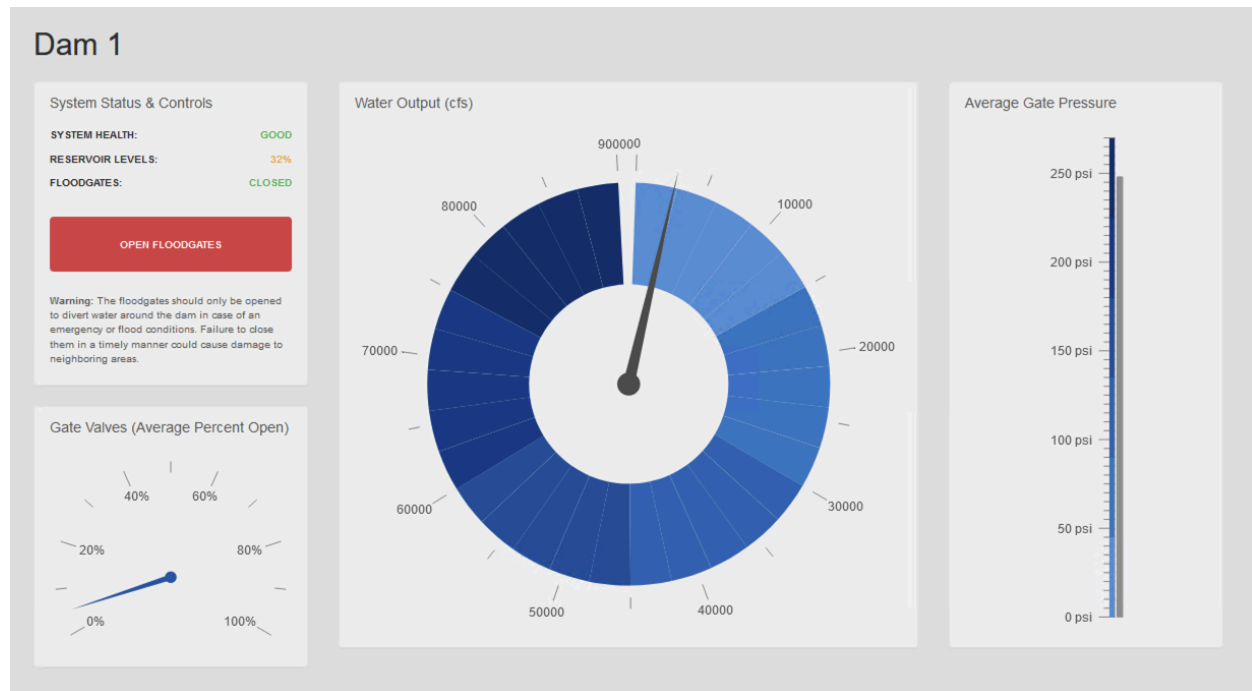
Username	Password
kgriffin	8675309
dnewsome	a1b2c3d4
wsanders	4runner
kburkhardt	1q2w3e4r
kmciver	7dwarfs
jkeener	57chevy
wgilbert	123go

- **Access to HMI Controls:** The access to the employee portal revealed critical usernames and passwords necessary for accessing the HMI controls, which manage the operational parameters of the dam's floodgates. To ensure effective management, a modification to the username structure was required. The confirmed credentials for HMI control access, which we successfully utilized to manage the dam's floodgates, are as follows:

Username	Password
newsomed	a1b2c3d4
sandersw	4runner

- **Successful Closure of the Floodgates:** Leveraging the access obtained through the employee portal, we executed commands to control the HMI systems operating the dam's floodgates. This critical step was conducted under strict operational protocols to ensure safety and minimize risk to infrastructure. We successfully closed the floodgates,

preventing the imminent threat of flooding and securing the water company's infrastructure from further manipulation.



4. Post-Exploitation

The post-exploitation phase focused on securing the compromised systems and preventing any future unauthorized access, ensuring the integrity of CyberApolis Water Company's operations.

- **Immediate Security Measures:** We initiated immediate containment measures, deactivating compromised accounts to prevent unauthorized access and setting up a comprehensive monitoring system to detect suspicious activities.
- **System Cleanup and Patching:** A thorough cleanup was conducted to remove any traces of intrusion. All systems were updated and patched to close off the vulnerabilities exploited during the attack.

- **Account Security Overhaul:** All affected user accounts underwent a security overhaul, with passwords reset and multi-factor authentication added to enhance security.
- **Continuous Monitoring and Logging:** Enhanced monitoring tools were installed to monitor network traffic and activities continuously, ensuring any anomalies are detected and addressed promptly.
- **Stakeholder Communication and Coordination:** We maintained open lines of communication with all relevant stakeholders, providing updates on the situation and coordinating with local law enforcement to bolster security measures.
- **Documentation and Legal Compliance:** Detailed documentation of the breach and subsequent actions was compiled for internal records and compliance with legal requirements, ensuring transparency and accountability.

5. Summary and Mitigation

In summary, our response to the cybersecurity breach at CyberApolis Water Company was complete. It addressed immediate threats and laid the groundwork for robust long-term security improvements.

- **Strategic Mitigations Implemented:** Following the breach, we rolled out strategic mitigations, including installing state-of-the-art security software and hardware and redesigning network architecture to enhance defenses against potential cyber-attacks.
- **Employee Training and Awareness:** Recognizing the importance of human factors in cybersecurity, we implemented regular training sessions for all employees, focusing on security best practices and awareness of phishing and other cyber threats.

- **Regular Audits and Assessments:** We instituted a schedule of regular security audits and vulnerability assessments to identify and address potential security gaps proactively.
- **Community and Industry Engagement:** Finally, we engaged with the broader community and industry peers to share learnings and best practices, fostering a collaborative approach to cybersecurity.

These actions not only restored the security of the CyberApolis Water Company's systems but also enhanced their resilience against future cyber threats, ensuring the safety and reliability of critical infrastructure.