D2 | CYBERSECURITY

Perimeter Security Services for Technology Risk Management

2022 TRICO Planning Retreat

Gloucester, Salem, Cumberland Counties Municipal Joint Insurance Fund
Established in 1991
South Jersey Communities Securing Their Future

Presented by:

Suby Gupta
President

28 WORLDS FAIR DRIVE
SOMERSET NJ 08873

732.507.7320
D2CYBERSECURITY.COM

Introduction

D2 CYBERSECURITY

D2 Cybersecurity has been contracted by the TRICO Municipal Joint Insurance Fund as a valued strategic partner in delivering world class Network Vulnerability Assessment and External Penetration Testing to identify and reduce its members cyber exposure and susceptivity.

We have over 20 years of experience involving real time traffic monitoring, deep packet inspection and forensic analysis of some of the most complex networks in the world.

Our parent company, AIP is a provider of interactive training, software solutions, and digital communications services for the United States Government, as well as various healthcare, academic, corporate clients.

Our team comprises of highly proficient and certified security professionals.

Our Mission

D2 | CYBERSECURITY

- Discover, Report, and furnish steps to Remediate your perimeter weaknesses before the hackers can breach.
- Immediate communication on all critical findings & successful intrusions.
- Actionable Reports to Municipalities and Monthly briefings to JIF.
- Economy of scale via service automation & dedicated reporting portal.
- Detail remediation recommendations to each Members.

Perimeter Security Services

D2 | CYBERSECURITY

- Our current service components for the FUND consist of:
  - **Network Vulnerability Assessment**: **is similar to visually inspecting the locks in the doors & windows in your building!**
  - **External Penetration Testing**: **is analogous to attempting to break in either through the doors or windows without the intention of actual burglary!**
- The results of these services will help you to identify your perimeter security gaps which have been overlooked, but that an attacker would likely find and exploit.

Deliverables:

1. An **Executive Summary** that gives a high-level overview of the scope, testing performed, and assessment results.
2. A **Detailed Technical** report including:
   - Attack summary, and
   - Findings and remediation actions

Why Vulnerability Assessment?

D2 | CYBERSECURITY

Conducting a Network Vulnerability Assessment (NVA) has numerous benefits, including:

- **Identifying vulnerabilities before hackers find them**. NVA scans all the network components, verifying whether they have weaknesses that cybercriminals can use to attack the organization.
- **Proving to your taxpayers, and other stakeholders that your systems are secure.** You need to assure taxpayers who have entrusted you with their data that you can protect their assets. You can use vulnerability assessment as a cyber loss control tool to reduce cyber insurance claims.
- **Evaluating the performance of third-party IT service providers.** If you rely on third-party vendors for IT solutions such as email, backup or system administration, an independent NVA can help you cross-check their performances.
- **Complying with industry and regulatory requirements.** If you operate in a regulated sector, a rigorous NVA can help you comply. NVA is also critical to achieving and retaining security certifications such as ISO 27001 and others.
- **Saving time and costs.** Security breaches can hurt an organization on many fronts, creating limitations and liabilities that are costly. NVA mitigates such risks, allowing the organization to save time and stop expensive litigations arising from data breaches.

NVA Sample Report Snapshot

D2 | CYBERSECURITY

D2 | CYBERSECURITY

Analyze | Educate | Train | Communicate

External Vulnerability Assessment Report

Vineland City

D2|Cybersecurity

Report generated by Nessus™ Tue, 15 Mar 2022 21:00:05 Eastern Standard Time

199.245.253.194

5	19	15	1	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Tue Mar 15 21:25:44 2022
End time: Tue Mar 15 21:51:08 2022

Host Information

DNS Name: vmupay.vinelandcity.org
IP: 199.245.253.194
OS: Microsoft Windows 10 Enterprise

Vulnerabilities

95438 - Apache Tomcat 6.0.x < 6.0.48 / 7.0.x < 7.0.73 / 8.0.x < 8.0.39 / 8.5.x < 8.5.8 / 9.0.x < 9.0.0.M13 Multiple Vulnerabilities

Synopsis

The remote Apache Tomcat server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the Apache Tomcat service running on the remote host is 6.0.x prior to 6.0.48, 7.0.x prior to 7.0.73, 8.0.x prior to 8.0.39, 8.5.x prior to 8.5.8, or 9.0.x prior to 9.0.0.M13. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists that is triggered when handling request lines containing certain invalid characters. An unauthenticated, remote attacker can exploit this, by injecting additional headers into responses, to conduct HTTP response splitting attacks. (CVE-2016-6816)

- A denial of service vulnerability exists in the HTTP/2 parser due to an infinite loop caused by improper parsing of overly large headers. An unauthenticated, remote attacker can exploit this, via a specially crafted request, to cause a denial of service condition.
Note that this vulnerability only affects 8.5.x versions. (CVE-2016-6817)

- A remote code execution vulnerability exists in the JMX listener in JmxRemoteLifecycleListener.java due to improper deserialization of Java objects. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-8735)

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

199.245.253.194 92

See Also

http://www.nessus.org/u?1e8a81e1
http://www.nessus.org/u?1c7e7b23
http://www.nessus.org/u?833cb56a
http://www.nessus.org/u?87d6ed56
http://www.nessus.org/u?5f7bb039

Solution

Upgrade to Apache Tomcat version 6.0.48 / 7.0.73 / 8.0.39 / 8.5.8 / 9.0.0.M13 or later.

Risk Factor

High

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

References

BID	94097
BID	94461
BID	94463
CVE	CVE-2016-6816
CVE	CVE-2016-6817
CVE	CVE-2016-8735

Plugin Information

Published: 2016/12/01, Modified: 2020/03/11

Plugin Output

tcp/443/www

```
Installed version : 7.0.39
Fixed version     : 7.0.73
```

199.245.253.194 93

DISTRIBUTABLE COPY

Why Penetration Testing?

D2 | CYBERSECURITY

- Recent study by **Ponemon Institute** that surveyed *350 Municipalities* in the nation, more than half of them (53%) said that cyber breaches were a result of system glitches and human errors.
- Recent research by **Barracuda Networks** indicates that 44% of global ransomware attacks in 2021 targeted Municipalities.
  - Often strapped with small IT departments, aging computer systems and limited budgets to allocate to cybersecurity, local governments across the country make for ill-equipped and easy targets for cybercriminals.
  - As the gatekeepers for voter records, tax information, social security numbers and essential access information to the full range of critical infrastructure managed in the municipality's workload, it is of little surprise that they have become a focal point of cyberattacks.
- The main reason Penetration Tests are crucial to a municipality's security is that they help personnel learn how to handle any type of break-in from a malicious entity.
  - It serves as a type of fire drill to examine whether your municipality's security implementation are genuinely effective.
  - It also provide solutions that will help organizations to not only prevent and detect attackers but also to expel such an intruder from your systems in an efficient way.

Pen Test Sample Report Snapshot

D2 CYBERSECURITY

D2 CYBERSECURITY

CONFIDENTIAL

AUTHORIZED EYES ONLY

External Network Penetration Test Report

Borough of Stone Harbor

February

2022

D2 CYBERSECURITY

Above Average Standard Below Average

Testing Area	Above Average	Standard	Below Average
External Network		●	

Conclusion: Stone Harbor meets the security level that D2 Cybersecurity typically finds when compared to organizations of a similar size and organizations in the same industry.

Summary of Findings

Below is a summary of issues identified during our testing. A detailed explanation of risk levels can be found later in this report, but the following are very basic definitions:

- **Critical:** Could directly lead to a security incident if discovered by an attacker.
- **High:** Could help lead to a security incident if discovered or could allow for additional access to information and systems in the event of a security incident.
- **Medium:** Could be used in combination with other vulnerabilities to create a security incident or used by an attacker to further extend a security incident.
- **Low:** Could be used to divulge information or create an issue that could combine with other vulnerabilities to lead to a security incident.

Please note that organizations often do not remediate some items because of business or system requirements, mitigating controls, or risk acceptance calculations. This information is provided to facilitate informed decisions regarding the reduction of risk within the context of business requirements.

External Network Vulnerabilities

Risk	Vulnerability	Issue Scope
Critical	Unsupported Microsoft IIS 7.5 Web Server	1 Host
Critical	Unsupported Microsoft Exchange Server	1 Host
Critical	Default Password '1234' for 'admin' Account on Internet Exposed Device	1 Host
Medium	Unencrypted Web Login Page	1 Host

Remediation Recommendations

The security of the external network appeared to be satisfactory. However, D2 Cybersecurity recommends the following remediation action be evaluated to further increase security:

- Update host [redacted] to current versions of Microsoft IIS and Exchange Server
- Change the password on the VMS portal to a secure password that cannot be guessed by an attacker and force the use of HTTPS encryption on the device's web login page.

Future Penetration Testing

Based on the results of this test, D2 Cybersecurity recommends that a subsequent penetration test be conducted on the external network, under similar or identical parameters to this test, within one-year. Further, D2 Cybersecurity recommends an email phishing assessment and an internal network penetration test to evaluate other potential information technology attack surfaces.

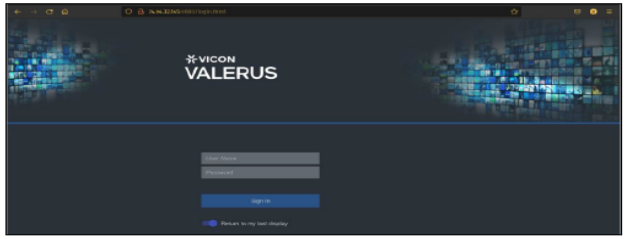


FIGURE 4: INTERNET EXPOSED LOGIN LOCATED AT HTTP://74.94.32.145:9080/

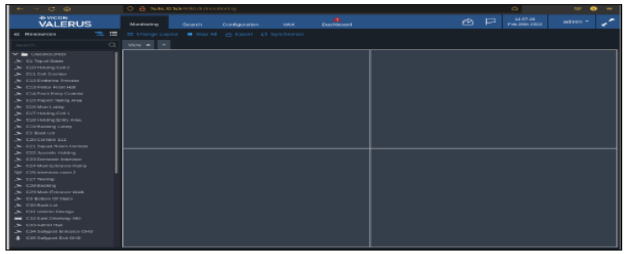


FIGURE 5: LOGGED INTO THE DEVICE WITH DEFAULT CREDENTIALS, WITH ~40 CAMERAS AND DEVICES LISTED IN LEFT PANEL

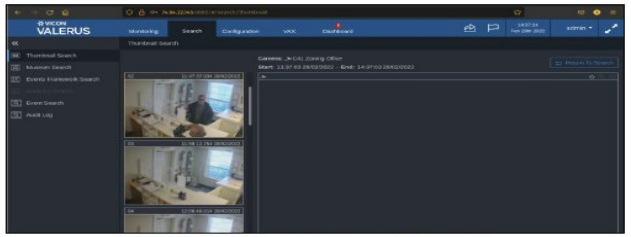


FIGURE 6: ACCESS TO LIVE CAMERAS AND RECORDED VIDEOS

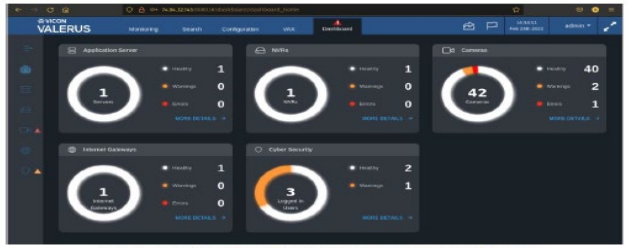


FIGURE 7: ACCESS TO ADMINISTRATIVE FUNCTIONS ON THE VMS PLATFORM

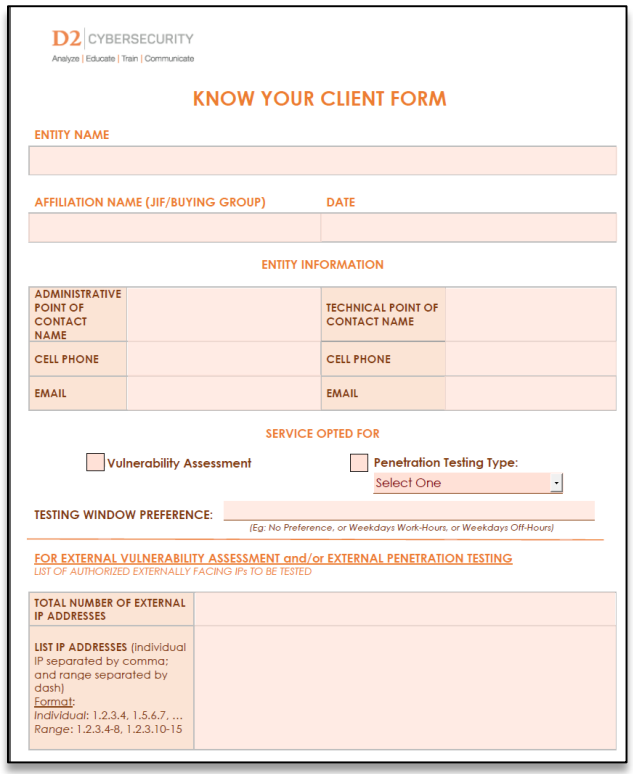
DISTRIBUTABLE COPY

How do you get started?

D2 | CYBERSECURITY

The service is already paid for you by TRICO

1. Fill out and return the fillable KYC PDF form



D2 | CYBERSECURITY
Analyze | Educate | Train | Communicate

KNOW YOUR CLIENT FORM

ENTITY NAME

AFFILIATION NAME (JIF/BUYING GROUP) DATE

ENTITY INFORMATION

ADMINISTRATIVE POINT OF CONTACT NAME		TECHNICAL POINT OF CONTACT NAME	
CELL PHONE		CELL PHONE	
EMAIL		EMAIL	

SERVICE OPTED FOR

☐ Vulnerability Assessment ☐ Penetration Testing Type: Select One

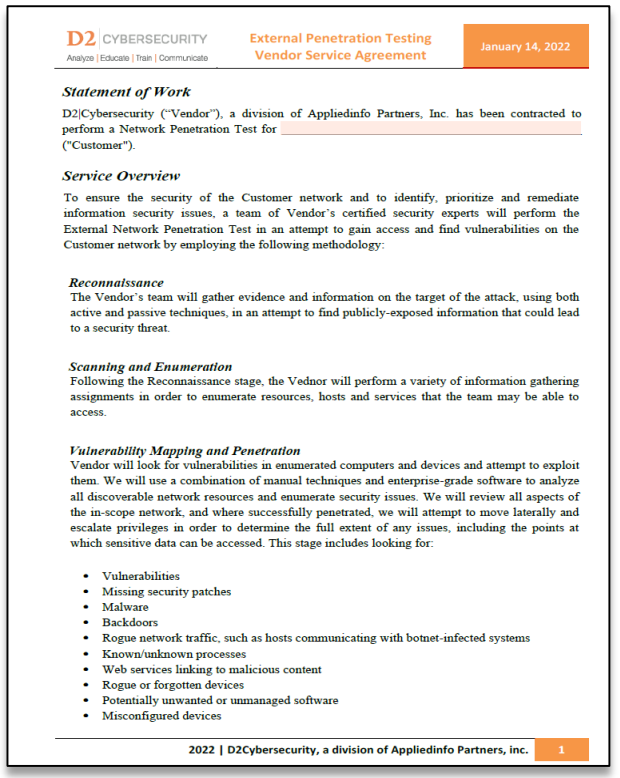
TESTING WINDOW PREFERENCE:
(Eg: No Preference, or Weekdays Work-Hours, or Weekdays Off-Hours)

FOR EXTERNAL VULNERABILITY ASSESSMENT and/or EXTERNAL PENETRATION TESTING
LIST OF AUTHORIZED EXTERNALLY FACING IPs TO BE TESTED

TOTAL NUMBER OF EXTERNAL IP ADDRESSES	
LIST IP ADDRESSES (individual IP separated by comma; and range separated by dash) Format: *Individual*: 1.2.3.4, 1.5.6.7, … *Range*: 1.2.3.4-8, 1.2.3.10-15	

DONE

2. Sign and return the fillable VSA PDF form



D2 | CYBERSECURITY
Analyze | Educate | Train | Communicate

External Penetration Testing Vendor Service Agreement

January 14, 2022

Statement of Work

D2|Cybersecurity ("Vendor"), a division of Appliedinfo Partners, Inc. has been contracted to perform a Network Penetration Test for _____ ("Customer").

Service Overview

To ensure the security of the Customer network and to identify, prioritize and remediate information security issues, a team of Vendor's certified security experts will perform the External Network Penetration Test in an attempt to gain access and find vulnerabilities on the Customer network by employing the following methodology:

Reconnaissance
The Vendor's team will gather evidence and information on the target of the attack, using both active and passive techniques, in an attempt to find publicly-exposed information that could lead to a security threat.

Scanning and Enumeration
Following the Reconnaissance stage, the Vednor will perform a variety of information gathering assignments in order to enumerate resources, hosts and services that the team may be able to access.

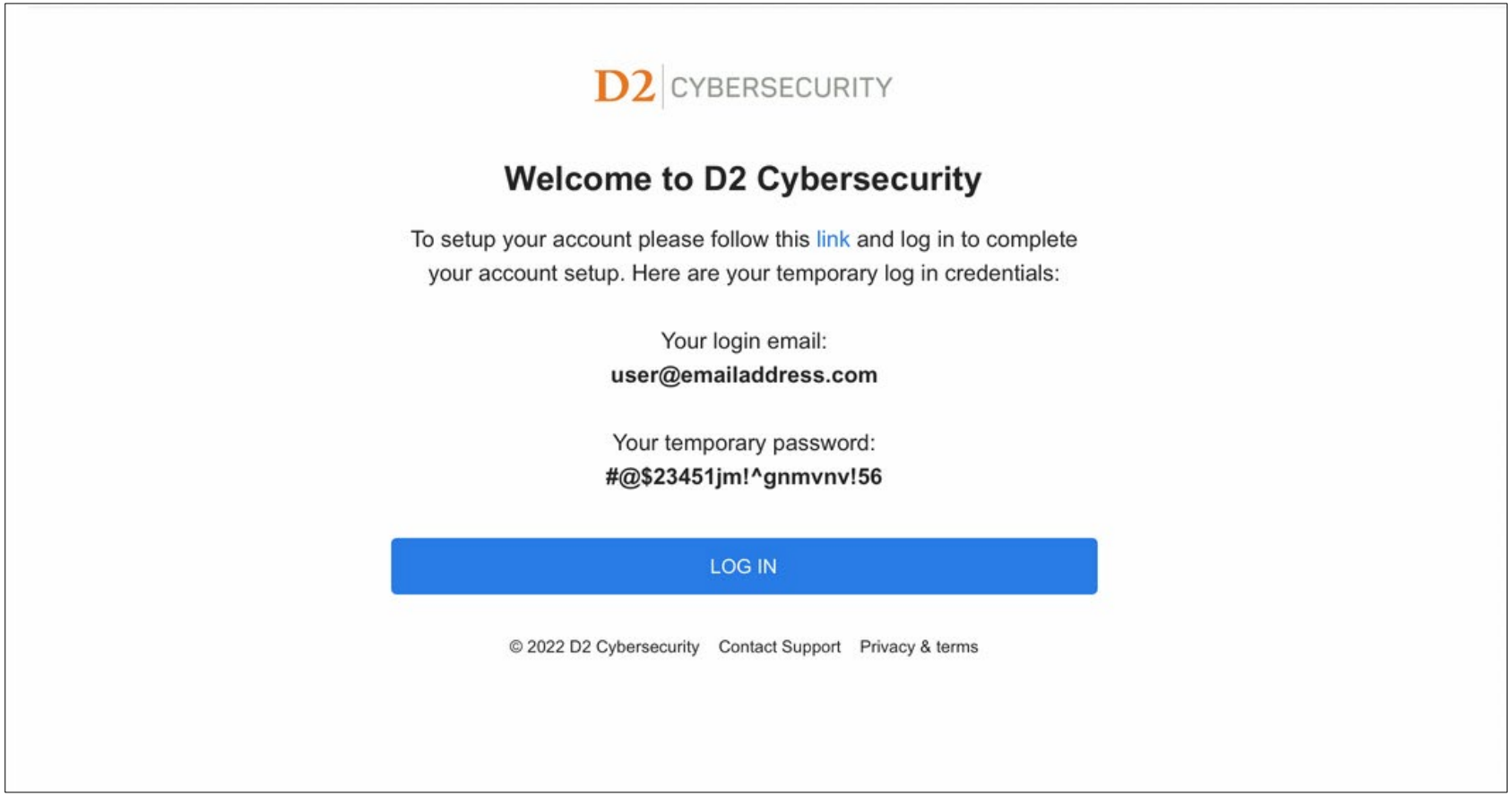
Vulnerability Mapping and Penetration
Vendor will look for vulnerabilities in enumerated computers and devices and attempt to exploit them. We will use a combination of manual techniques and enterprise-grade software to analyze all discoverable network resources and enumerate security issues. We will review all aspects of the in-scope network, and where successfully penetrated, we will attempt to move laterally and escalate privileges in order to determine the full extent of any issues, including the points at which sensitive data can be accessed. This stage includes looking for:

- Vulnerabilities
- Missing security patches
- Malware
- Backdoors
- Rogue network traffic, such as hosts communicating with botnet-infected systems
- Known/unknown processes
- Web services linking to malicious content
- Rogue or forgotten devices
- Potentially unwanted or unmanaged software
- Misconfigured devices

DISTRIBUTABLE COPY

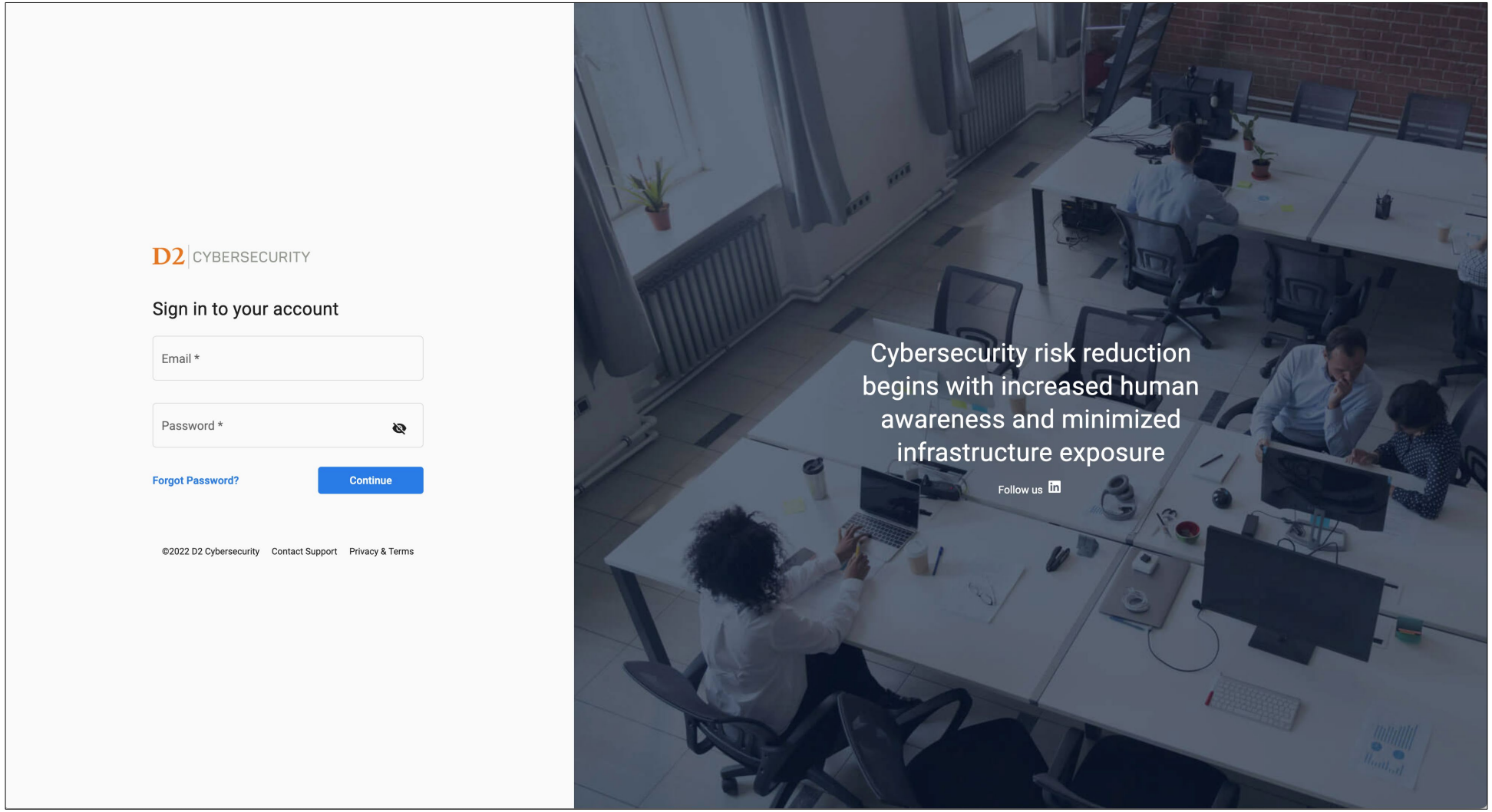
Welcome Email

D2 CYBERSECURITY



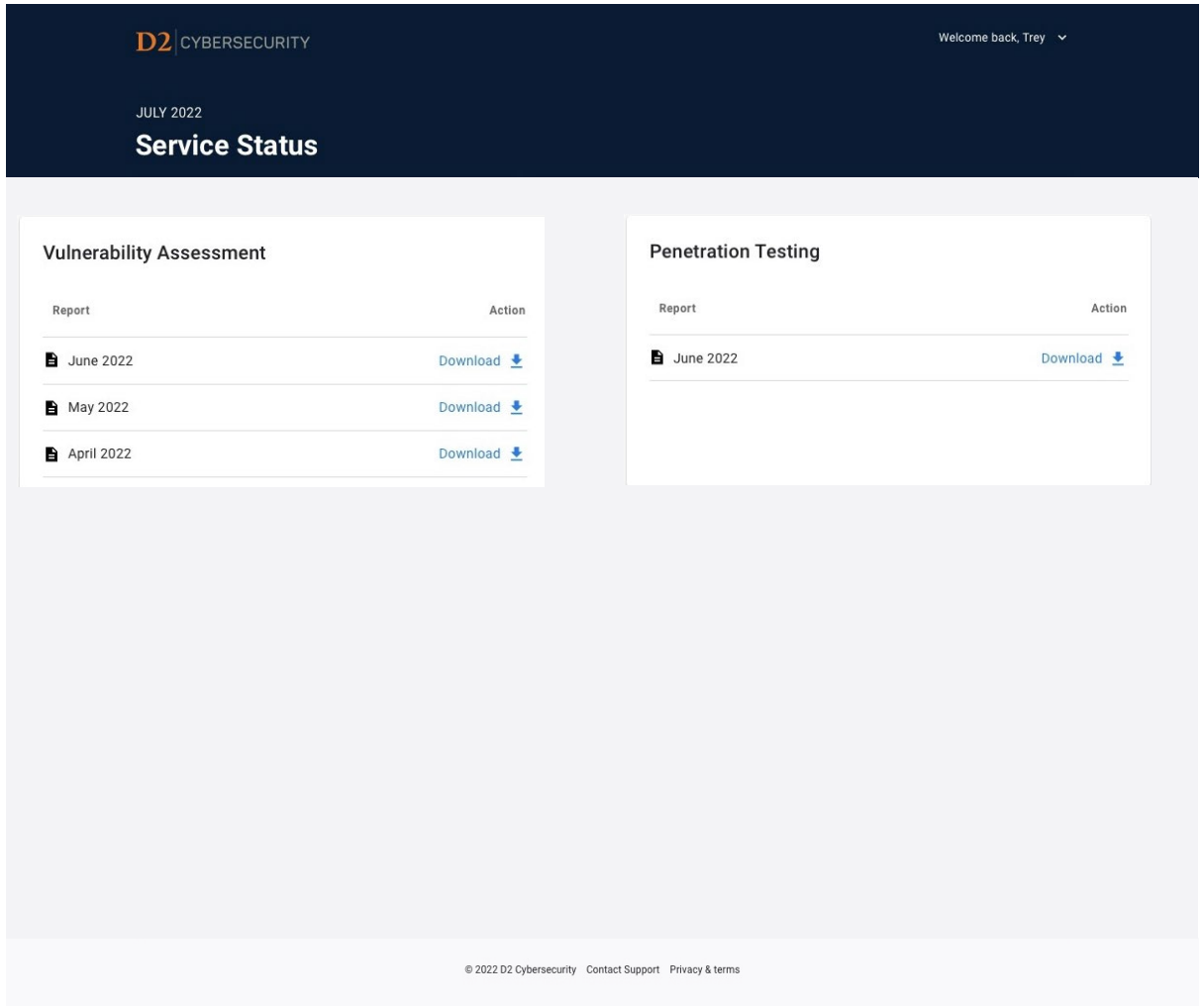
Insight Portal Login

D2 CYBERSECURITY



Insight Dashboard

D2 CYBERSECURITY



DISTRIBUTABLE COPY

Some Lessons Learnt

D2 | CYBERSECURITY

- Our Pen testers detected a critical vulnerability and immediately notified the municipality. The municipality emailed us back shortly thereafter saying that they had restarted a mail server that had been decommissioned in 2021 to migrate a mailbox for a user. They overlooked shutting down the mail server, leaving an exposed vulnerability which was immediately remediated upon discovery.

- We found a critical vulnerability in a network that was related to a device with security feature enabled that had been deprecated back in 2011. The Tech POC didn't think anyone ever used it anymore. Basically, it was a forgotten device that left a hole in their perimeter. The Tech POC immediately locked down the port and took the device offline to close the hole and in the process fixed a couple of lower level vulns we had detected as well.

- A medium level vulnerability was recently uncovered with a module for an application on an internet connected device that was the web portal for the security camera system. The cameras covered public parks, municipal buildings, and the PD. Once the municipality realized what the issue was and tried to patch the system, they realized that the company that produced the cameras and monitoring software was a Chinese company that was owned by the Chinese govt and as of Oct 2021 was banned from sales in the US due to the *Secure Equipment Act of 2021*.

Lessons Learnt – contd.

D2 | CYBERSECURITY

- Our vulnerability scans have detected several outdated OS & critical SSL vulnerabilities across many municipalities.
  - Microsoft Windows Server 2008 R2 and Ubuntu 14.04 pop up a lot.
  - SSL v2 and v3 are the common culprit.

- We have situations where third party vendors that are unwilling to update their systems. VOIP system operator that has critical vulns could expose members to attacks.

- A word of caution to all municipalities to revisit their system passwords. We have been frequently noticing passwords like: *<townname><year>* in several systems. Also, if you're using new IP connected devices like printer, fax, camera, etc. please change the default factory password before connecting it to your network.

Uncovered SSL vulnerabilities

D2 | CYBERSECURITY

Our monthly Vulnerability scans have detected critical SSL vulnerability (CVE-2022-0778) across many Municipalities.

What is it?

- Generally speaking, secure communications using SSL should be part of the solution set, not part of the problem. In March 2022 it was revealed that a maliciously crafted SSL certificate could lead to Denial of Service (DoS) attacks on both client machines and web servers.

Why do you need to fix it?

- This vulnerability can lead to malfunction of:
  - Municipal Websites
  - Financial Processing system
  - Firewall, Switches, and Internet facing devices
  - ISP/VoIP services
  - Web Applications
  - Etc.

How do you fix it?

- https://thesecmaster.com/how-to-fix-cve-2022-0778-a-denial-of-service-vulnerability-in-openssl/

Blocking Pings

D2 | CYBERSECURITY

Our Monthly Vulnerability scans have detected some municipalities blocking pings to their external IP from anywhere.

The Good

- It is definitely a good first step to eliminate broad exploratory sweep of IP's usually conducted by hackers at the outset. When an initial ping is blocked most hackers move on to easier targets.

The Bad

- With additional configuration changes one can bypass the block, as we had done.
- It also takes away your ability to ping your own server to determine whether it is responding.

The Proper

- Instead of blocking pings from all IPs, create a whitelist of IP that would be allowed to ping (internal IPs, our service IP, etc.)

Summary

D2 | CYBERSECURITY

- Our overnight vulnerability scanning has identified a number of critical vulnerabilities so far with various municipalities who were notified within 24-hours.

- Some municipalities begin remediation procedures immediately, however, our pen testers shortly thereafter were able to breach few of the municipality network by exploiting detected vulnerabilities from the scan.

- From our experience so far, not only are we finding critical weaknesses in some municipality network perimeter, but if they are not fixed in a timely fashion they can be breached!

- Our Perimeter security services will remove the guesswork in your risk reduction effort.

Questions