BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Building PEN Testing Capability within your Security Department

bio. John Cuzzola

MSc. Info. Systems, BSc. Math, CEH/CEPT

Information Security Director (2021 - current)

Network Manager (2001 – 2008)
Director of Information Technology (2008 – 2021)

Research Associate @ Ryerson University
(2012 – current)

Laboratory for Systems, Software and Semantics

Sessional Faculty (2017 - 2021)
Java, Ethical Hacking, Biometric Authentication

Why?

SHOW

not

TELL

The Management

CVE has just issued critical advisory CVE-2022-0666 with a severity score of 9.8. Details are embargoed but vendors are urging to apply the latest patches.

Our servers appear they might be vulnerable to CVE-2022-0666 leading to remote code execution.

No proof-of-concept code yet.

There’s an exploit in the wild

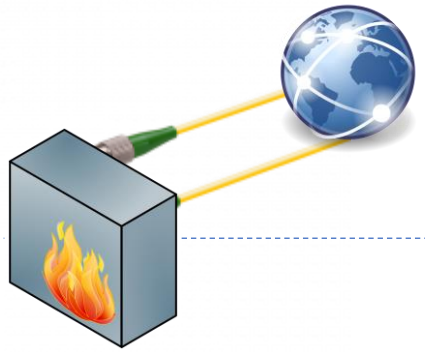
for CVE-2022-0666 and I ran it…

… here’s all our employees’

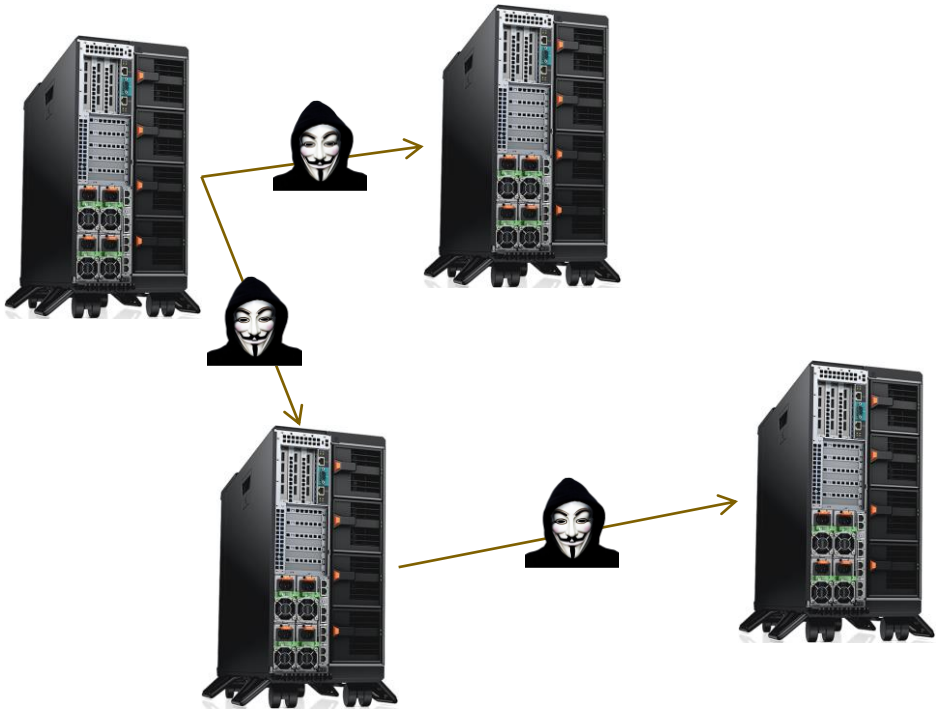
permanent records…

The Management

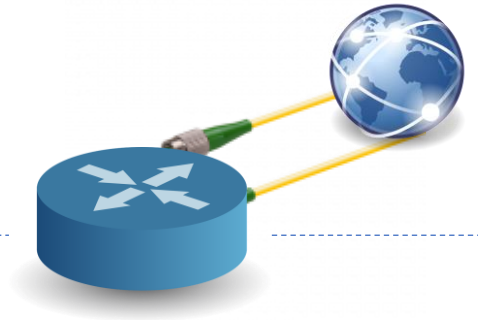
PERIMETER



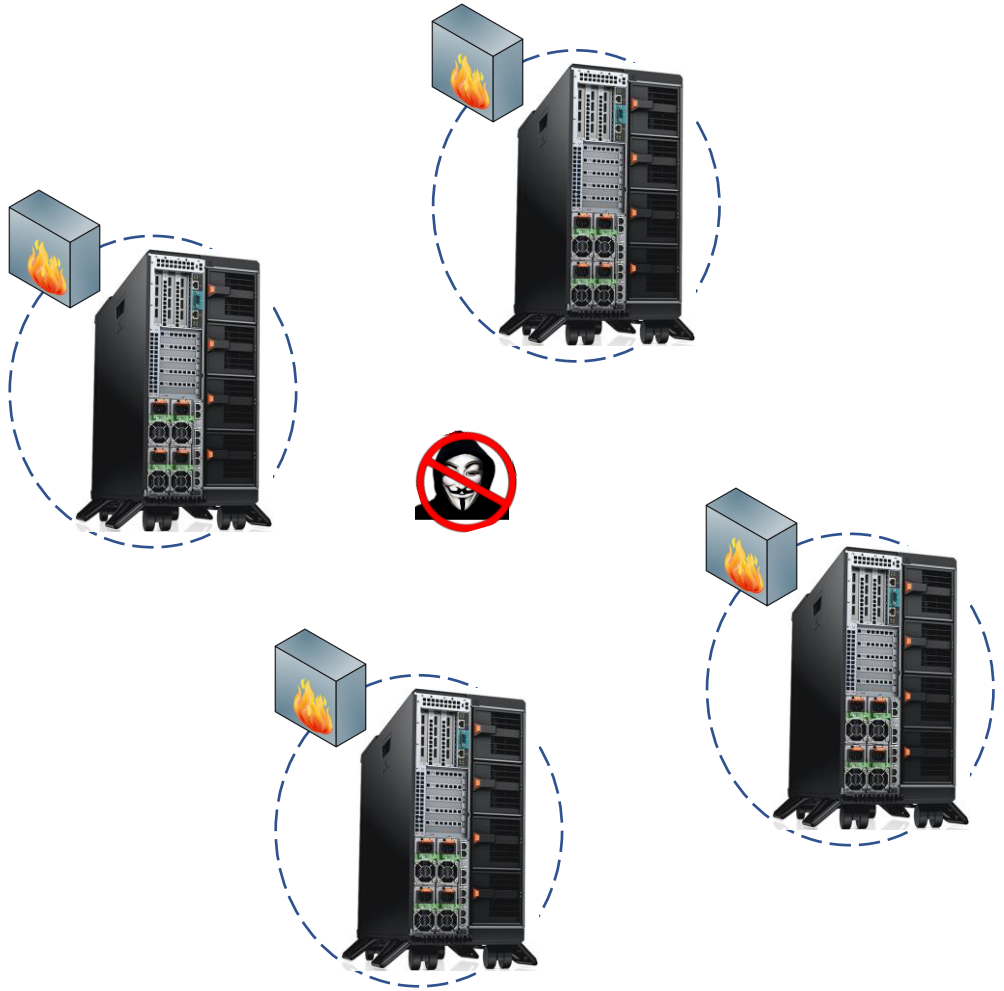
(external PEN test)



ZERO TRUST



(internal PEN test)

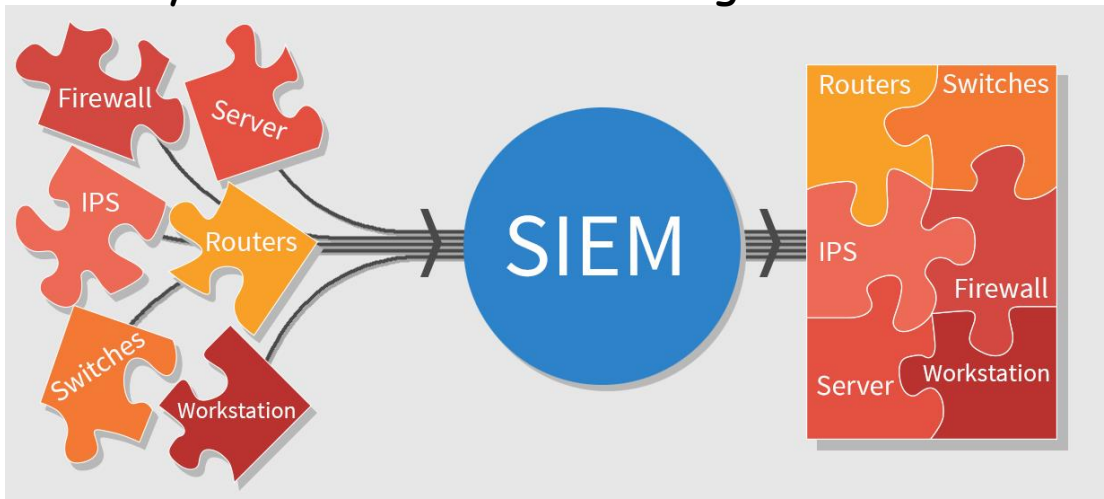


IDS/IDP, EDR/XDR TESTING

Did the IDS/IDP, EDR/XDR detect/stop the PEN test?

Did the SIEM record the PEN test?
(post-mortem forensics)

Security Incident & Event Management



CYBER

Please tick all the boxes below that relate to controls that you currently have implemented within your IT infrastructure (including where provided by a third party). If you're unsure of what any of these tools are, please refer to the explanations on the final page of this document.

☑ Application Whitelisting	☑ Asset Inventory	☑ Custom Threat Itelligence	☑ Database Encryption
☑ Data Loss Prevention	☑ DDoS Mitigation	☑ DMARC	☑ DNS Filtering
☑ Email Filtering	☑ Employee Awareness Training	☑ Endpoint Protection	☑ Incident Response Plan
☑ Intrusion Detection System	☑ Mobile Device Encryption	☑ Network Monitoring	☑ Penetration Tests
☑ Perimeter Firewalls	☑ Security Info & Event Management	☑ Vulnerability Scans	☑ Web Application Firewall
☑ Web Content Filtering			

Recruitment

Remote learning made universities more vulnerable to cyberattacks

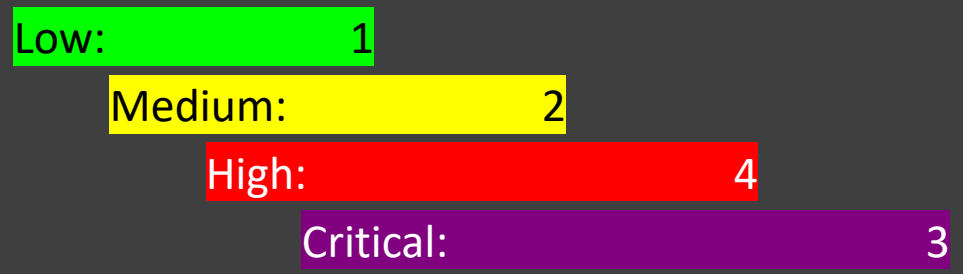
Ransomware and data breaches lead cyberthreats at colleges

Ransomware Attacks Double Against Global Universities

THOMPSON RIVERS UNIVERSITY

WHAT WE DID @

- ✓ Introduced (internal) PEN Testing
- ✓ Created a standard Reporting Template



Where to start?

academy binsec

Secure Coding Training
OWASP Top 10 + PCC-DSS

Try Hack Me

PentesterLab

PortSwigger

HBH

Hellbound Hackers

HACKTHEBOX

TRAINING

Where to start?

PEN TESTING
IS
VERIFICATION

PCI-DSS:

11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.

BCNET CONNECT