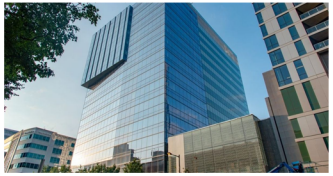
CCI Penetration Test

Daniel Cayelli, Ben Coleman, Daniel Grant, Jake Naccarella, Irfanullah Khan

Drexel University College of Computing & Informatics

Drexel's College of Computing & Informatics



CCI Building, 3675 Market Street Philadelphia PA 19104

Why assess CCI's security?

- Regularly handles sensitive student info and research data
- Ethical and legal responsibilities to comply with data protection
- Breaches could impact school's credibility/reputation
- Need to protect sensitive research projects or information

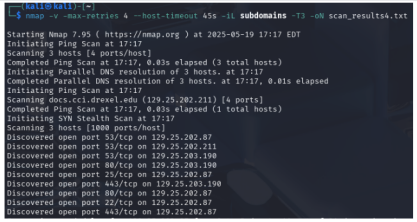
Problem Statement

The goal of our tests are to:

- Ensure the cybersecurity stature of CCI and its environments
- Protect any exposed student, faculty, or research information
- Protect testing environments and virtual resources
- Identify potential vulnerabilitites within CCI infrastructure
- Identify weaknesses in physical access within CCI building
- Report on recommendations to mitigate any deteceted vulnerabilities

10th Floor Lobby, CCI Building

Gallery



Nmap Scan Discovering Open Ports

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	1 (3.4%)	0 (0.0%)	1 (3.4%)
	Medium	0 (0.0%)	5 (17.2%)	4 (13.8%)	1 (3.4%)	10 (34.5%)
	Low	0 (0.0%)	2 (6.9%)	9 (31.0%)	1 (3.4%)	12 (41.4%)
	Informational	0 (0.0%)	0 (0.0%)	3 (10.3%)	3 (10.3%)	6 (20.7%)
	Total	0 (0.0%)	7 (24.1%)	17 (58.6%)	5 (17.2%)	29 (100%)

ZAP Scan Risk Matrix

Methods and Tools

1. **Pre-Engagement:** Gaining approval to test CCI's security
2. **Reconnaissance:** Collect information on hosts, systems, infrastructure or any other potentially vulnerable areas.
3. **Scanning/Enumeration:** Internal scans and testing of CCI's vCenter environments and configuration
4. **Testing:** Testing/Exploitation of any detected vulnerabilities
5. **Reporting:** Submitted report of findings to CCI, Drexel IT, Drexel Security

Tools and References Used:

•Kali Linux	•Nikto	•Searchsploit
•Shodan.io	•Zed Attack Proxy (ZAP)	•CVE Database
•Nmap	•Metasploit	•NIST Cybersecurity Framework

Findings

From our tests we found several small-medium sized risks that could impact CCI operations or the confidentiality of any information they store, as well as vulnerabilities in physical access that may require further investigation.

Per out agreement with CCI our specific findings are confidential, but they generally involve:

- Physical security vulnerabilities leading to unauthorized access to some areas of the CCI building
- Missing security headers on the CCI domain
- Headers on the CCI domain that could leak software names and version numbers
- Outdated software or servers within CCI domain

Remediation

- Reporting any physical or virtual vulnerabilities detected to John McNamara, CCI's Executive Director of Technology Platforms and Services
- Prepared and provided a detailed vulnerability report with remediation recommendations based on risk level
- Advocate for routine vulnerability scans or automated monitoring on our findings

Acknowledgements

Our team would like to thank Dr. Peiper for his ongoing support and guidance throughout the course of our project. We'd also like to thank CCI's administration and Drexel IT, especially Director McNamara and Brian Bijeau, for their support and allowing us to conduct these tests on CCI and its systems, giving us valuable experience applying these tools..