DSci526:
Secure Systems Administration

Mid-Semester Change of Gears

Prof. Clifford Neuman

Lecture 10
25 March 2021
Online

Agenda

- This lecture was originally titles Network Monitoring and Attack Forensics, but
  - Much of network monitoring was covered last week.
  - Some attack forensics was also last week and we will see more in the SIEM lecture later.
  - There are many other things to cover today, including review of the mid-term, and transitioning from Group project 1 to Group Project 2.
- Therefore today's agenda will be a little bit different.

Agenda

1405 Web Penetration tools -Pratyush Prakhar
1425 Configuration Management – Marco Gomez and Louis Uuh
1505 Review of questions from Mid-term exam
1535 Break
1545 Presentation by Dark Seas Bank
1605 Team 2 Presentation of Banking Project
1625 Opportunity for Live Presentations of Systems
1645 Discussion of Second Group Project (team assignments)
1700 Breakouts for Second Group Project

March 31st – Security Incident Event Management

- Malavika Prabhakar
- Anthony Cassar
- Dwayne Robinson (Network Perimeter Detection)
- MaryLiza Walker (Attack Forensics)
- Jason Ghetian

Linux Related Topics – April 14th

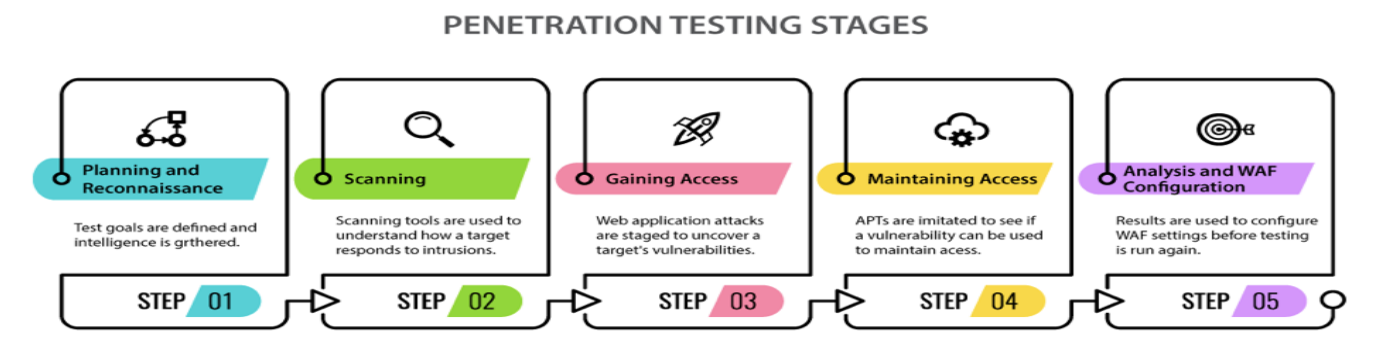
- Azzam Alsaeed – SELinux
- Alejandro Najera – Linux Administration
- Tejas Pandey – Identity Management in Linux
- Ayush Ambastha – Linux Kernel Security

WEB APPLICATION PEN TESTING TOOLS

Pratyush Prakhar
DSci 526
2468183206

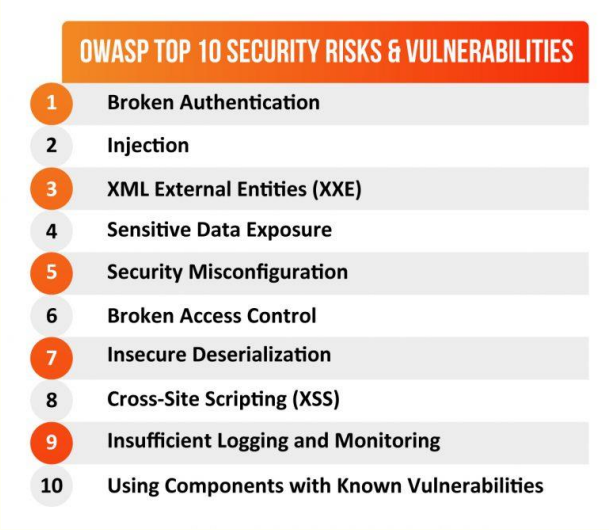
What is Web Application Penetration Testing?

- It is a subset of the process of penetration testing focused on detection and mitigation of the exploitable vulnerabilities present on a target Web Applications. It involves both manual and automated testing.
- This can involve attempting to breach or hack number of application systems such as frontend, backend and even APIs. Bypassing or subverting WAFs is also a prime motive. The WAFs then can be configured later provide better security.
- The tester can uncover multiple web related vulnerabilities such as Injection attacks, XSS and so on in such scenarios.
- The methodology of pen testing is as follows.



What should be tested?

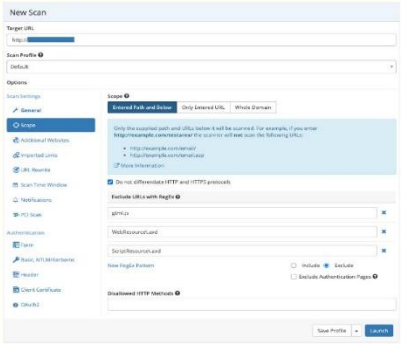
- Every tester has their own playbook with their testing techniques and customized tools. But they are mostly centralized around industrial security best practices and checklists like OWASP Top 10 and OTG.
- In the coming sections, we'll discuss the most used web application pen testing tools by the security professionals today.

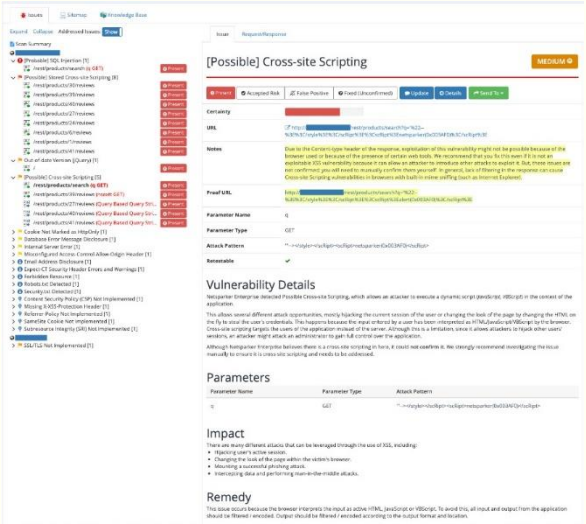


AUTOMATED FRAMEWORKS

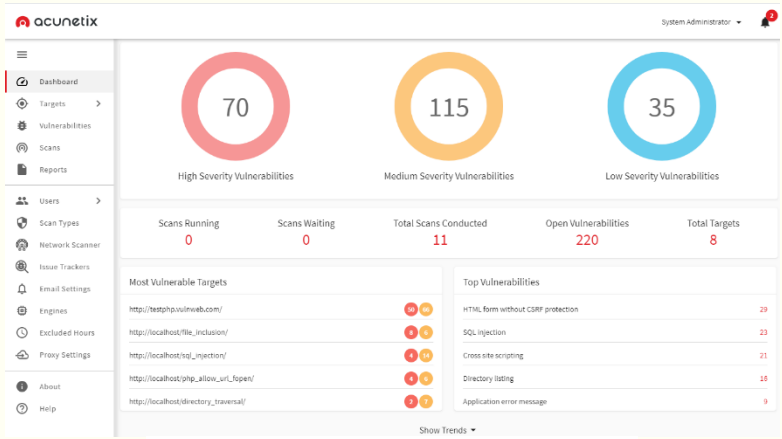
Netsparker

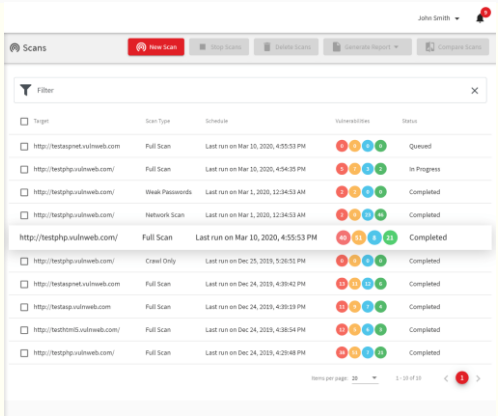
- One of the most famous automated web penetration testing tool. This tool automatically helps you identify the security gaps in your web related resources with support for latest applications such as HTML5 and Web 2.0.
- It helps you identify vulnerabilities scaling form XSS to Injection attacks. One can customize the scans according to one's own need and scope.
- There are couple of features which sets it apart from the other tools in the market:
  - **Advanced crawling** for Single Page Applications and fewer False Positives.
  - Support for scanning over 1000 websites a day.
  - **Proof based Scanning** giving use detailed information about the exploit.
  - **Netsparker Hawk** - out of the band vulnerability scanner.
  - Easy to integrate with CI/CD pipelines such as Jenkins, Jira and Github with support for over 100 members.
  - Helps you generate compliance reports including standards such as ISO 27001, PCI DSS and even HIPPA.





Acunetix Scanner





- It is another automated platform for web app penetration testing. It has all the features that were mentioned in Netsparker. On top of it, the selling points would be
  - Detection for over 6500 vulnerabilities such as SQL Injection, Weak credentials, and exposed sensitive information.
  - Has **Macro Recording** feature that simplifies the complex application data flow.
  - Has support for various well-known vulnerabilities for WordPress and Joomla.
  - It can integrate easily with WAFs deployed and helps in bug tracking through SDLC.
  - Components like **DeepScan** crawl the websites emulating a real hacker like behavior while **AcuSensor agent and AcuMonitor** allow the platform to detect vulnerabilities combing the concepts of black box testing and code analysis. The mitigation and notification phase can also be automated.

Intruder

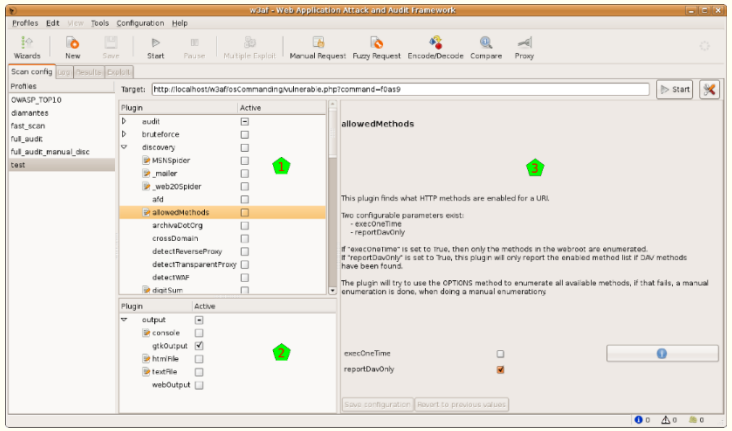
- Intruder Systems based out of London also have their own automated vulnerability scanner. The key features involve
  - Minutely configured security checks ranging over 10000
  - Automated Common Weakness and Vulnerability scanner leading to proactive and automated analysis.
  - Integration through plugins for latest testing tools and intuitive interaction.
  - End points for common cloud platforms like Azure, AWS and Google cloud.

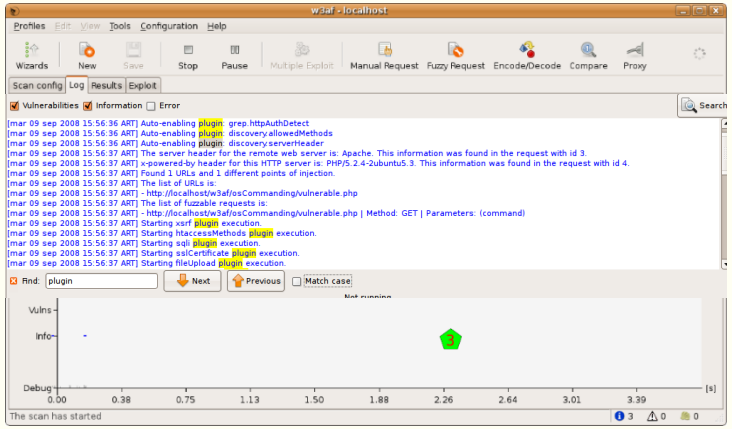
EXPLOITATION FRAMEWORKS – MANUAL TESTING

W3AF

- It is one of the most utilized web penetration testing framework which is developed over Python. This can help you find over 200 known security flaws such as CSRF, XSS and Insecure Deserialization.
- It has three distinctive plugins categories as
  - Attack
  - Audit
  - Discovery

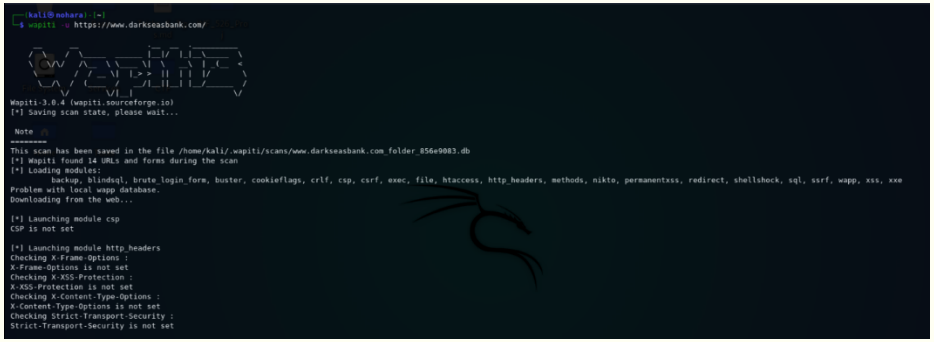
  The plugins can communicate with each other to create small automated paths.
- The key highlights include
  - MiM proxy to intercept the web requests which the discovery plugins can use to segregate URLs.
  - HTTP and DNS response cache
  - Cookie handling
  - Spoofing user agent and other fields.
  - Full customization of the headers for requests.





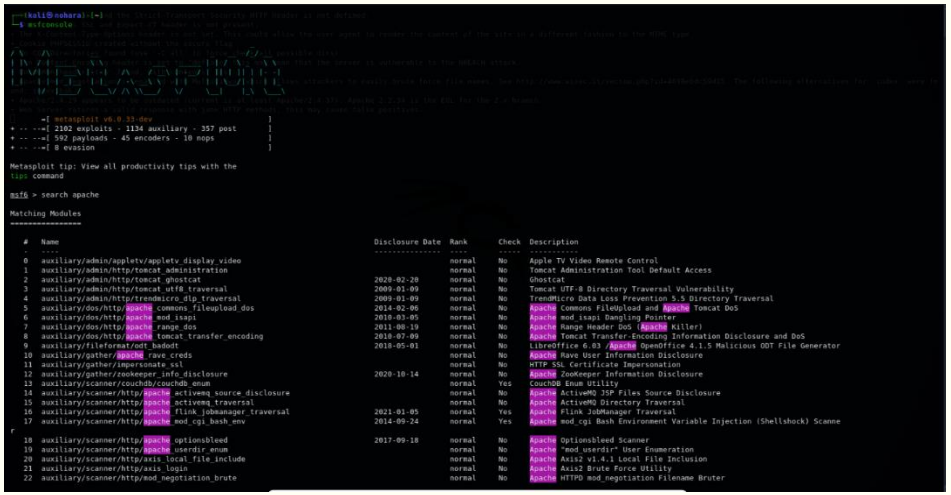
Wapiti

- Termed as a Web Application Vulnerability Scanner, Wapiti performs “**black-box**” scans on the target web application and present data to the fuzzing component. It is an open-source project from SourceForge and devloop.
- The fuzzer is responsible to test the various injectable points on the scanned URLs with scripts to detect vulnerabilities such as
  - LFI/RFI
  - SSRF
  - Injection attacks
  - Bypassing weak configuration files.
  - Brute force directories
  - CSP policy and Header flags evaluation
- The tool supports both **GET and POST** methods for the attacks. It uses modules **like buster** for directory brute forcing and **wapp** for web app versions.
- Also provides support to various Authentication methods like Kerberos and NTLM.



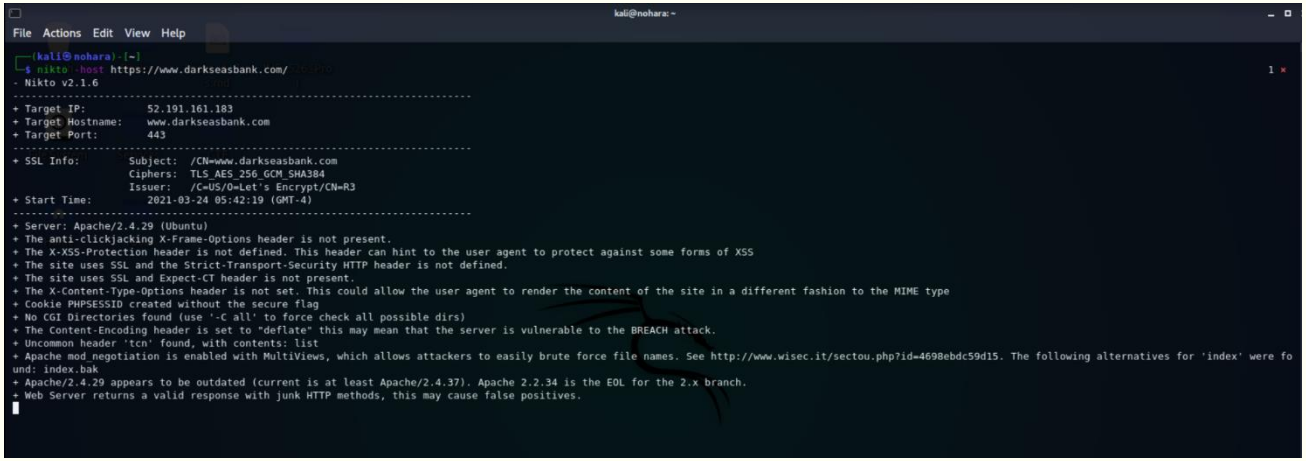
Metasploit

- It is termed as one of the most advanced and popular framework used for penetration testing. It consist of various modules for almost every component out there with known vulnerabilities.
- It is an open-source tool created by Rapid7. The framework is written in **Ruby.**
- It is a flexible framework allowing the testers to create and modify the module files to create their own customized scripts.
- The Metasploit framework relies on multiple modules to create a whole attack path or bits and parts of it. They are as:
  - Auxiliary – Scanner
  - Exploits – Known exploits for the target software
  - Payloads – Various payloads available for injection
  - Post – for post exploitation phase for exfiltration or creating persistence
  - Others



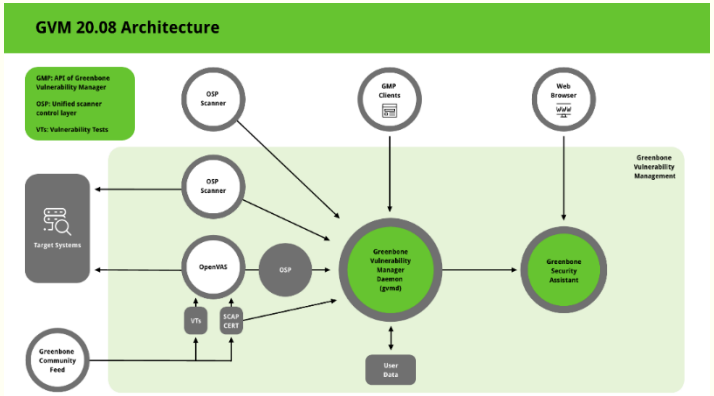
Nikto

- Nikto is an open-Source web server scanner performing a comprehensive scan of the target website for over 6700 vulnerable programs.
- It has support for modern day server technology as well as legacy. But it is not a stealthy tool and creates lot of noise. It will be easily caught by the IDS/IPS in place.
- It is coded on the Perl environment. Has host authentication and encoding capabilities.
- Other key features include:
  - SSL/TLS support for HTTPs requests
  - Multiple file format support such as HTML, CSV, XML..
  - Basic authentication methods
  - Credentials stuffing for Apache and IIS
  - Picks up unusual headers as well as automated evasion techniques.
  - CLI accessibility.



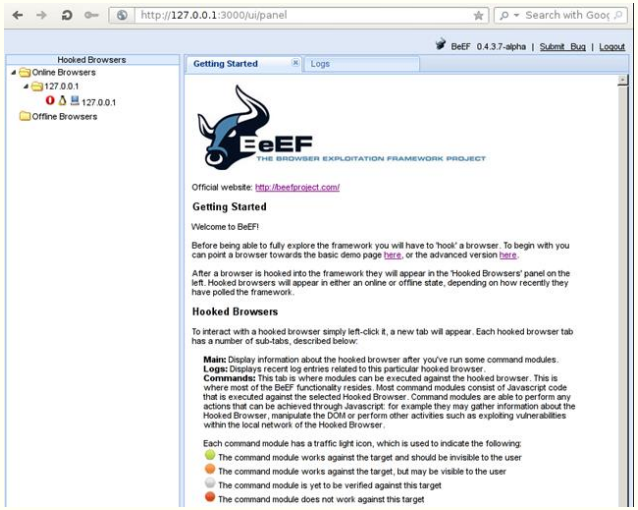
OpenVAS

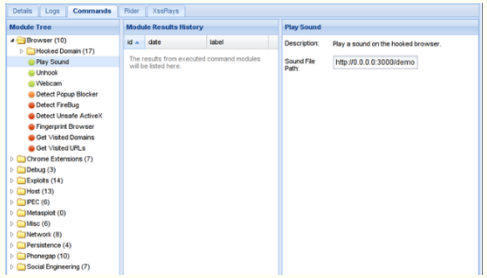
- Open Vulnerability Assessment System is a framework with multiple network as well as web services for vulnerability assessment.
- It has comprehensive list of plugins and features that collect and analyses web responses and then this can be used by other tools like Metasploit.
- The scan scope is very large and contains over 80,000 known vulnerabilities. It is maintained by Green bone Networks since 2009. Has both paid and free version.
- It is controlled via Open Scanner Protocol daemon which communicates with gmvd which is responsible for maintaining the vulnerability test database and decision making. The data is transported through XML files.



BeEF

- It stands for Browser Exploitation Framework. It is largely focused on the web bowser exploitation. It is adapted to web borne attacks.
- BeEF is designed to analyze and explore weaknesses in the target's framework and network perimeter. Its whole exploitation is based on single source, the browser.
- A hook is used as a js script to be included on the website and then the various modules can run on the webserver through this agent.





FUZZERS

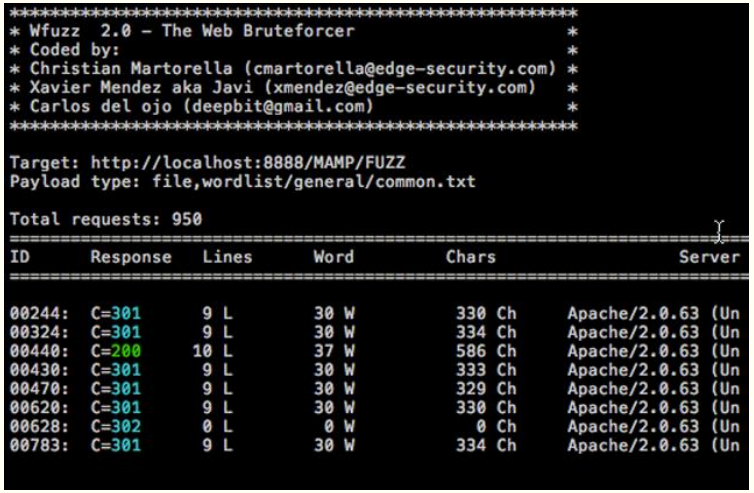
Directory Brute force and Fuzzing

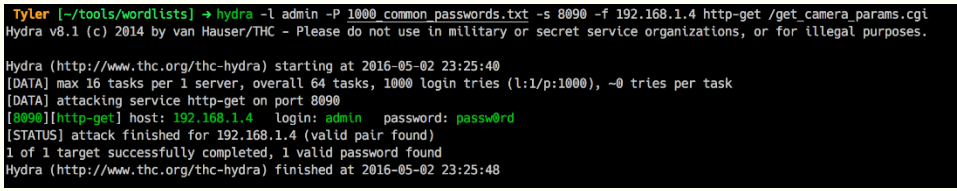
WFUZZ

- It is a tool used to brute force Web applications.
- It has wide range of capabilities from GET and POST parameters fuzzing to SQL, XSS and other injection attacks.
- It has features like Recursive search, header brute forcing, multi threading and SOCK support, multiple payloads and encoding to name a few.

THC HYDRA

- Hydra is a parallelized login cracker and pen testing tool. It is very fast and flexible, and new modules are easy to add. This tool allows researchers and security consultants to find unauthorized access.
- It has supportive features such as rainbow tables, multiple hash techniques, GET and POST parameters and login forms too.





Some others in my toolkit

- Proxies such as **Burp Suite and ZAP Proxy** with additional web exploitation features.
- **SQLMap and SQL Ninja** used to find out SQL Injection attacks against all known databases.
- **Nessus** is another vulnerability scanner with similar features to **NMAP** Scripting Engine (**NSE).**
- Directory Brute forcers such as **Dirb, Dirbuster and latest Gobuster.**
- **Wpscan and JoomlaScan** depending upon the related web applications. They have extensive checks for themes and plugins.
- **John the Ripper, Cain & Able and Hashcat** are commonly used for credentials cracking. Wide support for hashes and even encrypted files.

THANK YOU

Configuration Management

Marco Gomez
Louis Uuh
DSci 526
24 Mar 2021

NIST 800 – 171 r2

3.4.1

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2

Establish and enforce security configuration settings for information technology products employed in organizational systems.

3.4.3

Track, review, approve or disapprove, and log changes to organizational systems.

NIST 800 – 171 r2

3.4.4

Analyze the security impact of changes prior to implementation.

3.4.5

Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

3.4.6

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

NIST 800 – 171 r2

3.4.7

Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8

Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9

Control and monitor user-installed software.

Startup 3.4.1

Inventory

Must inventory the entire system. All HW and their FW version, SW and their version, Documentation

-Low Level / End Point SW Listing

Use MS Power Shell to obtain a list of running SW.

-Higher System Level

Use Tripwire to obtain SW throughout the system.

-Collaborate with Logistics to gather information on purchased HW; obtain current level of FW onboard.

-Must update documentation as updates/changes occur

Baselining

3.4.1 - In order to know what changes need to occur or have occurred, you must know where you started.

Tools to Help with 3.4.2/3/4/5 (Enforce)/7

Security Technical Implementation Guide (STIG) Viewer / Security Content Automation Protocol (SCAP) Benchmarks

Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline.

Microsoft Power Shell

Low Level / End Point SW Listing

Use MS Power Shell to obtain a list of running applications:

```
Get-ItemProperty
HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
\* | Select-Object DisplayName, DisplayVersion, Publisher, InstallDate |
Format-Table –AutoSize > C:\Users\USERNAME\Desktop\Installed.txt
```

Tools to Help with 3.4.2/3/4/5 (Enforce)/7 cont.

Tripwire

Detects changes in the system based off its initial scan of the system (baseline) and monitors for change.

AFICK

Detects changes in files. Provides an alert when an unauthorized change has occurred/is occurring.

Privilege Management

System

3.4.6: The entire system whether it be on network devices, end points, or in between must have least privilege applied. Role Based can be instituted but, monitoring the system for inadvertent or unauthorized privilege escalation could be a sign that an attacker is in your system.

NIST 800-53r5 can also assist in guiding your implementation.

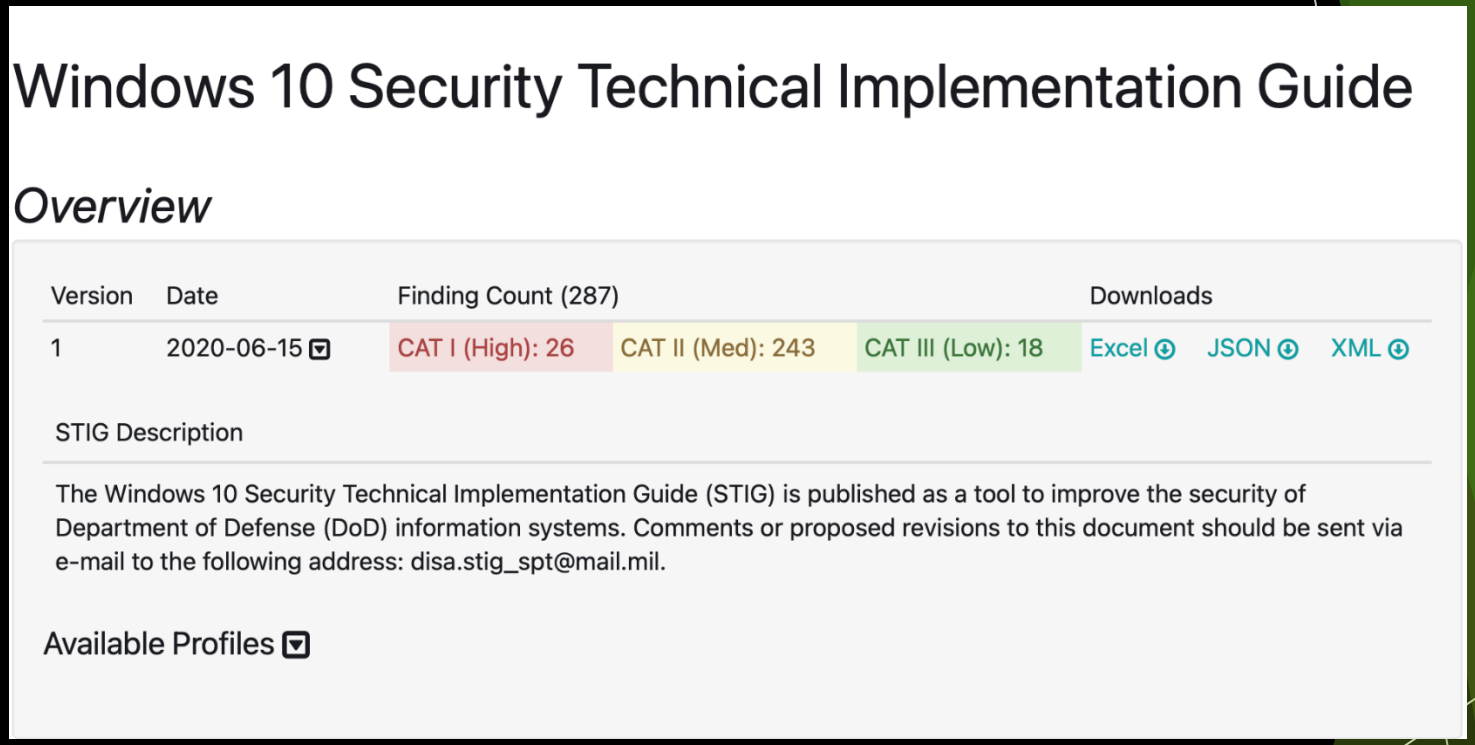
Thycotic

Can check accounts and point out if they may be overprivileged.

Centrify

Allows for the management of privileges.

Live Demo



Windows 10 Security Technical Implementation Guide

Overview

Version	Date	Finding Count (287)			Downloads		
1	2020-06-15	CAT I (High): 26	CAT II (Med): 243	CAT III (Low): 18	Excel	JSON	XML

STIG Description

The Windows 10 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. Comments or proposed revisions to this document should be sent via e-mail to the following address: disa.stig_spt@mail.mil.

Available Profiles

Patch Management 3.1/3/4

Change Management

End Point

3.4.8/9: Management can be difficult in small company settings and it can be expensive for them to purchase SW to aid in managing and monitoring for changes. Users must be controlled from uploading/installing unauthorized SW.

Larger organizations should have personnel in place to handle and even prevent this from occurring.

System

Small systems must have a few select individuals that make changes to the overall system and close collaboration must be maintained with management.

Large scale systems usually come along with bigger budgets. Thus, instituting a full CM system should be easier.

References

NIST 800-171r2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

NIST 800-70r4
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf

NIST 800-128
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

NIST 800-167
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

NIST 800-53r5
https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

DoD Cyber Exchange
https://public.cyber.mil/

Thycotic
https://thycotic.com/solutions/free-it-tools/least-privilege-discovery-tool/

Centrify
https://www.centrify.com/pam/privilege-elevation/privilege-elevation/

DSci526:
Secure Systems Administration

Discussion of Mid-Term Exam

Prof. Clifford Neuman

Lecture 10
24 March 2021
Online

Mid-Term Exam

https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/

1. **(20 points) Describe a high-level security policy that would be appropriate for the system maintained by the US as described in the article you just read. Specifically, start with the motivation and principles to be applied? Secondly, discuss requirements on the strength of protection that must be achived, and the kinds of threats against which the system shal remain "secure". Hint: You should consider the outline of organizational policies discussed in lecture 2, but it will need to be abbreviated because you are only allotted 20 minutes for this question.**

2. **(25 points) How would effective configuration management (as discussed in lecture 5) assist in achieving the goals you set forth in (1). Specifically, what aspects of configuration management might help to prevent compromise from supply chain attacks such as solar wind, and how might it leave us in a better position to detect AND recover from such a compromise.**

3. **(25 points) Composition of systems and protection domains - Containment Architecture - Discuss your recommendation for a containment architecture for this system. Specifically, what are the classes of data, the required access to that data, what do you advise for protection domains, and how will you implement containment across domains witin the system. Note that this is similar to the initial homework assignment, and the individual assignment preceding your group project, and we also discussed some aspects of this in one of our lectures. Note also that at least one aspect of this is explicitly mentioned within the news article that you just read.**

Mid-Term Exam

4. **(20 points) There are many places where access decisions are implemented within the system that you have re-designed. List several (at least the two best examples of each) of the Policy Enforcement Points (PEP) and Policy Decision Points (PDP) in your system. For each, tell me also whether there is a policy information point (PIP), and where the Policy Administration Point (PAP) resides.**

5. **(10 points) NIST 800-171 - When we discussed NIST-800-171 in lecture 3, there was one recommendation that was described in the introduction, but which was not a specifically listed control among the 110 controls we discussed. It appears that this this recommendation was not followed in the originally deployed architecture of the court's information system. Please tell me what the recommendation was and tell me also how proper implementation of the recommendation might have limited the impact of the solar winds breach on the system described in the Krebs on Security article.**

DSci526:
Secure Systems Administration

First Group Project
Final Reports to Class

Prof. Clifford Neuman

Lecture 10
24 March 2021
Online

Wrapping up Project One

- It is time to wrap up exercise One by today, March 24th - each group prepared a report describing:
  - User documentation for their application (high level)
  - Their network and server architecture (what servers are on what VM's and how they are interconnected)
  - A risk assessment/vulnerability analysis enumerating the risks, explaining the mitigation of those risks, and listing those threats that are not defended against (i.e. where you accept the risks).
  - A description of the steps taken for pen testing of your system.
  - Next week, your team will have 20 minutes to present this summary to the entire class (this time, no withholding of information from the other team)
  - (today, the basic presentation, and breakout groups)
- We will use 20 minutes today to demonstrate the operation of your systems.
  - I would like an opportunity to access your system at some point in the next week, before the next lecture.
  - We will perform additional testing during next week's lecture.
  - Please prepare a list of tests (with appropriate scripts) that you believe should be run against your system, and the other team's system, and send me that list of tests by Monday..

DarkSeas Bank

Team 1

Masterminds of DarkSeas Bank!

–Shagun Bhatia
–Anthony Cassar
–Sarahzin Chowdhury
–Aditya Goindi
–TejasKumar Pandey
–Malavika Prabhakar
–Pratyush Prakhar
–Dwayne Robinson
–Christopher Samayoa
–Amarbir Singh
–Louis Uuh
–Shanice Williams

Agenda

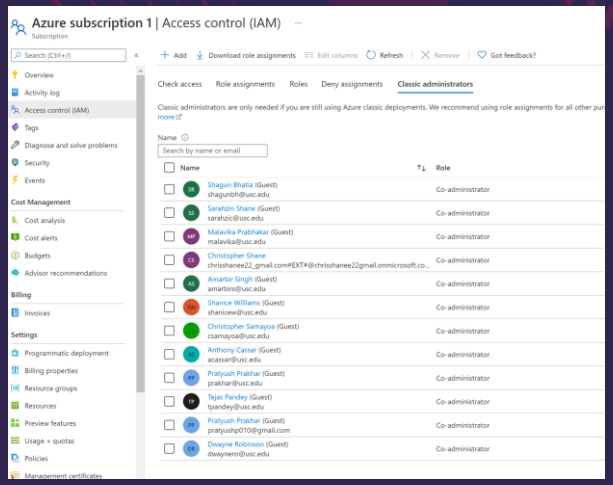
- Platform Administration / Server Deployment
- VPN / Firewall
- Front End Web Application
- SIEM
- Red Team

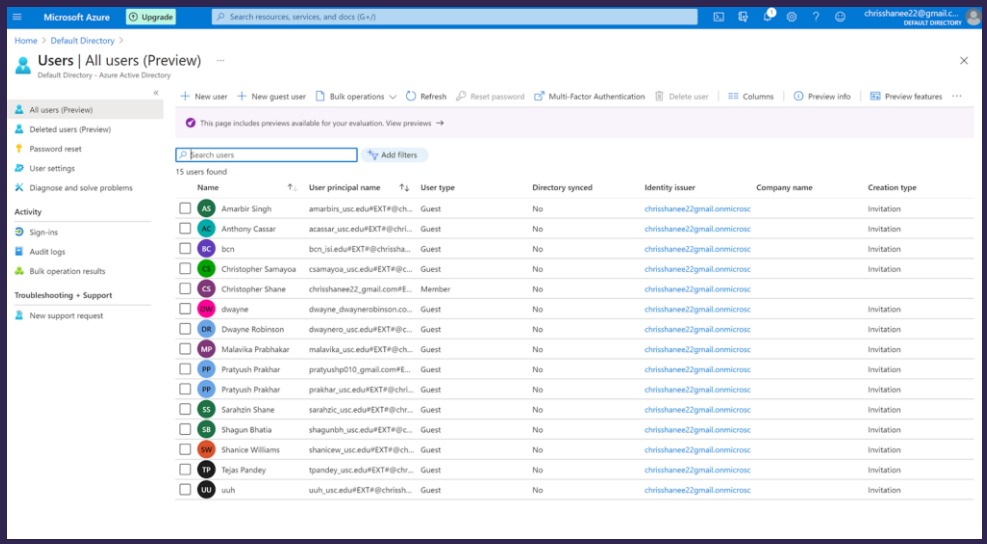
Why Azure?

Feasibility, Centralized Location, Access Control

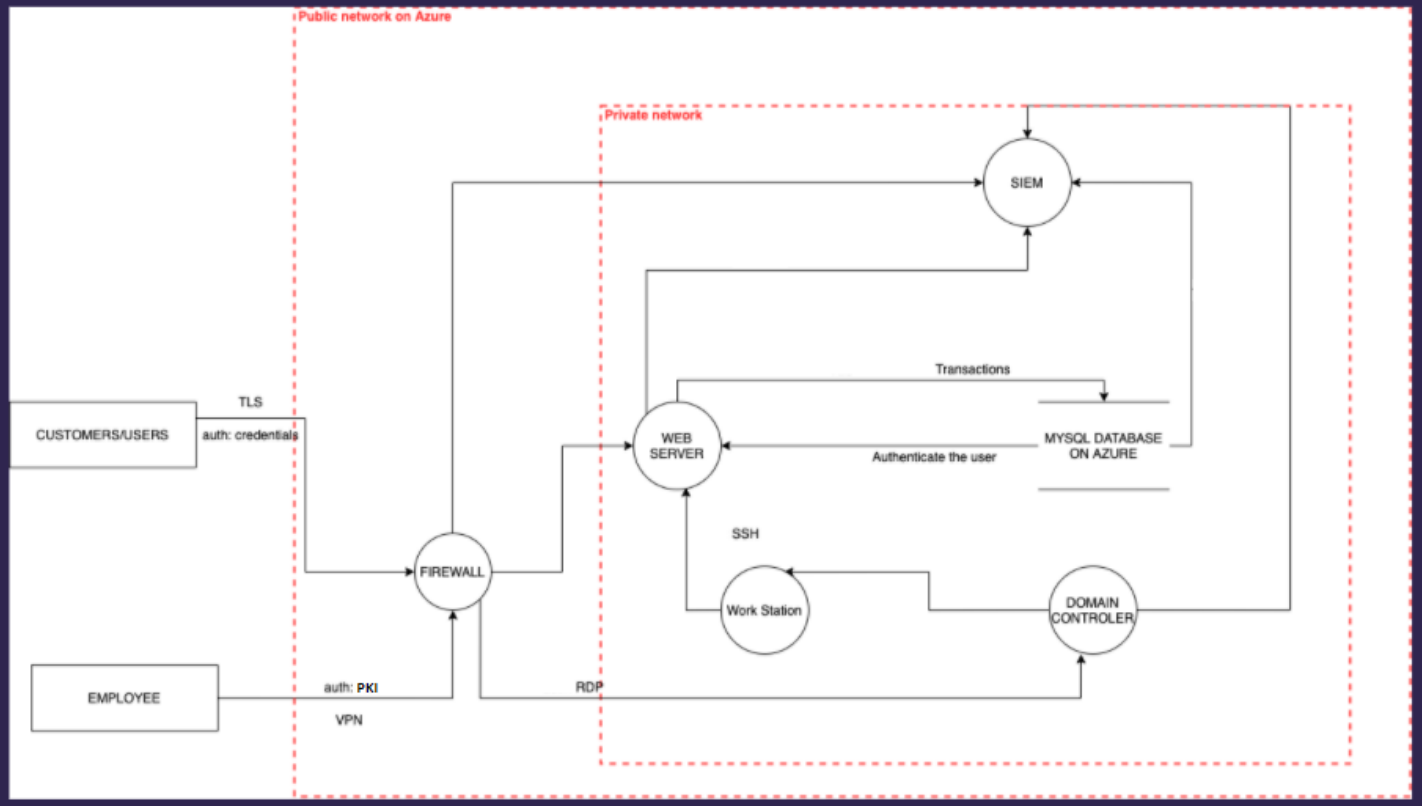
On-premises, across multiple clouds, and at the edge; integrations to manage all aspects of the cloud and On prem environment (hybrid cloud).

Microsoft Azure





Architectural Design



List of Servers

- Windows Servers
  - Domain Controller
  - Certificate Authority (CA)
  - Management box
- Linux Servers
  - Web Server
  - MySQL server

Windows Hardening

DoD and NIST Configuration

- STIG February 2021
- Active Directory Challenges
- Azure Defense Mechanisms
- Positives and Negatives

Image Source:https://www.threatstack.com/blog/what-is-the-nist-cybersecurity-framework

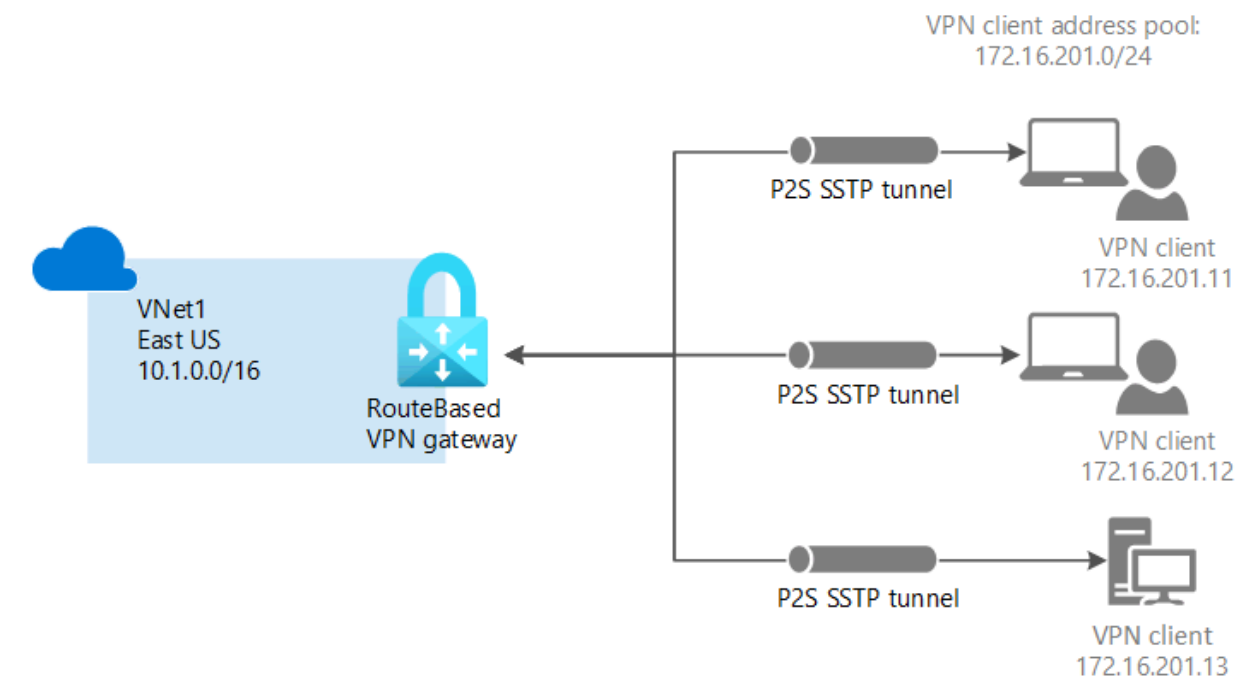
Linux Servers

- Web Server Deployment Detail
  - Ubuntu 18.04
  - Apache 2.4.29
  - PHP 7.2.24
  - SFTP
    - Non-administrative group (no SSH access) for website management

```
Match Group sftpusers
        ChrootDirectory /var/www/
        ForceCommand internal-sftp
        X11Forwarding no
        AllowTcpForwarding no
```

- MySQL Server
  - Version 5.7
  - Azure specific instance

VPN - Azure Virtual Network Gateway



Source: Microsoft

DarkSeas Bank Firewall

- We analyzed numerous firewall options provided by vendors listed below.
  - Juniper Networks
  - ThreatStop
  - 5nine Technologies
  - Fortinet
  - Barracuda
  - ForcePoint
  - Cisco
- We decided to implement the built-in Azure firewall
  - Pros
    - Intuitive Interface
    - Seamless Integration
  - Cons
    - Costs – The per hour rate of the product was expensive, due to the Azure environment we were able to leverage the costs but shutting down the servers when not in use for a development environment.

DarkSeas Bank Firewall

MACHINE NAME: DC DARK

PUBLIC IP: N/A

PRIVATE IP: 10.0.2.7

OPEN PORTS: none externally

MACHINE NAME: DS-Web01-Ubuntu

PUBLIC IP: 52.191.161.183

PRIVATE IP: 10.0.2.4

OPEN PORTS: 80, 3306, 465, 587, 443

MACHINE NAME: Dark-WK-01

PUBLIC IP: N/A

PRIVATE IP: 10.0.2.8

OPEN PORTS: none externally

- In addition the the external firewall, we also decided to use host based firewall for each system to enable extra protection to the machines.

Front-End Web Server

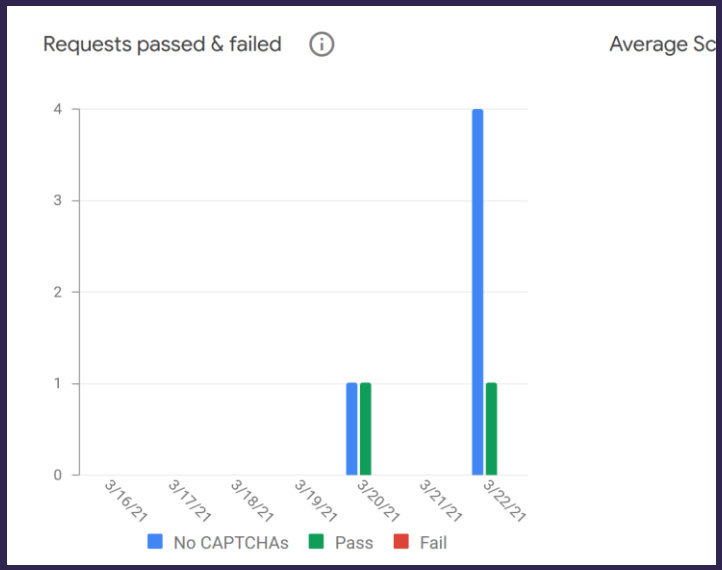
Live password feedback helps users avoid using commonly used and weak passwords

Google reCaptcha helps verify legitimate users are accessing the website

Email verification is used to verify accounts, so users are not creating accounts with fake information

Two factor authentication is used to sign in, so only the compromised passwords won't lead to unauthorized access

SSL helps avoid sensitive information disclosure during transfer



Database Server

Standalone minimized database server promotes principle of least of functionality

Connections only from pre configured endpoints are allowed

Separate databases used for different classes of information

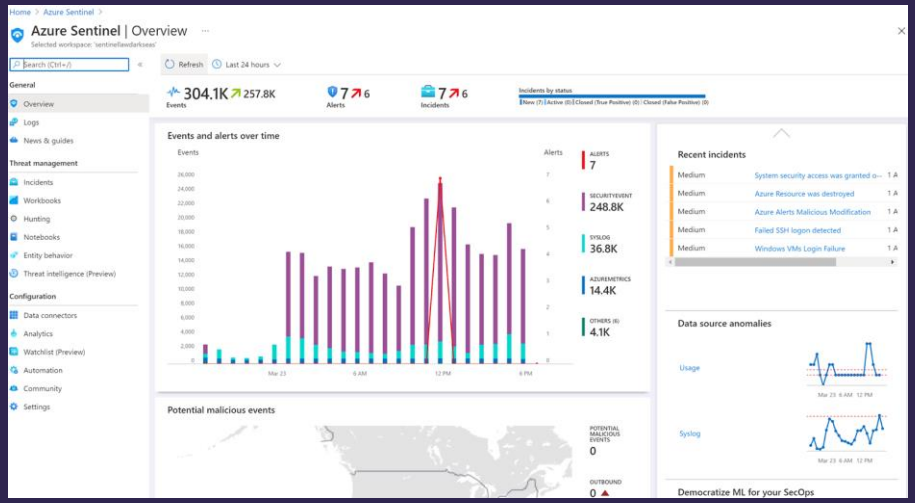
User authentication before data retrieval helps stop unauthorized access

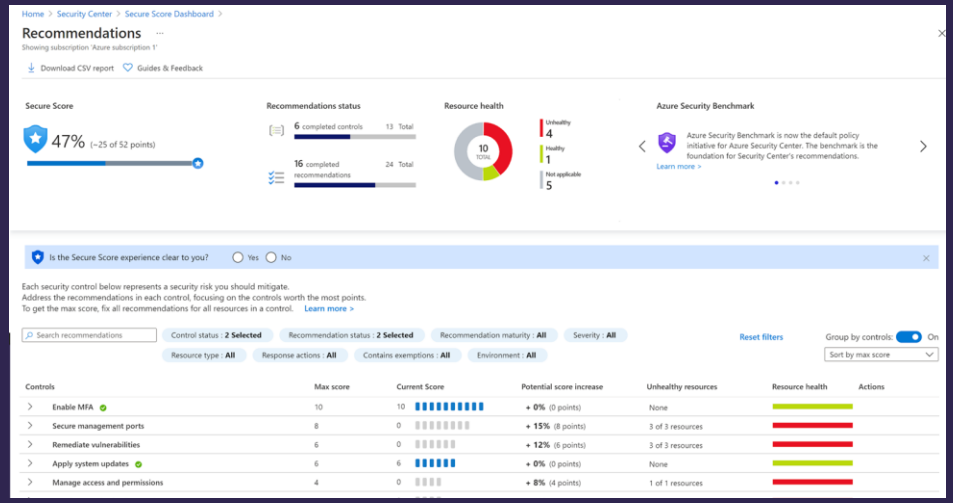
Sensitive data is not stored in cleartext, mitigates damage in case of compromise

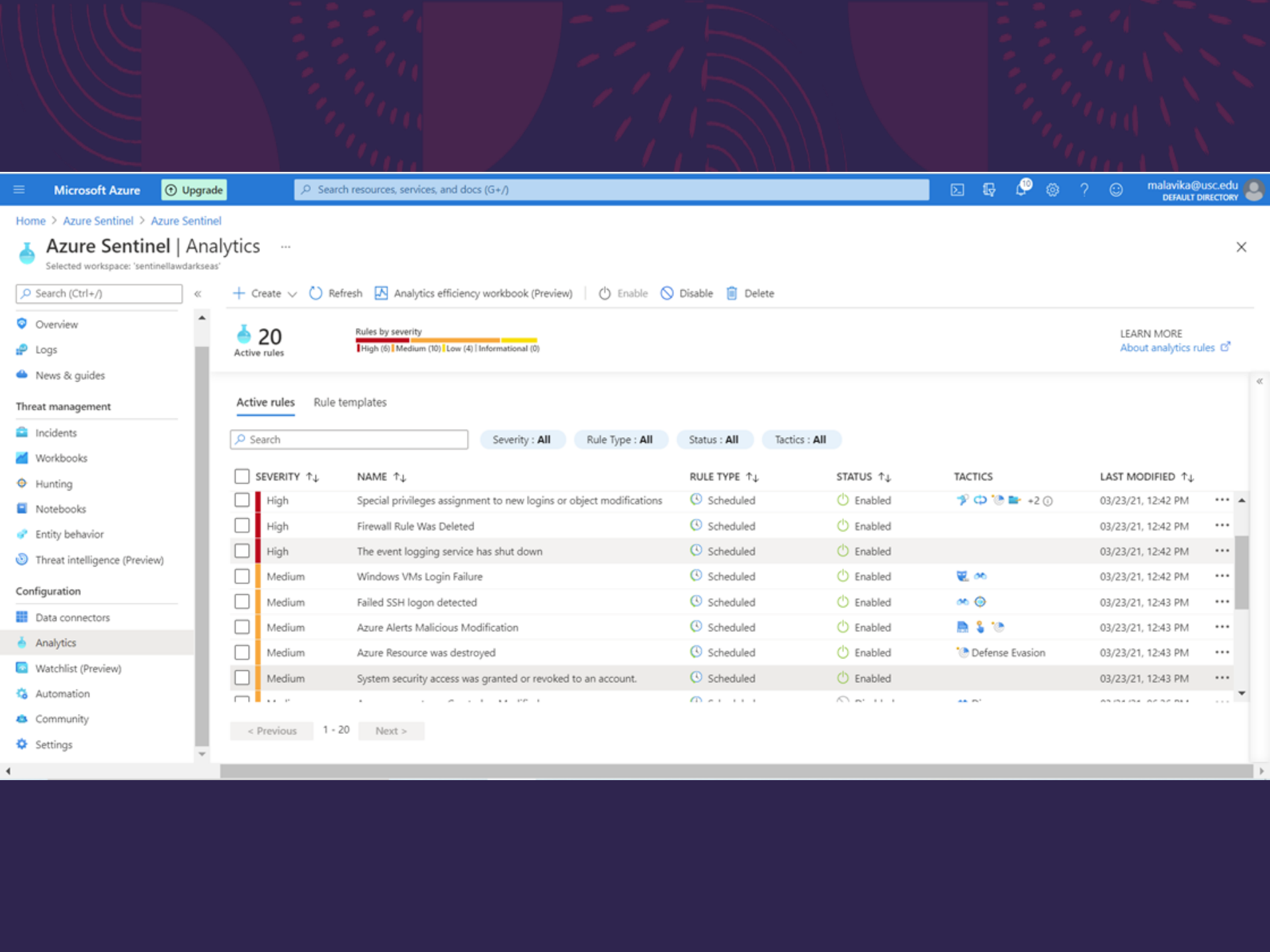
Sentinel (SIEM)

Cloud native, easy connectors, centralized log collection, scaling, speed, and ingestion benefits.

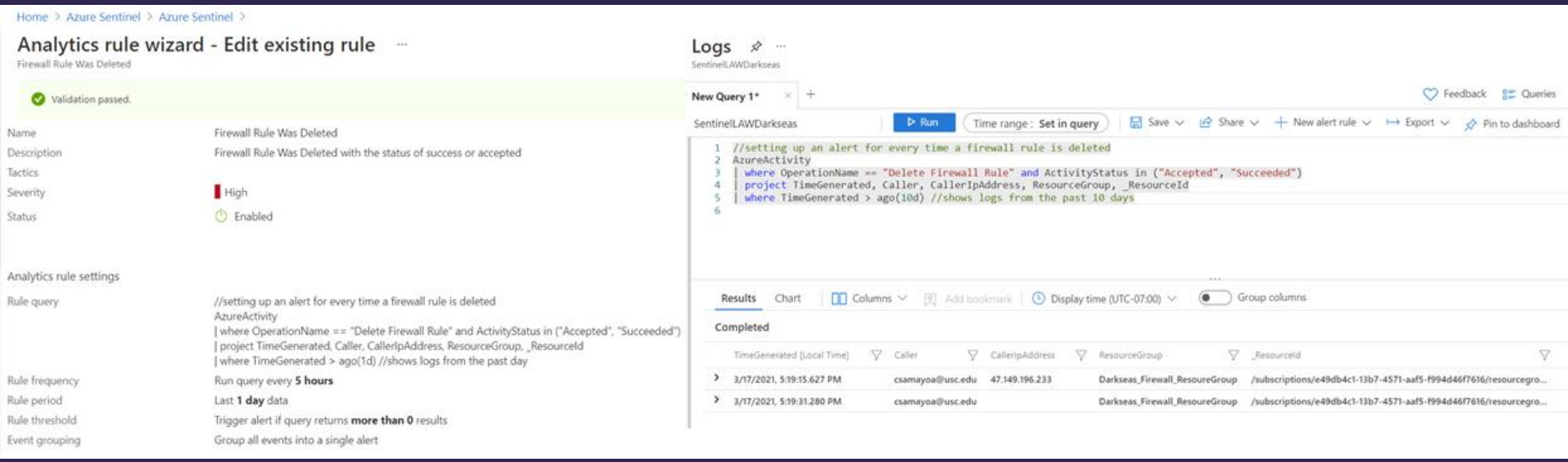
Azure Activity Logs, Office 365 Audit Logs (all SharePoint activity and Exchange admin activity), and **Azure Security Center** (among many more) can be ingested at no additional cost into both Azure Sentinel, and Azure Monitor Log Analytics.



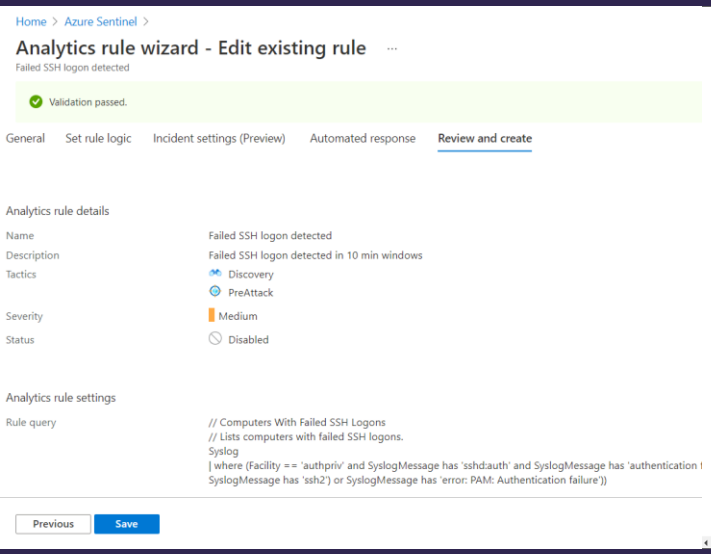


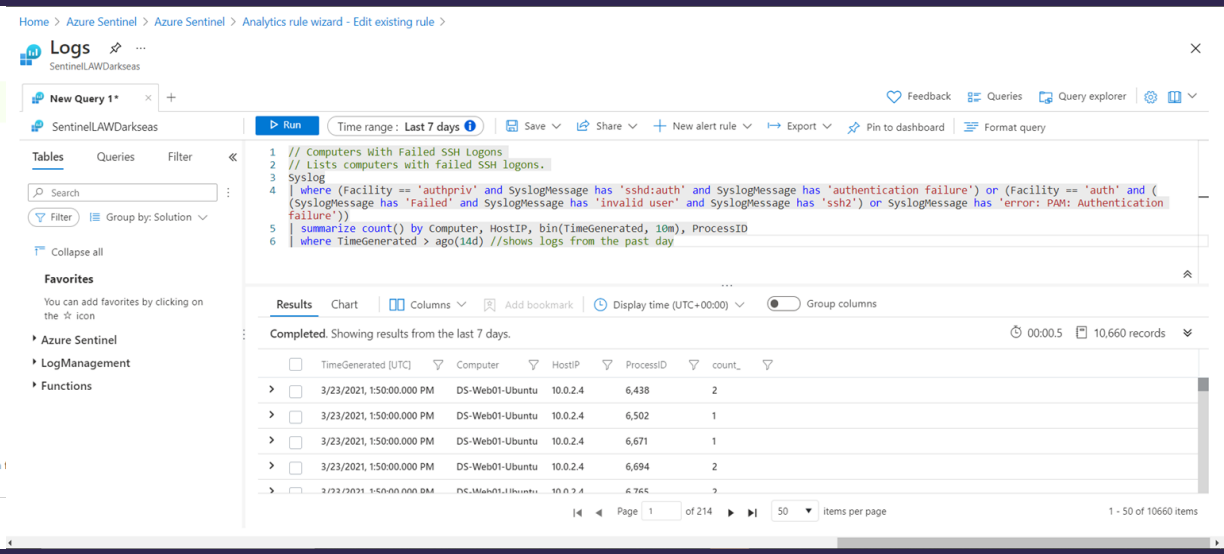

Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
malavika@usc.edu
DEFAULT DIRECTORY
Home > Azure Sentinel > Azure Sentinel
Azure Sentinel | Analytics
Selected workspace: 'sentinellawdarkseas'
Search (Ctrl+/)
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence (Preview)
Configuration
Data connectors
Analytics
Watchlist (Preview)
Automation
Community
Settings
Create
Refresh
Analytics efficiency workbook (Preview)
Enable
Disable
Delete
20
Active rules
Rules by severity
High (6) Medium (10) Low (4) Informational (0)
LEARN MORE
About analytics rules
Active rules
Rule templates
Search
Severity : All
Rule Type : All
Status : All
Tactics : All
SEVERITY
NAME
RULE TYPE
STATUS
TACTICS
LAST MODIFIED
High Special privileges assignment to new logins or object modifications Scheduled Enabled +2 03/23/21, 12:42 PM
High Firewall Rule Was Deleted Scheduled Enabled 03/23/21, 12:42 PM
High The event logging service has shut down Scheduled Enabled 03/23/21, 12:42 PM
Medium Windows VMs Login Failure Scheduled Enabled 03/23/21, 12:42 PM
Medium Failed SSH logon detected Scheduled Enabled 03/23/21, 12:43 PM
Medium Azure Alerts Malicious Modification Scheduled Enabled 03/23/21, 12:43 PM
Medium Azure Resource was destroyed Scheduled Enabled Defense Evasion 03/23/21, 12:43 PM
Medium System security access was granted or revoked to an account. Scheduled Enabled 03/23/21, 12:43 PM
< Previous
1 - 20
Next >

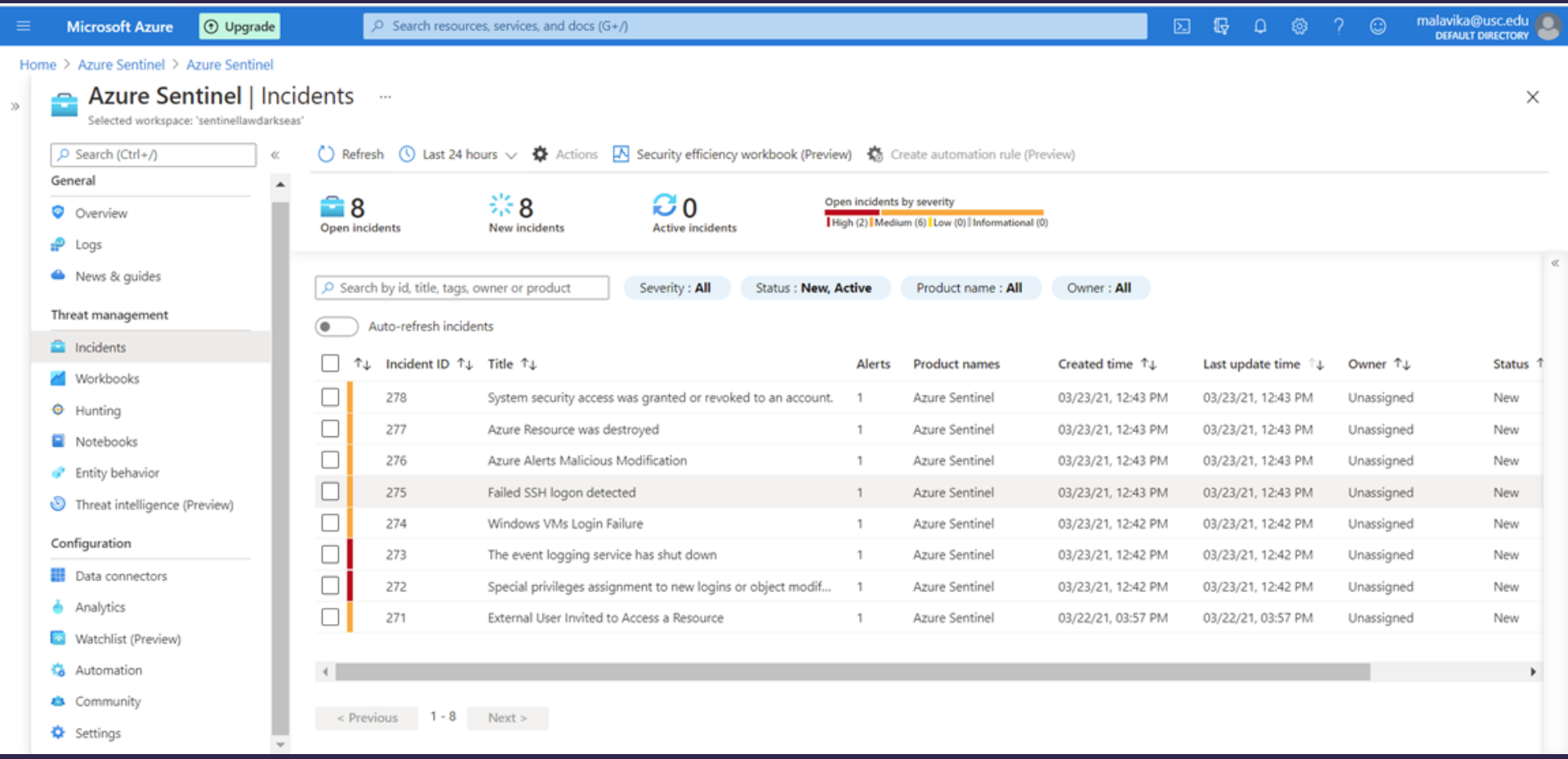
Sentinel Logic Example:



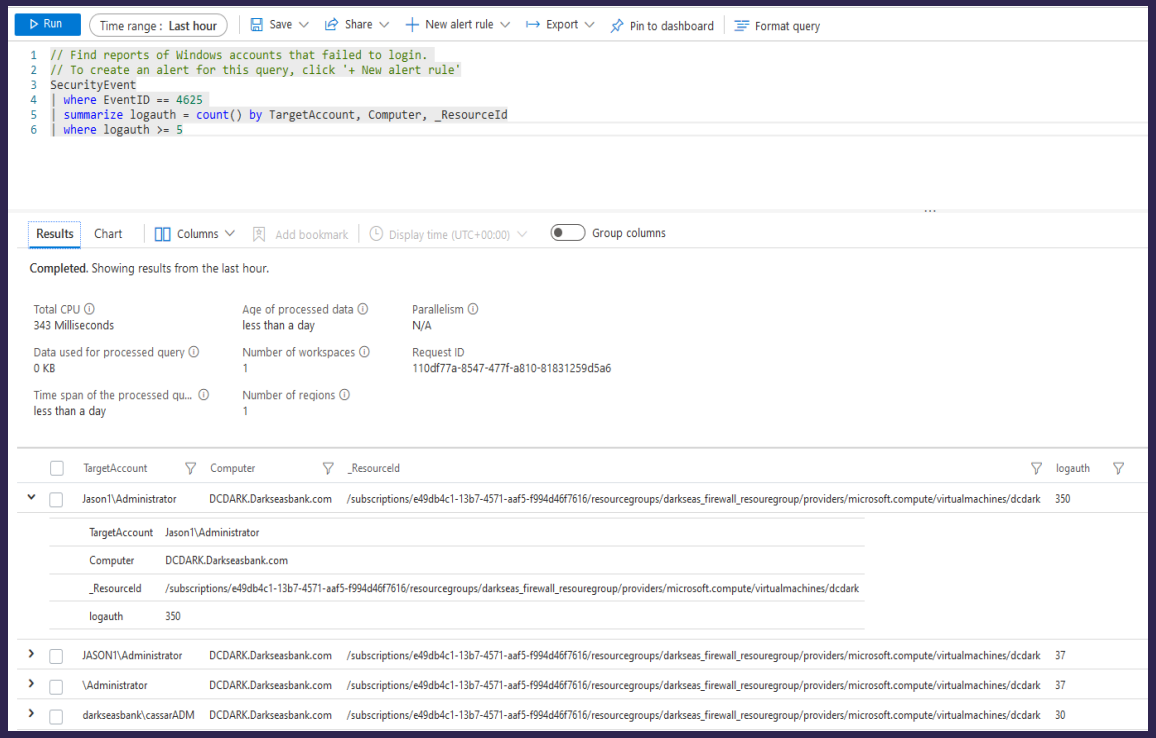
Sentinel Logic Example:






Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
malavika@usc.edu
DEFAULT DIRECTORY
Home > Azure Sentinel > Azure Sentinel
Azure Sentinel | Incidents
Selected workspace: 'sentinellawdarkseas'
Search (Ctrl+/)
General
Overview
Logs
News & guides
Threat management
Incidents
Workbooks
Hunting
Notebooks
Entity behavior
Threat intelligence (Preview)
Configuration
Data connectors
Analytics
Watchlist (Preview)
Automation
Community
Settings
Refresh
Last 24 hours
Actions
Security efficiency workbook (Preview)
Create automation rule (Preview)
8
Open incidents
8
New incidents
0
Active incidents
Open incidents by severity
High (2) Medium (6) Low (0) Informational (0)
Search by id, title, tags, owner or product
Severity : All
Status : New, Active
Product name : All
Owner : All
Auto-refresh incidents
Incident ID
Title
Alerts
Product names
Created time
Last update time
Owner
Status
278 System security access was granted or revoked to an account. 1 Azure Sentinel 03/23/21, 12:43 PM 03/23/21, 12:43 PM Unassigned New
277 Azure Resource was destroyed 1 Azure Sentinel 03/23/21, 12:43 PM 03/23/21, 12:43 PM Unassigned New
276 Azure Alerts Malicious Modification 1 Azure Sentinel 03/23/21, 12:43 PM 03/23/21, 12:43 PM Unassigned New
275 Failed SSH logon detected 1 Azure Sentinel 03/23/21, 12:43 PM 03/23/21, 12:43 PM Unassigned New
274 Windows VMs Login Failure 1 Azure Sentinel 03/23/21, 12:42 PM 03/23/21, 12:42 PM Unassigned New
273 The event logging service has shut down 1 Azure Sentinel 03/23/21, 12:42 PM 03/23/21, 12:42 PM Unassigned New
272 Special privileges assignment to new logins or object modif... 1 Azure Sentinel 03/23/21, 12:42 PM 03/23/21, 12:42 PM Unassigned New
271 External User Invited to Access a Resource 1 Azure Sentinel 03/22/21, 03:57 PM 03/22/21, 03:57 PM Unassigned New
< Previous
1 - 8
Next >

Sentinel Logic Example:



Run | Time range : Last hour | Save | Share | New alert rule | Export | Pin to dashboard | Format query

```
1  // Find reports of Windows accounts that failed to login.
2  // To create an alert for this query, click '+ New alert rule'
3  SecurityEvent
4  | where EventID == 4625
5  | summarize logauth = count() by TargetAccount, Computer, _ResourceId
6  | where logauth >= 5
```

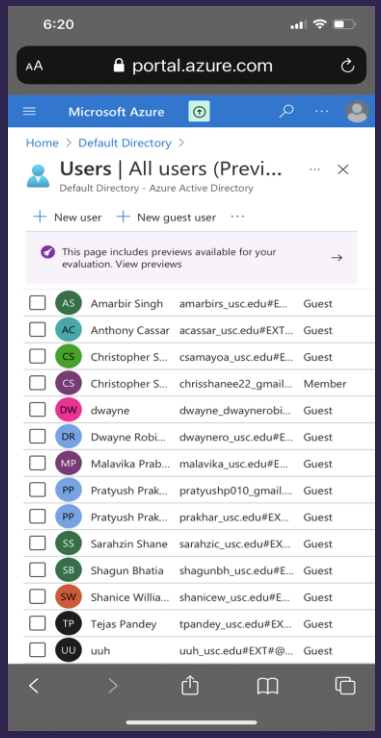
Results | Chart | Columns | Add bookmark | Display time (UTC+00:00) | Group columns

Completed. Showing results from the last hour.

Total CPU 343 Milliseconds	Age of processed data less than a day	Parallelism N/A	
Data used for processed query 0 KB	Number of workspaces 1	Request ID 110df77a-8547-477f-a810-81831259d5a6	
Time span of the processed qu... less than a day	Number of regions 1		

TargetAccount	Computer	_ResourceId	logauth
Jason1\Administrator	DCDARK.Darkseasbank.com	/subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark	350
JASON1\Administrator	DCDARK.Darkseasbank.com	/subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark	37
\Administrator	DCDARK.Darkseasbank.com	/subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark	37
darkseasbank\cassarADM	DCDARK.Darkseasbank.com	/subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark	30

TargetAccount	Jason1\Administrator
Computer	DCDARK.Darkseasbank.com
_ResourceId	/subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark
logauth	350



RED TEAM / PENETRATION TESTING

1. Burp Suite Professional
2. SSL Labs
3. Nessus Professional Scanner
4. Nmap
5. Nikto
6. OpenVAS

Threat Model

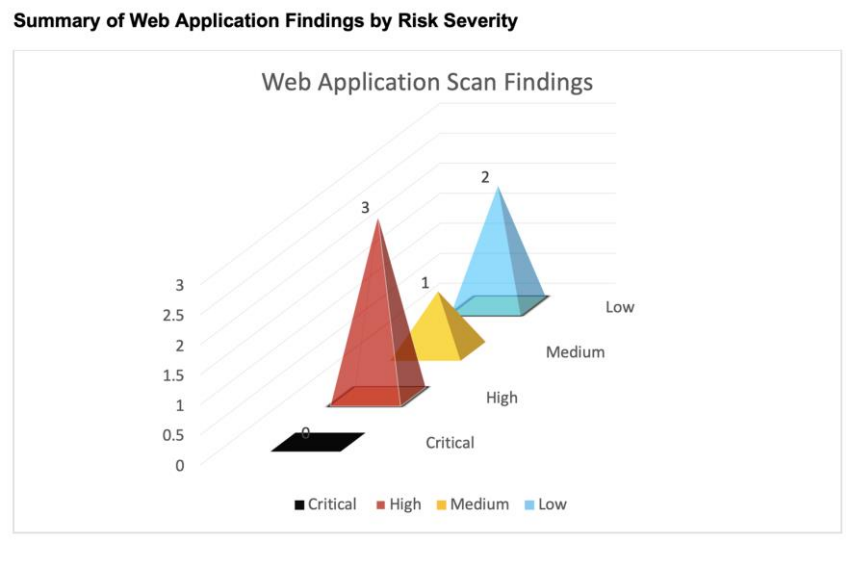
Listed are all the components

1. External Entity:
    a. Customer
    b. Employee
2. Process:
    a. Webserver
    b. Firewall
    c. SIEM
    d. Domain Controller
    e. WorkStation
3. Data Flow:
    a. Customer ←→ Webserver (through Firewall)
    b. Webserver ←→ Mysql database
    c. Employee ←→ Domain Controller (though Firewall)
    d. Domain Controller ←→ Workstation
    e. Workstation ←→ Webserver
    f. Webserver → SIEM
    g. Mysql database → SIEM
    h. Domain Controller → SIEM
    i. Firewall → SIEM
4. Data Store:
    a. Mysql Database

ENTITY	THREAT	ATTACKS	MITIGATION
EXTERNAL ENTITY			
Customer	S, R	1. Enact as another customer 2. Perform MITM to get user credentials 3. Phishing to get user credentials	Users use credentials and security question
Employee	S, R	1. Enact as another employee 2. Perform MITM to get credentials 3. Phishing to get credential	Employee use VPN which is to log into the DC using credentials
PROCESS			
Webserver	S, T, R, I, D, E	1. Someone can act as a webserver and access web server 2. Webserver can claim it did not fulfill the request 3. Overwhelming requests can make the webserver unavailable 4. The web server can be tweaked and changed	1. Webserver has a static IP 2. Logs from the server is sent to SIEM 3. There is a firewall which prevents DOS
Firewall	S, T, R, I, D, E	1. Someone can act as a firewall 2. Firewall can claim it did not fulfill the request 3. Overwhelming requests can bring down the firewall 4. The firewall rules can be tweaked and changed	1. Logs from firewall are being sent to SIEM 2. Firewall rules are sent and can be changed only if employee has access to azure instance
SIEM	S, T, R, I, D, E	1. Someone can act as a SIEM and collect all the logs 2. Overwhelming requests can make the webserver unavailable 3. The SIEM can be tweaked and changed	1. SIEM communicates with all the services using keys which are generated by Azure 2. These keys autorotate 3. SIEM access is limited to special employee who hace access
			to azure instance
Domain Controller	S, T, R, I, D, E	1. Someone can act as a Domain Controller and access Jump box 2. Domain Controller can claim it did not push a policy or access the box 3. Overwhelming requests can make the webserver unavailable 4. The Domain Controller can be tweaked and changed	1. Logs are sent to SIEM 2. DC can only be accessed over VPN using RDP by selected employee
Workstation	S, T, R, I, D, E	1. Someone can act as a workstation and access server 2. Workstation can claim it did not fulfill the request 3. The workstation can be tweaked and changed	1. Logs are sent to SIEM 2. SSH keys is needed to access webserver
DATA STORE			
Mysql Database	T, R, I, D	1. Someone can access the data from database 2. Database can claim it did not fulfill the request 3. Overwhelming requests can make it unavailable 4. The Database can be tweaked and changed	1. The database itself is encrypted 2. Logs are sent to SIEM 3. Database can only be accessed by webserver from specific IP
DATA FLOW			
Customer←→Webserver	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
Webserver ←→ Mysql	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
Employee ←→ DC	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
DC ←→ Workstation	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
Workstation←→Webserver	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
Webserver → SIEM	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used
Mysql → SIEM	T, I	An attacker can intercept the data flow, read and modify the data	TLS is being used

Web App Scan

The Pentesting team performed 3 tests and the report was generated. Some of the Vulnerabilities were patched



3 rounds of Pentest

- March 11
- March 16
- March 22

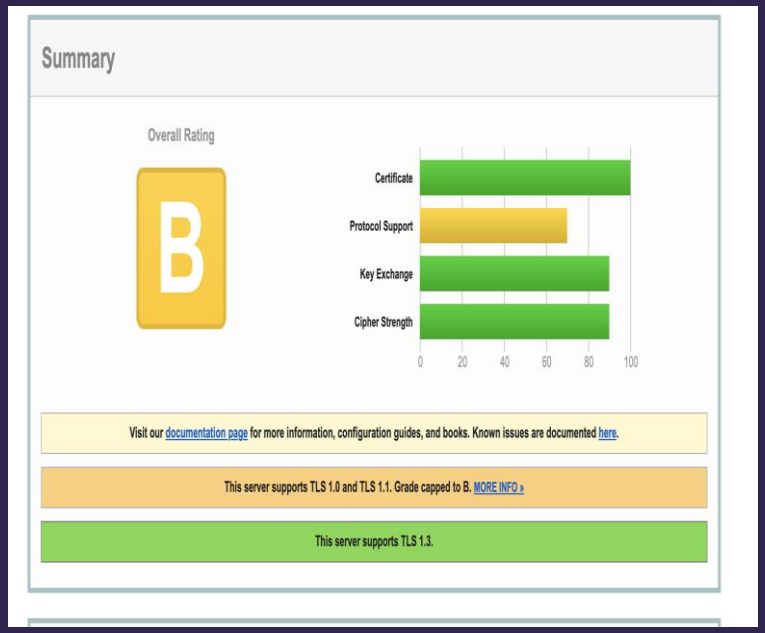
The Vulnerabilities that were patched

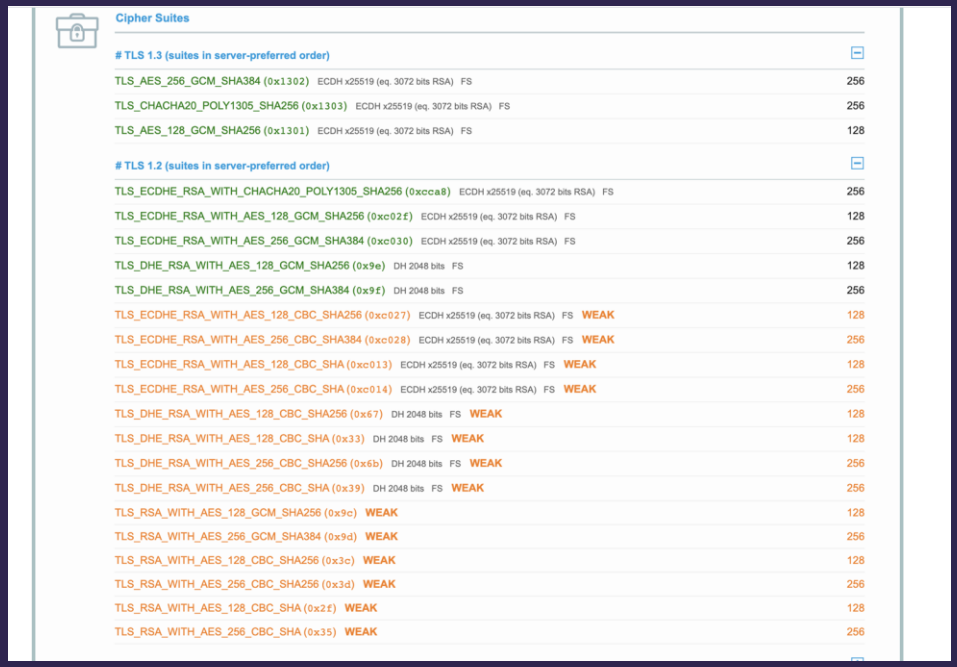
- Clear Text submission of password
- Cross Site scripting
- Unencrypted communication

Vulnerability still present due to limited resources and time

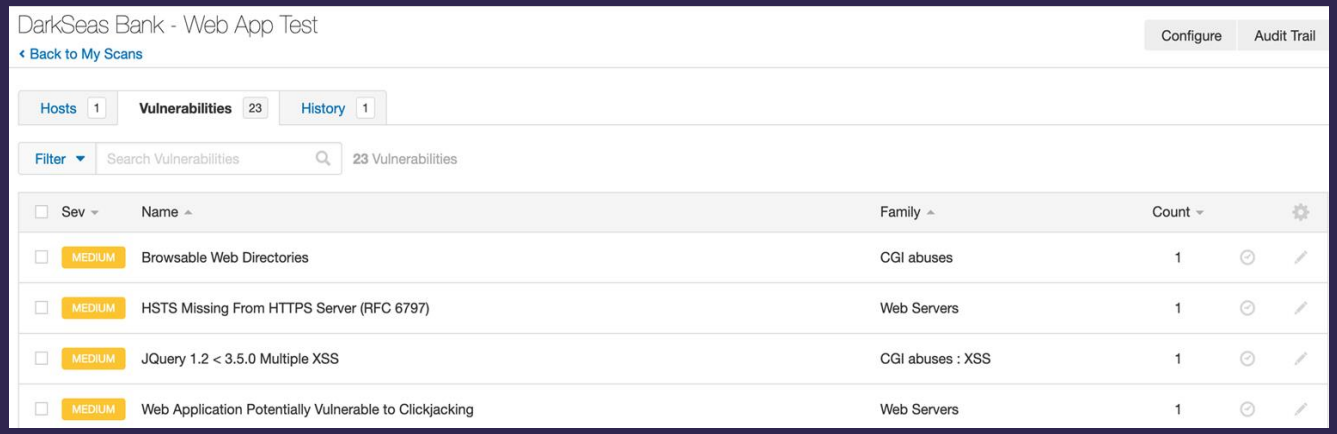
- TLS cookie without secure flag
- Clickjacking
- DOM based Link Manipulation
- Vulnerable javascript and bootstrap versions
- HSTS not set
- Cross site Request Forgery

SSL Lab


Summary
Overall Rating
B
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »
This server supports TLS 1.3.


Cipher Suites
TLS 1.3 (suites in server-preferred order)
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS 128
TLS 1.2 (suites in server-preferred order)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS 128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 2048 bits FS 128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK 256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 2048 bits FS WEAK 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 2048 bits FS WEAK 128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS WEAK 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS WEAK 256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK 128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK 256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK 128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK 256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK 128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK 256

Nessus




```
The following directories are browsable :

https://www.darkseasbank.com/css/
https://www.darkseasbank.com/download/
https://www.darkseasbank.com/embrace/
https://www.darkseasbank.com/embrace/Mailer/
https://www.darkseasbank.com/embrace/Mailer/language/
https://www.darkseasbank.com/embrace/Mailer/src/
https://www.darkseasbank.com/img/
https://www.darkseasbank.com/js/
```

Browsable Web Directories
Information Disclosure

Nmap

```
Nmap scan report for 52.191.161.183
Host is up (0.054s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:3e:17:cd:23:55:65:fc:bd:28:64:32:d1:26:02:a8 (RSA)
|   256 0a:b7:02:7f:a0:e8:f6:b7:24:9d:9f:56:1a:95:98:70 (ECDSA)
|_  256 82:1c:ae:14:c3:0e:ba:2e:5c:fa:60:28:cd:d6:4f:86 (ED25519)
80/tcp   open   http     Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Did not follow redirect to https://www.darkseasbank.com/
443/tcp  open   ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: DarkSeas Bank
| ssl-cert: Subject: commonName=www.darkseasbank.com
| Subject Alternative Name: DNS:www.darkseasbank.com
| Not valid before: 2021-03-11T23:55:42
|_Not valid after:  2021-06-09T23:55:42
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
465/tcp  closed smtps
3306/tcp closed mysql
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X (86%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:4.2 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:wat
chguard:fireware:11.8 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Linux 2.6.32 (86%), Linux 2.6.32 or 3.10 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%), Linux 3.5 (86%), Linux 4.2 (86%), Linux 4.4 (86%), Synology Di
skStation Manager 5.1 (86%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 23 hops
Service Info: Host: www.darkseasbank.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

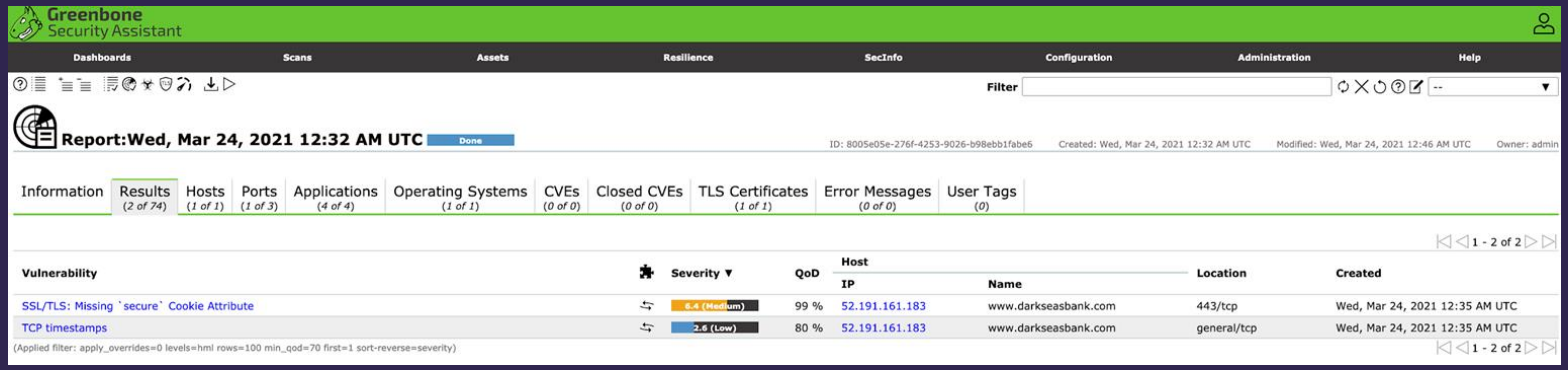
Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.191.161.183
+ Target Hostname:    www.darkseasbank.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.darkseasbank.com
                   Altnames: www.darkseasbank.com
                   Ciphers:  ECDHE-RSA-CHACHA20-POLY1305
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2021-03-23 17:48:42 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the secure flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alterna
tives for 'index' were found: index.bak
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-3268: /download/: Directory indexing found.
+ OSVDB-3092: /download/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7517 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2021-03-23 18:18:46 (GMT-7) (1804 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto Top Vulnerabilities

1) Traversal or web directories (/download, /img, /Mailer, /js)
   a) https://www.darkseasbank.com/js/pwdStr.js (zxcvbn.js library)
2) PHPSESSID token set without “Secure” attribute
3) CSRF Token not set

OpenVAS



The host is running a server with SSL/TLS and is prone to information disclosure vulnerability.

Detection Result

The cookies:
Set-Cookie: PHPSESSID=***replaced***; path=/; HttpOnly
are missing the "secure" attribute.

Insight

The flaw is due to cookie is not using 'secure' attribute, which allows cookie to be passed to the server by the client over non-secure channels (http) and allows attacker to conduct session hijacking attacks.

Solution Type:
Mitigation
Set the 'secure' attribute for any cookies that are sent over a SSL/TLS connection.

Residual Risk

- One subnet
- No Anti Virus (it was costly)
- The file server is on the web server
- Separate gateway
- Not enough resources to fix webapp vulns
- Not enough CPU cycle to make a different auth server
- Malware checker not available

Group 2

- Shared Screen from word document of final report.

DSci526:
Secure Systems Administration

Second Group Project
Initial Discussion

Prof. Clifford Neuman

Lecture 10
24 March 2021
Online

Teams for Second Group Project

- Team One
  - Shagun Bhatia
  - Anthony Cassar
  - Sarahzin Chowdhury
  - Tejas Kumar Pandey
  - Pratyush Prakhar
  - Christopher Samayoa
  - Louis Uuh
  - Ayush Ambastha
  - Jason Ghetian
  - Abhishek Tatti
  - MaryLiza Walker
  - Hanzhou Zhang
- Team Two
  - Azzam Alsaeed
  - Marco Gomez
  - Alejandro Najera
  - Doug Platt
  - Carol Varkey
  - Yang Xue
  - Aditya Goindi
  - Malavika Prabhakar
  - Dwayne Robinson
  - Amarbir Singh
  - Shanice Williams

Teams

- You already enumerated data and users and suggested a containment architecture.
- There are 11 or 12 members per team
- Teams until end of semester to complete project
- Teams should decide on sub-groups
  - Based on skill sets
  - 2 or 3 members per sub-group
  - These members will focus on different aspects of deployment.

In your Breakout Groups

- Decide on a team name
- Decide on Tasks for sub-groups, I'd suggest:
  - Platform administration (including configuration management)
  - Network administration and deployment
  - Firewall / VPN administration and deployment
  - Server Development and deployment (web server)
  - Server Development and deployment (back-end, database)
  - Intrusion Detection/SIEM
  - Red Teaming and Penetration Testing
- Share (by email) last weeks assignment
- Discuss (by email) combined architecture
- A spokesperson (different each week) will report for 10 minutes to the entire class on your progress each week (starting next week)
  - All can chip into the discussion, but the spokesperson will lead it.
  - Teams will provide a progress update, but will likely withhold some information if it provides an advantage.
- Today try to organize into roles in terms of who will do what for development and deployment.
  - With 11 or 12 members, there should be 2 or 3 team members in each role (i.e. you will have sub-teams)

Group Exercise One

- Decide on the software components to be deployed to implement software requirements on next slide.
  - Custom development should be simple scripts.
  - Use packages for database and other components.
- Decide on the VM's to be created to run those software components.
  - You can run more than one software component within a VM if you choose.
  - Decide on the methods you will use to contain access to those software components, and to the information managed by those components.
- Configure communication between VM's and to the outside
- Install packages
- Write scripts and demonstrate basic flow through system.
- Report on progress as group before class on March 31st.

Second Exercise - Criminal Enterprises

- Chosen because of differences in the high-level principles.
  - Not because I expect you to implement these kinds of systems in your future endeavors.
  - But you may be called upon to break some of these systems if later employed by government organizations.
- Your organization must:
  - Accept Bitcoin as payment (not really, but it must accept something that stands in for bitcoin)
  - Manage an inventory of stolen account identifiers with passwords
    - Enable the sale of collection of such information in exchange for your stand-in for bitcoin
    - Control access to such information
  - Prevent collection of evidence or intelligence by third parties.
  - Note, do not deal in any illegal goods, but use dummy information to stand in for such goods. Also, do not use terms associated with such illegal goods or information in communications, make up new names for this dummy information.