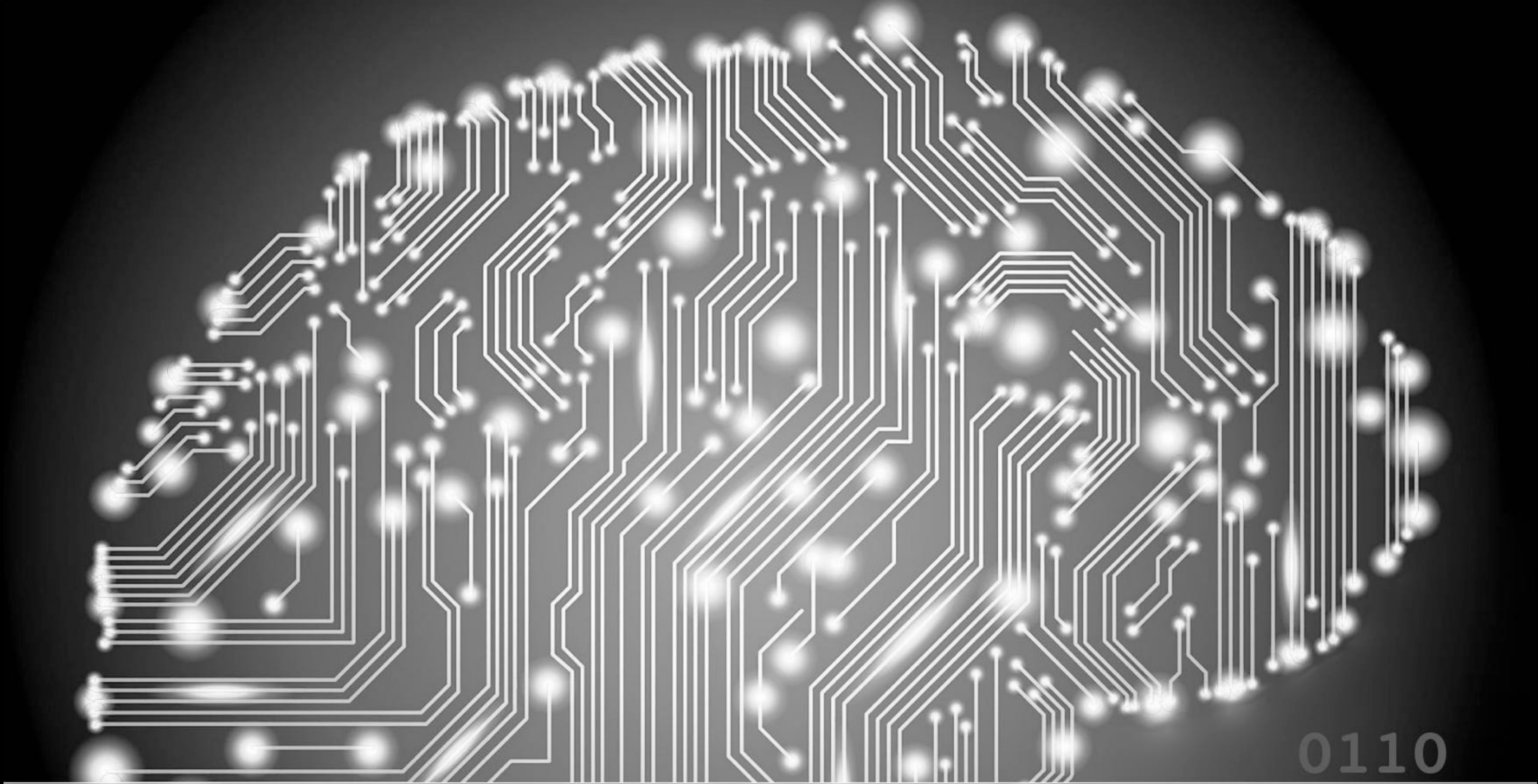
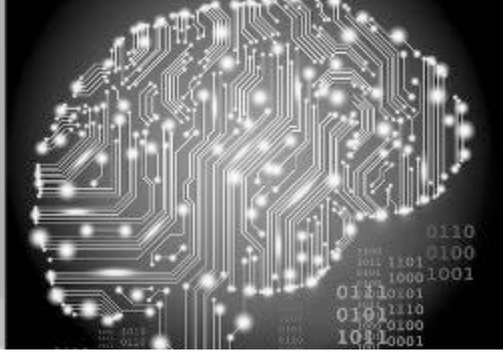


A Colloquy on Security Alchemy

Mike Pullen – Baraboo   Jim Blodgett – Middleton

Pat Zielke – Viroqua   Kevin Capwell – META



Middleton-Cross Plains School District

Duluth
eapolis
WISCONSIN
Green Bay
Rochester
Oshkosh
Lake Michigan
Madison
Milwaukee

Map Data: 2020 Google

- Jim Blodgett
  Director of Technology – 8 years
- Enrollment: 7,450
- Total Staff: 1,098
- Buildings: two High Schools, two Middle Schools, seven Elementary Schools, District Office.
- Desktops 2000, Laptops 1000, Chromebooks 6500, iPads 1200.

Baraboo School District

Duluth
eapolis
WISCONSIN
Green Bay
Rochester
Oshkosh
Lake Michiga
Madison
Milwaukee

Map Data: 2020 Google

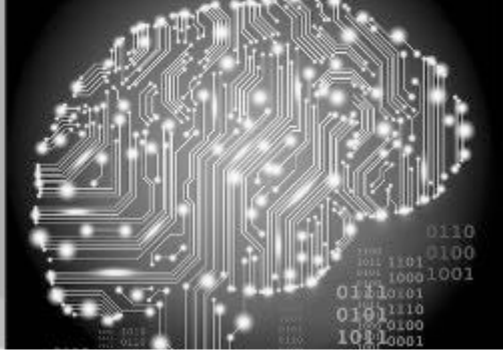
- Mike Pullen
  Computer Technician – 12 years
- Enrollment: 2,972
- Total Staff: 466
- Buildings: High School, Middle School, five Elementary Schools, multiple 4K sites, District Office.
- Computers: ~350 iMacs and Macbooks, ~250 Windows desktops and notebooks, ~2500 Chromebooks, ~700 iPads.

Viroqua Area Schools

Duluth
eapolis
WISCONSIN
Green Bay
Rochester
Oshkosh
Lake Michigan
Madison
Milwaukee
Map Data: 2020 Google

- Pat Zielke
  Technology Coordinator – 20 years
- Enrollment: 1,191
- Total Staff: 184
- Buildings: Shared High School/Middle School a separate Elementary all on the same campus.
- Computers: Desktop 400, Chrome books 800, Other mobile 90.

Security Alchemy

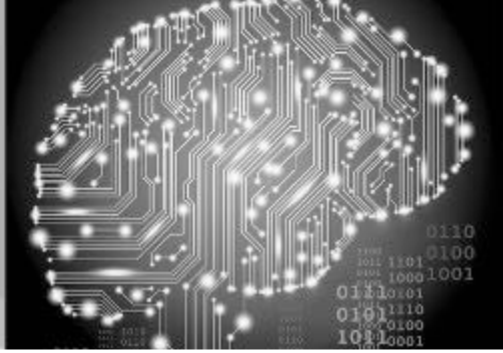


School District of Onalaska

Duluth
eapolis
WISCONSIN
Green Bay
Rochester
Oshkosh
Lake Michigan
Madison
Milwaukee
Map Data: 2020 Google

- Kevin Capwell
  fmr → Data Systems Director – 24 years
- Enrollment: 3,166
- Total Staff: 425
- Buildings: High School, Middle School, three Elementary Schools, District Office, and School Nutrition.
- Computers: Desktops 1400, Chrome books 1400, Other mobile ~200.

Security Alchemy



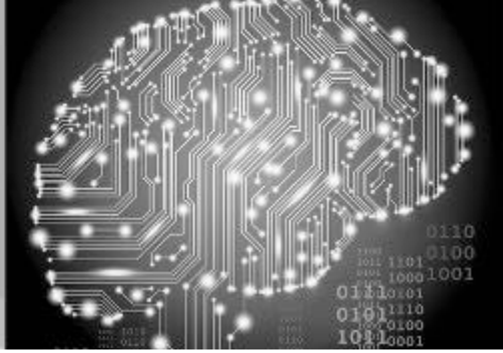
Cybersecurity

is the ***art*** of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

--Department of Homeland Security

Common Cybersecurity Excuses

- we have nothing that hackers want
- too small of a company to be a target
- we don’t have the time to fix them
- upgrading will cost us too much
- cybersecurity is not in the budget
- it might break the system
- compliance is enough
- we have a firewall to protect us
- we have cybersecurity insurance
- we are unhackable
- Don’t be like "Bob"!



Enterprise Cyberattacks are on the Rise

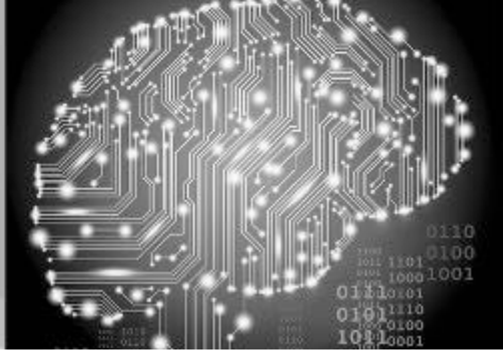
- Cybercriminals stole headlines with attacks against some of the country's most important sectors.
- Hackers targeted schools to steal and then sell staff and student data while grinding instructional hours to a halt.
- The use of ransomware, trojans and malware helped stop key services and vital infrastructure.

--Malwarebytes Labs Nov: 2019

Educational Institutions are a Target

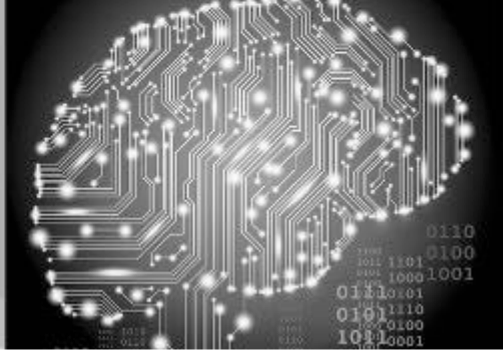
- Most vulnerable industry: education!
- Education is a priority target due to the large number of endpoints that are accessed by students, staff, and others. Combined with outdated security infrastructure, limited budgets and staffing, the result is a nightmare scenario for network security.
- Identity theft involving a student may not be caught for years!

--Malwarebytes Labs Nov: 2019



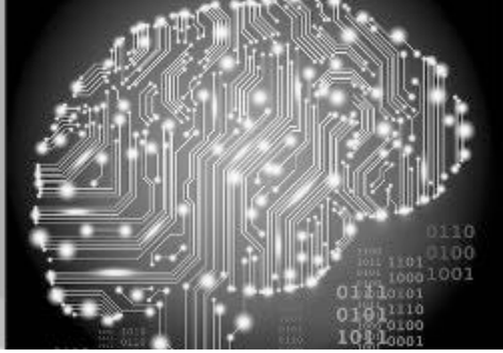
Why Hackers are Targeting Schools

- Schools have important data: including staff and student names, Social Security numbers, email addresses, academic / health / financial records.
- Professional development is often focused on curriculum, or institution.
- Students can be more tech-savvy than staff, but security is **<u>not</u>** paramount.
- Headaches: 1:1, BYOD, VoIP, cameras, PA/bell, HVAC, IoT, & rogue devices.



Common Attack Vectors

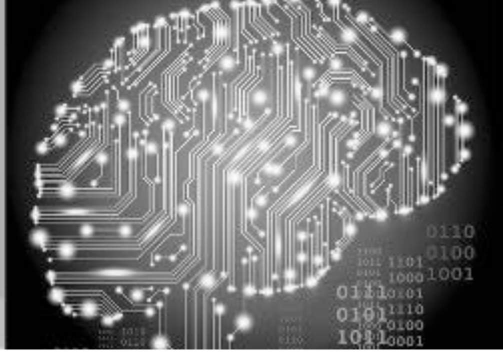
- **Malware** includes spyware, ransomware & viruses → data breaches & identity theft.
- **Phishing** is sending fraudulent communication *(email)* that appears to be legitimate.
- **Man-in-the-middle** occurs when attackers spoof your Wi-Fi network to capture data.
- **A denial-of-service** attack floods servers or networks with traffic to exhaust bandwidth.
- **A SQL injection** attack forces a db server to reveal information it normally would not.
- **A zero-day exploit** hits after a vulnerability is announced, but before a patch is released.
- **Social engineering** tempts staff and students into ignoring cybersecurity "best practices".



Know Your Foe (…and Yourself)

- **Cyber mercenaries -** serving as a third-party aide to other attackers.
- **Nationalist hackers -** State sanctioned users / military / intelligence with advanced tools.
- **Hacktivists** – use DDoS or web defacements.
- **Organized criminals -** these are groups that are very efficient with turning a profit.
- **Disorganized criminals** – possess skills, are loosely organized, & can monetize an attack.
- **The insider threat -** never underestimate the power of a disgruntled employee or volunteer.
- **Script kiddies -** attention-seeking, rebellious hackers with very little skill, but still a threat.

Example 1: 2018 Atlanta/SamSam



City of Atlanta - Hack Analysis

- Attack recognition: March 22, 2018
- Almost every department was infected
- Ransom: about $51,000
- First reboot: March 27, 2018
- January 2018 audit found 1,500 to 2,000 critical vulnerabilities remaining from last year
- SamSam does not rely on phishing, it utilizes a brute-force attack to guess weak passwords
- Agencies involved: FBI, Department of Homeland Security, and Secret Service
- Third Party firms: included SecureWorks
- Cost: $17 million

Example 2: 2019 Baltimore/RobinHood

Baltimore - Hack Analysis

- Attack recognition: May 7, 2019
- PC and server issues: 10,000 city government computers are frozen
- Ransom: about $76,280
- First reboot: May 20, 2019
- Baltimore was susceptible to such an attack due to its IT practices
- Agencies involved: FBI, Department of Homeland Security, and Secret Service
- Hacked twice in two years
- Unlike Baltimore, Atlanta had cyberinsurance
- Cost: $18 million including remediation, new hardware, and lost or deferred revenue

Example 3: 2019 Texas/REvil

Texas Coordinated - Hack Analysis

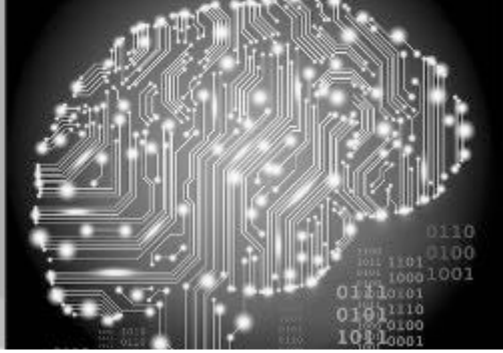
- Attack recognition: August 16, 2019
- Mass ransomware attack that simultaneously hit 22 different locations simultaneously
- Ransom: $2.5 million
- First reboot: August 20, 2019
- REvil is Ransomware-as-a-Service where one group maintains the code and another group spreads the ransomware
- Agencies involved: FBI, Department of Homeland Security, and Texas DIR
- Targeted at mainly small, local governments
- Cost: $12 million+ including remediation

Example 4: 2019 Lake City/Ryuk

Lake City Florida - Hack Analysis

- Attack recognition: June 10, 2019
- "Triple Threat" ransomware attack: Emotet trojan installs the TrickBot trojan to deliver the Ryuk ransomware!
- Ransom: $460,000
- Cyberinsurance covered Lake City’s incident
- Lake City is a 12,000-person municipality
- Lake City IT director fired June 27th
- Cost: $10,000 to decrypt.
- New backup storage, hardware and multi-factor authentication, have cost the municipality about $330,000 – so far

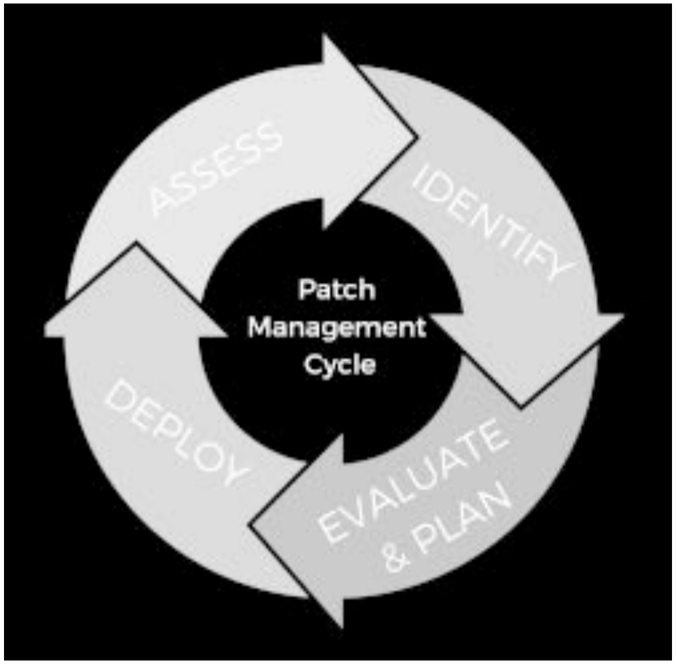
Example 5: 2019 Louisiana/Ryuk



Louisiana Schools - Hack Analysis

- Attack recognition: July 8-21, 2019
- Impacted school systems in Sabine, Morehouse, Monroe City and Ouachita parishes
- Ransom: typically range $300,000 to $1 million
- Ryuk is often dropped on a system by other malware, most notably TrickBot
- TrickBot is a trojan. It comes disguised as something harmless, via an attachment
- Statewide Emergency Declaration allows cybersecurity experts from state agencies such as the Louisiana National Guard, Louisiana State Police, and the the Office of Technology Services to assist local governments

How do we Protect Ourselves?

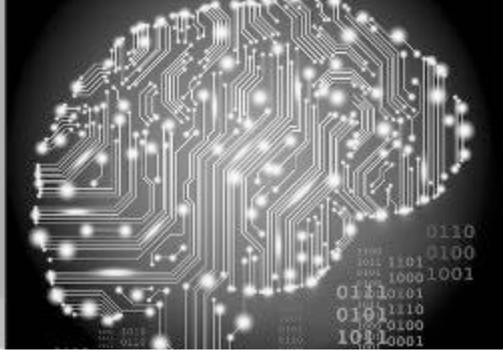


- The goal isn’t to eliminate risk. The goal is to manage risk.
- The "Patch Management Cycle" balances the risk of disrupting internal workflows with the risk of not updating these systems. Reasonable patch management processes will test updates, correct any errors, and keep unnecessary downtime at bay from critical apps and services.
- The "Patch Management Cycle" never ends
- Having a test environment is crucial for testing updates before you deploy them in your production environment.

How do we Protect Ourselves?

- Cybersecurity Best Practices

- It is everyone’s responsibility to remain cyber aware and practice information safety.
- Do not open suspicious or unexpected links or attachments in emails.
- Hover over hyperlinks in emails to verify they are going to the anticipated site.
- Be aware of malicious actors attempting to impersonate legitimate staff, and check the email sender name against the sender’s email address.



How do we Protect Ourselves?

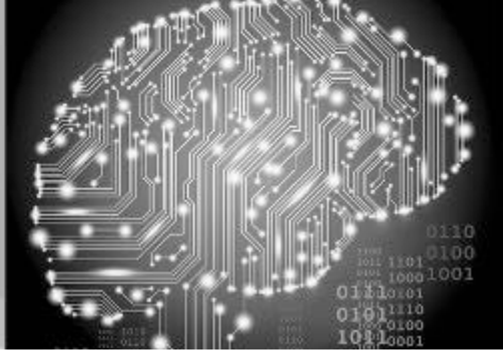
DIR
Texas Department of Information Resources

- Cybersecurity Best Practices (part 2)

- Use unique strong passwords or pass-phrases for all accounts [multi-factor authentication].
- Do not provide personal or organizational information unless you are certain of the requestor’s authority, identity, and legitimacy.
- Alert your IT staff or supervisor if you have any concerns about the legitimacy of any email, attachment, or link.
- Take advantage of available cybersecurity awareness training.

Know the Why

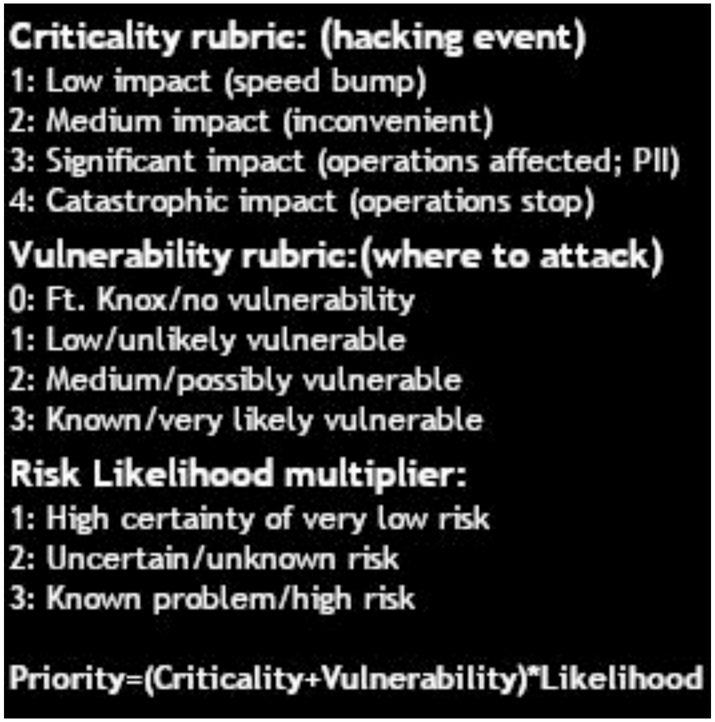
- Mission, vision, and goals of the district and the tech department's role
- Tech Department is a partner for staff and students, not a black box to "just make it work"



Protect the Golden Eggs

- Two people (at least) have to agree on cutting checks or money transfers
- ACH Changes made in person
- All ACH transactions are done from a single, hardened device with only essential Internet connectivity
- DLP filters on emails and storage
- Defined Procedures and policies
- Internal auditing
- Single Vendor Credit cards
- Audit high-level access accounts

Data Systems Catalog / Risk Inventory



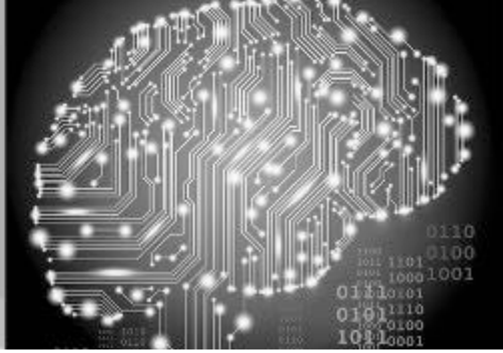
Criticality rubric: (hacking event)
1: Low impact (speed bump)
2: Medium impact (inconvenient)
3: Significant impact (operations affected; PII)
4: Catastrophic impact (operations stop)

Vulnerability rubric:(where to attack)
0: Ft. Knox/no vulnerability
1: Low/unlikely vulnerable
2: Medium/possibly vulnerable
3: Known/very likely vulnerable

Risk Likelihood multiplier:
1: High certainty of very low risk
2: Uncertain/unknown risk
3: Known problem/high risk

Priority=(Criticality+Vulnerability)*Likelihood

- Limited resources: Risk vs Cost analysis
- List all data processing and storage systems
- For each system, rate Criticality, Vulnerability and Likelihood
- Calculate Priority score
- Allocate limited resources (time, money, etc) to highest priorities first, lower priorities as possible



Segmentation

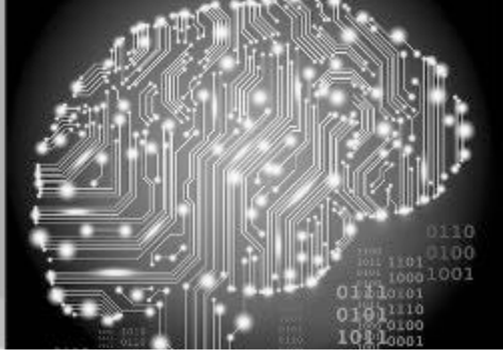
- Use firewalls and ACLs to group users
- Access is given as needed
  - We know who needs access to our systems
  - We know where our users are coming from
- No Internet access with elevated privileges
- Vulnerable Systems (HVAC, Cameras, IoT) isolated with limited access through hardened interfaces
- Protect DNS and Email
- Role-based security for all systems

Security Alchemy

Monitor

- Capture keystrokes, mouse clicks, web traffic, unexpected events
- Correlate event data across systems
- Listen to staff and student and reward paranoia (no shaming)
- Check and export key logs
- Consider centralized log management
- Listen to NIST, NSA, DHS, US-Cert and act on the advice

Security Alchemy



Educate

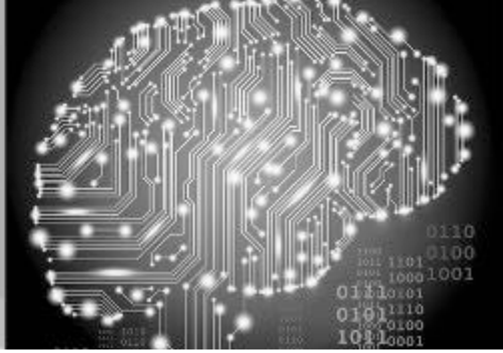
- Social engineering awareness
- Cybersecurity and digital citizenship education for all staff and students
- Targeted education for HR, Finance, Benefits, Payroll, and Facilities staff
- Targeted education for tech staff

- Training and Certification- importance?

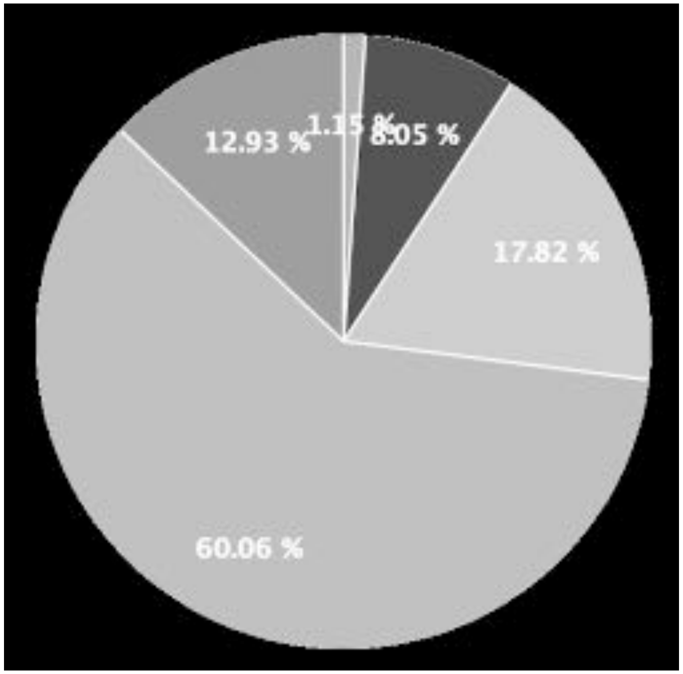
Security Alchemy

Make Time to be Proactive & Strategic

- Good security comes in layers
- Patch process
- Snapshot/backup and verify
- Ready to go spares
- Identify vulnerabilities and mitigate
- Consider geolocation blocking
- Create a disaster recovery plan
- Out of band knowledge repository



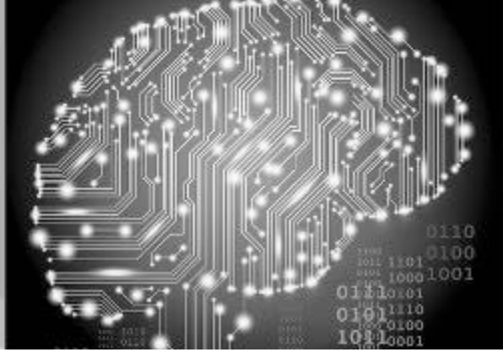
K-12 Cyber Incidents: 2019



- ■ 1.15% Denial of Service
- ■ 8.05% Phishing
- ■ 17.82% Ransomware
- ■ 60.06% Disclosure/Breach
- ■ 12.93% Other Incident

- **Note**: Publicly-disclosed incident reports represent a **small** percentage of actual incidents.

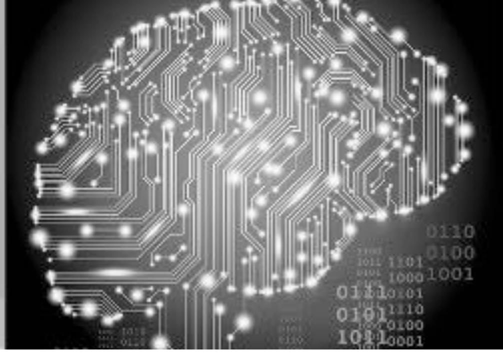
-- k12cybersecure.com



How do we Protect our Networks?

- Backups – All data / offline / tested
- Risk Analysis - of the full organization
- Staff Training - on cybersecurity best practices
- Vulnerability Patching – known system holes
- Application Whitelisting – only approved apps
- Incident Response – does a *tested* plan exist
- Business Continuity – sustain ops & how long
- Penetration Testing – hack your own systems

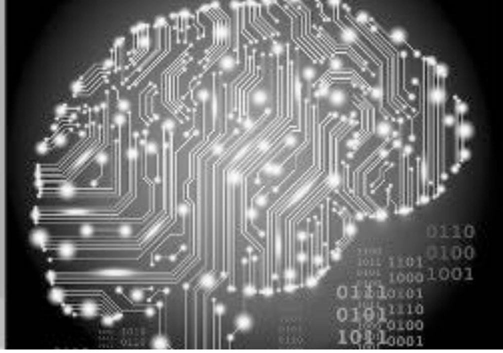
- If your network sustains a cyberattack:
- Contact law enforcement immediately. FBI, Department of Homeland Security or Secret Service.



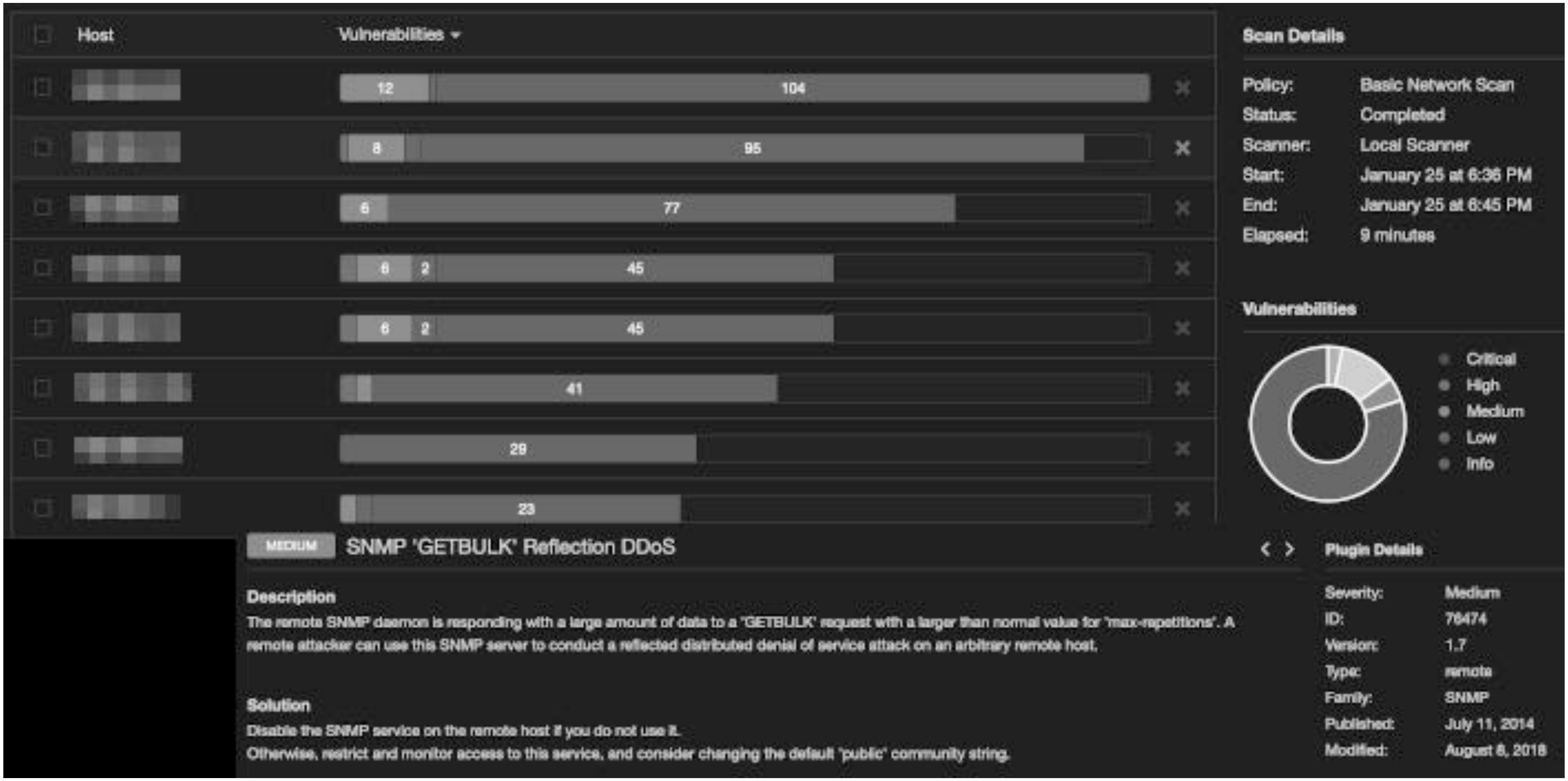
Preventative Measures can Help!

- Strong spam filters and authenticate inbound email using SPF, DMARK and DKIM
- Scan all incoming and outgoing emails and filter executable [or encrypted] files
- Configure firewalls to use geolocation restrictions and block known bad IP addresses
- Consider using a centralized patch management system [+ firmware updates]
- Set anti-virus and anti-malware to scan automatically (and frequently)
- Disable Remote Desktop (RDP) if it is unused
- Manage user accounts by least privilege

Security Alchemy



Nessus Vulnerability Patching / Testing



Host	Vulnerabilities
[redacted]	12 104
[redacted]	8 95
[redacted]	6 77
[redacted]	6 2 45
[redacted]	6 2 45
[redacted]	41
[redacted]	29
[redacted]	23

Scan Details

Policy: Basic Network Scan
Status: Completed
Scanner: Local Scanner
Start: January 25 at 6:36 PM
End: January 25 at 6:45 PM
Elapsed: 9 minutes

Vulnerabilities

MEDIUM SNMP 'GETBULK' Reflection DDoS

Description

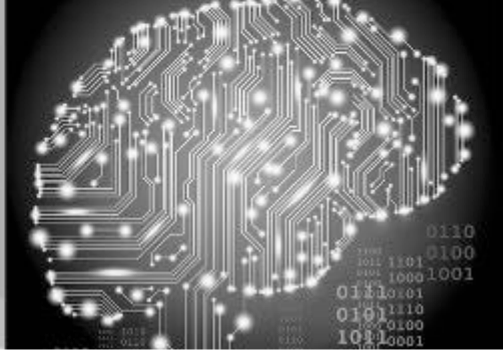
The remote SNMP daemon is responding with a large amount of data to a "GETBULK" request with a larger than normal value for "max-repetitions". A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.

Solution

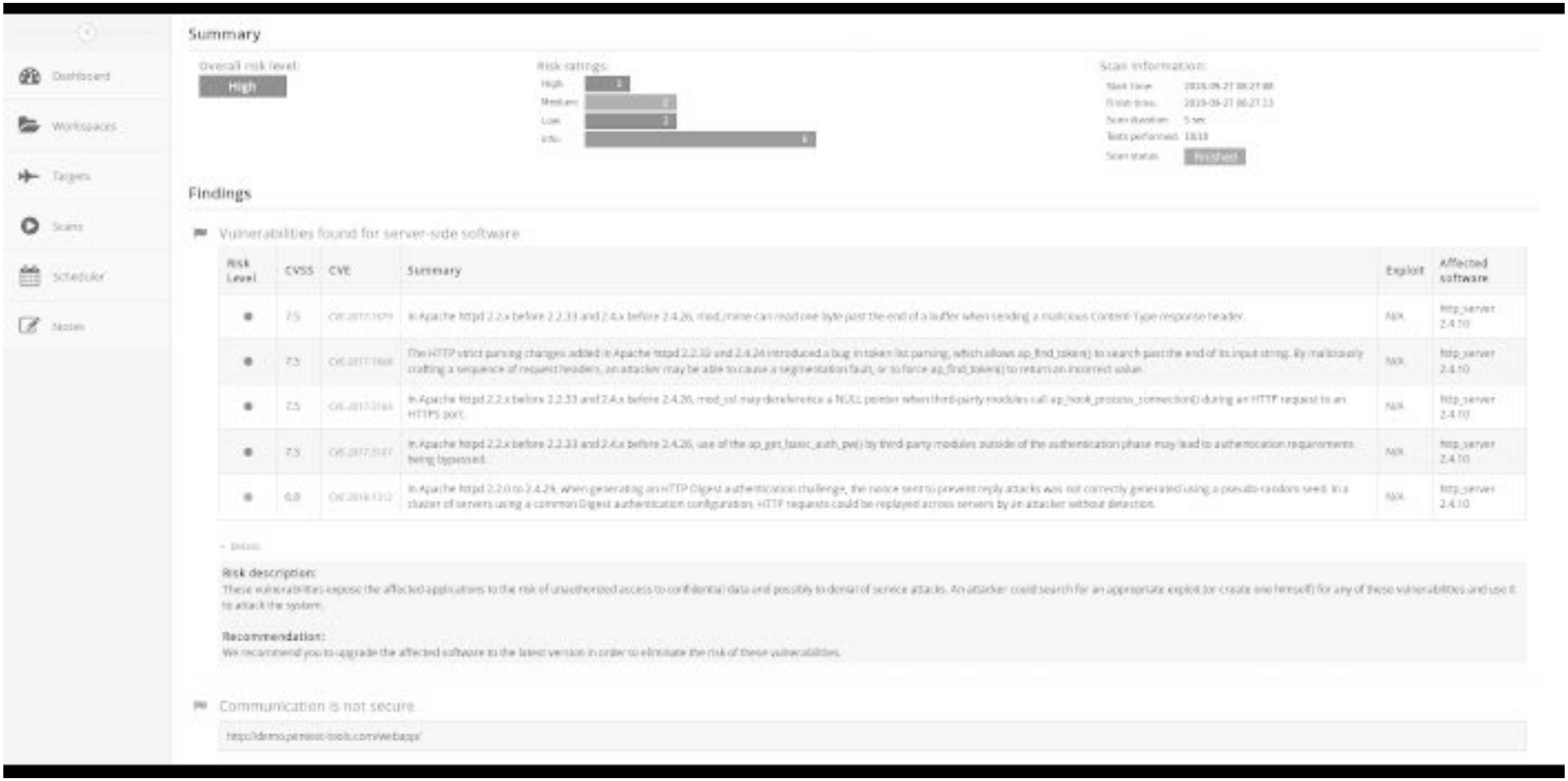
Disable the SNMP service on the remote host if you do not use it.
Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

Plugin Details

Severity: Medium
ID: 76474
Version: 1.7
Type: remote
Family: SNMP
Published: July 11, 2014
Modified: August 6, 2018



Pentest-tools.com Patching / Testing



Summary

Overall risk level:
High

Risk ratings:

High	1
Medium	2
Low	2
Info	6

Scan information:

Start time:	2019-09-27 08:27:08
Finish time:	2019-09-27 08:27:13
Scan duration:	5 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4.10
●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4.10
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4.10
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4.10
●	6.8	CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.	N/A	http_server 2.4.10

- Details

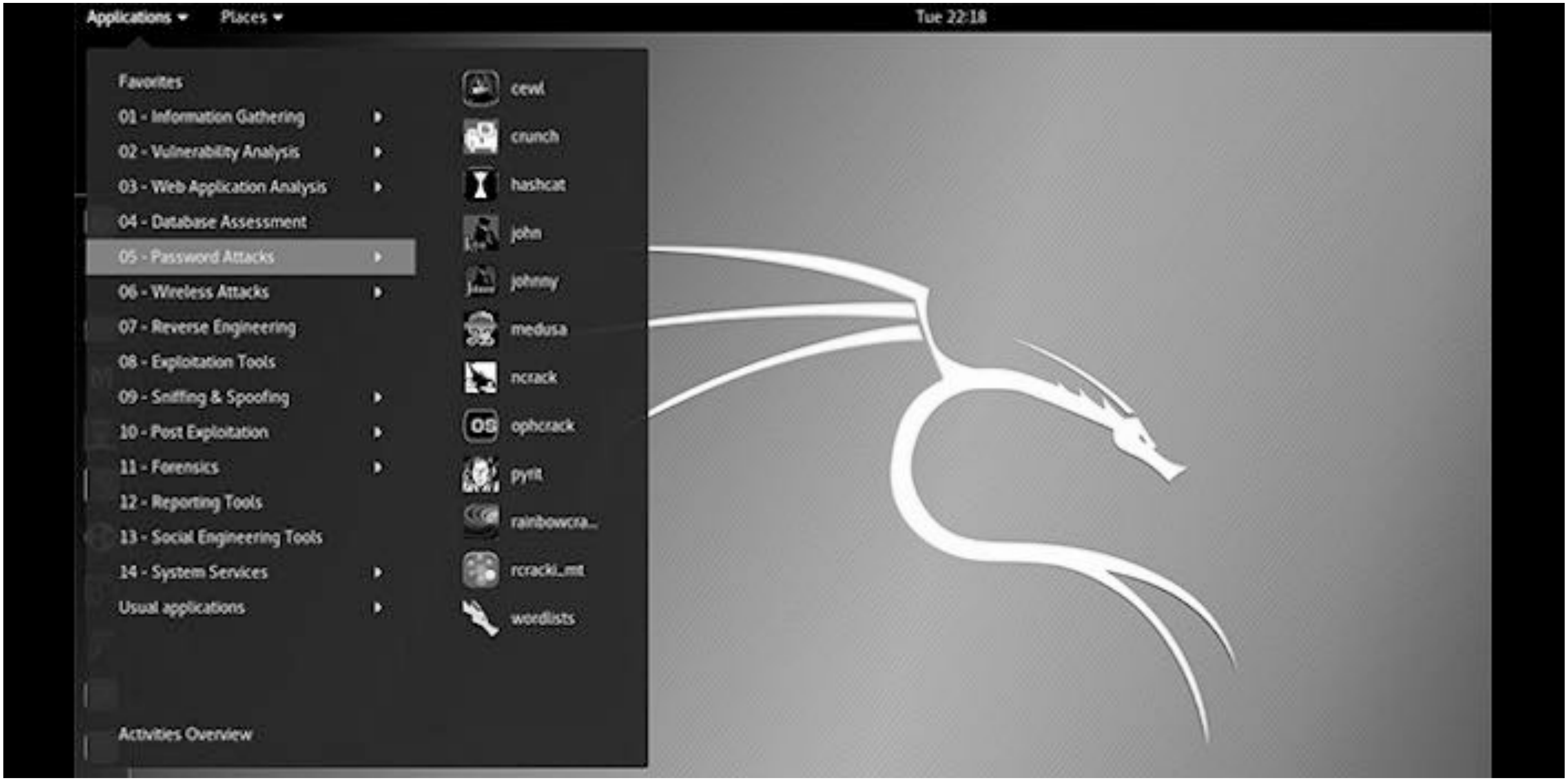
Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.

Communication is not secure

http://demo.pentest-tools.com/webapp/

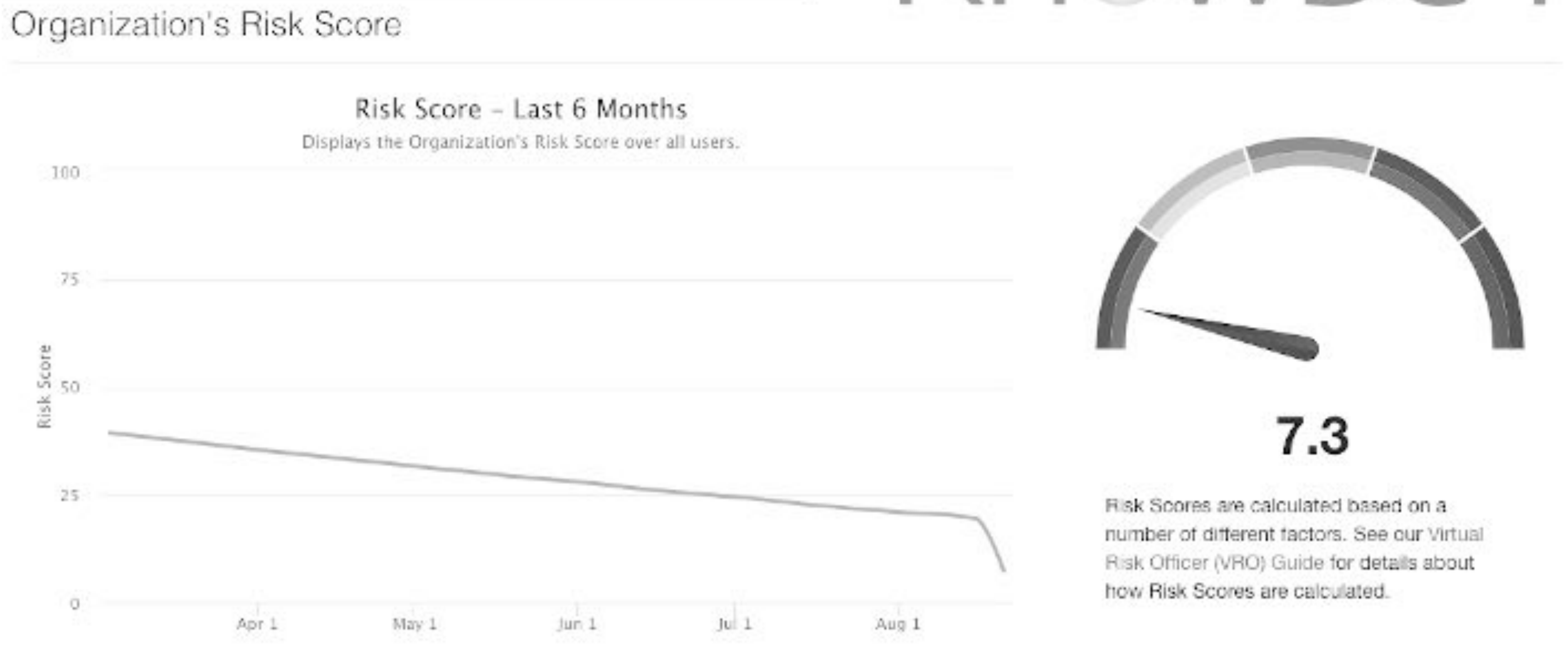
Kali Linux Patching / Testing



Knowbe4 - Phishing / Testing

[redacted]

KnowBe4



Organization's Risk Score

Risk Score – Last 6 Months

Displays the Organization's Risk Score over all users.

7.3

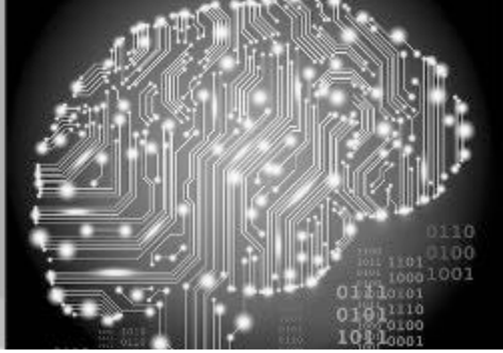
Risk Scores are calculated based on a number of different factors. See our Virtual Risk Officer (VRO) Guide for details about how Risk Scores are calculated.

Cyber Security: Links

- **CISA vulnerability scan**
  - cisa.gov/cybersecurity-assessments
- **CDW vulnerability scan**
  - cdwg.com/content/cdwg/en/solutions /cybersecurity/security-threat-check.html
- **SecurityOnion open-source monitoring**
  - securityonion.net
- **Greenbone vulnerability scanner**
  - greenbone.net/en/community-edition
- **WI DPI**
  - dpi.wi.gov/cyber-security
- **WI Cyber Response Teams**
  - det.wi.gov/Pages/Cyber-Response-Teams.aspx

January 7, 2020: Las Vegas Avoided Cyberattack!

Security Alchemy



?

Questions?

Jim Blodgett
Middleton-Cross Plains SD
jblodgett@mcpasd.k12.wi.us

Mike Pullen
Baraboo School District
mpullen@baraboschools.net

Pat Zielke
Viroqua School District
pzielke@viroqua.k12.wi.us

Kevin Capwell
Midwest Educational
Technology Association
kcapwell@brainstormk20.com