

# DSci526: Secure Systems Administration

## **Mid-Semester Change of Gears**

Prof. Clifford Neuman

**Lecture 10** 25 March 2021 Online



University of Southern California



- 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

- 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.



- 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.



| (kati@ nohara) - [~]<br>\$ wapiti -u https://www.   | x,darkceasbank.com/   |  |   |
|---|---|--|---|
| Wapiti-3.0.4 (wapiti.souro<br>[*] Saving scan state, ple  | >>          // \<br>_/  _     _/ /<br>_l // treeforge.io)<br>lesse wait   |  |   |
| Note 🍙  |   |  |   |
| This scan has been saved i<br>[*] Wapiti found 14 URLs a<br>[*] Loading modules:<br>backup, blindsql,<br>Problem with local wapp de<br>Downloading from the web.  | in the file /home/kali/ sapitl/scans/www.darkseasbank.com_folder_156+00<br>and forms during the scan<br>1, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, b<br>database.   | <pre>#3.db taccess, http_headers, methods, nikto, permanentxss, re</pre> | direct, shellshock, sql, ssrf, wapp, xss, xxe |
| [*] Launching module csp<br>CSP is not set  |   |  |   |
| [*] Launching module http<br>Checking X-Frame-Options :<br>X-Frame-Options :<br>Checking X-XSS-Protection<br>X-XSS-Protection is not set<br>Checking X-content-Type-Options is<br>Checking Structure Type-Options is<br>Checking Struct Type-Options is<br>Checking Struct Transport<br>Struct-Transport-Security | by Johanders<br>et<br>by the second second<br>Second second second<br>Second second second<br>Second second second<br>Second second |  |   |

#### 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

| ⊑s =                                    |  |            |        |    |  |
|---|--|------------|--------|----|--|
|   |  |            |        |    |  |
| • · · · · · · · · · · · · · · · · · · · | -[ metasploit vo.0.33:dev ]<br>-[ 2102 exploits - 1134 auxiliary - 357 post ]<br>[ 52 payloads - 45 encoders - 10 mops ]<br>[ 8 evasion ]  |            |        |    |  |
| Metas<br>tips                           | ploit tip: View all productivity tips with the<br>command  |            |        |    |  |
| msf6                                    | > search apache  |            |        |    |  |
| Match                                   | ing Modules  |            |        |    |  |
|   | Name   |            |        |    |  |
|   | auviliaru/admin/annlatu/annlatu/diralau video  |            | normal | Ma | Apple Ti Video Perete Control  |
| 1                                       | auxiliary/admin/http/toprat_administration   |            | normal | No | Tomcat Administration Tool Default Access                              |
| 2                                       | auxiliary/admin/http/tomcat_ghostcat   | 2020-02-20 | normal | No | Ghostcat   |
| 3                                       | auxiliary/admin/http/tomcat_utf8_traversal   | 2009-01-09 | normal |    | Tomcat UTF-8 Directory Traversal Vulnerability                         |
| 4                                       | auxiliary/admin/http/trendmicro_dlp_traversal  | 2009-01-09 | normal |    | TrendMicro Data Loss Prevention 5.5 Directory Traversal                |
| 5                                       | auxiliary/dos/http/apache_commons_fileupload_dos   | 2014-02-05 | normal |    | Apache Conmons FileUpload and Apache Tomcat DoS                        |
| 6                                       | auxiliary/dos/http/apache_mod_isapi  | 2010-03-05 | normal | No | Apache mod_isapi Dangling Pointer                                      |
| 7                                       | auxiliary/dos/http/apache_range_dos  | 2011-08-19 | normal | No | Apache Range Header DoS (Apache Killer)                                |
| 8                                       | auxiliary/dos/http/apache toncat_transfer_encoding   | 2010-07-09 | normal | No | Apache Toncat Transfer-Encoding Information Disclosure and Dos         |
| 10                                      | auxiliary/fileformat/out_badddt  | 2018-05-01 | normat | NO | Cibredifice 6.63 /Apache Openoffice 4.1.5 Haticious our file Generator |
| 11                                      | auxiliary/gather/impersonate ssl   |            | normal | No | HTTP SSL Certificate Impersonation                                     |
| 12                                      | auxiliary/gather/zookeeper info disclosure   | 2020-10-14 | normal | No | Anache ZooKeeper Information Disclosure                                |
| 13                                      | auxiliary/scanner/couchdb/couchdb enum   |            | normal |    | CouchDB Enum Utility   |
| 14                                      | auxiliary/scanner/http/apache activeng source_disclosure   |            | normal |    | Apache ActiveMQ JSP Files Source Disclosure                            |
| 15                                      | auxiliary/scanner/http/apache activeng traversal   |            | normal |    | Apache ActiveMQ Directory Traversal                                    |
| 16                                      | auxiliary/scanner/http/apache_flink_jobmanager_traversal   | 2021-01-05 |        |    | Apache Flink JobManager Traversal                                      |
| 17                                      | auxiliary/scanner/http/apache_mod_cgi_bash_env   | 2014-09-24 |        |    | Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanne |
| r                                       | and i any technology (http://www.line.chin | 1017 00 18 |        |    | Total Ontion bland Frances   |
| 10                                      | auxiliary/scamer/http/apacha userdir enum  | 2017-09-18 | normal | Mo | Inache "mod userdic" User Councertion                                  |
| 20                                      | auviliary/scanner/http/avis local file include   |            | normal | Mo | touche Avis2 v1 4.1 tocal Eile Inclusion                               |
| 21                                      | auxiliary/scanner/http/axis_lonin  |            | porgal | No | Anarhe Axis2 Brute Force Utility                                       |
| 22                                      | auxiliary/scanner/http/mod_negotiation_brute   |            | normal | No | Anarha HTTPD and negotiation Filename Bruter                           |

#### 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.



| Details Logs Commands   |
|---|
| Module Tree   |
| Comparison (1)     Comparis |



## **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.

| ******<br>* Wfuzz<br>* Codec<br>* Chris<br>* Xavic<br>* Xavic<br>* Carlo     | z 2.0 – Th<br>d by:<br>stian Marto<br>er Mendez a<br>os del ojo      | +++++++++<br>e Web Bru<br>rella (cm<br>ka Javi (<br>(deepbit@<br>++++++++ | *************<br>teforcer<br>artorella@edg<br>xmendez@edge-<br>igmail.com)<br>******** | **************<br>e-security.com<br>security.com)<br>*****                   | ***<br>*<br>) *<br>*<br>*<br>*   |  |
|--|--|---|--|--|--|--|
| Target:<br>Payload   | <pre>http://lo d type: fil</pre>                                     | calhost:8<br>e,wordlis  | 888/MAMP/FUZZ<br>t/general/com   | mon.txt  |  | Tyler [-/tools/wordlists] → hydra -l admin -P <u>1000 common_passwords.txt</u> -s 8090 -f 192.168.1.4 http-get /get_camera_params.cgi<br>Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes. |
| Total  | Total requests: 950  |   |  |  |  | Hydra (http://www.thc.org/thc-hydra) starting at 2016-05-02 23:25:40<br>[DATA] max 16 tasks per 1 server, overall 64 tasks, 1000 login tries (1:1/0:1000), ~0 tries per task   |
| ID   | Response   | Lines   | Word   | Chars  | Server   | [DATA] attacking service http-get on port 8090<br>[8090][http-get] host: 192.168.1.4 login: admin password: passw0rd   |
| 00244:<br>00324:<br>00440:<br>00430:<br>00470:<br>00620:<br>00628:<br>00783: | C=301<br>C=301<br>C=301<br>C=301<br>C=301<br>C=301<br>C=302<br>C=301 | 9 L<br>9 L<br>9 L<br>9 L<br>9 L<br>9 L<br>9 L<br>9 L                      | 30 W<br>30 W<br>37 W<br>30 W<br>30 W<br>30 W<br>30 W<br>30 W                           | 330 Ch<br>334 Ch<br>586 Ch<br>333 Ch<br>329 Ch<br>330 Ch<br>330 Ch<br>334 Ch | Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un<br>Apache/2.0.63 (Un | [STATUS] attack finished for 192.168.1.4 (valid pair found)<br>1 of 1 target successfully completed, 1 valid password found<br>Hydra (http://www.thc.org/thc-hydra) finished at 2016-05-02 23:25:48  |

- 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<mark>.4.8</mark>

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



University of Southern California
#### 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.





- 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



University of Southern California

# 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).
  - À 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





- 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).

| Search (Ctrl+/) *                           | + Add 🛓        | Download role assignments 💠 Edit columns 🕐 Refresh 📋 🗦                               | Remove Got feedback?                                 |
|---|----------------|--|--|
| † Overview                                  | A.             |  |  |
| Activity log                                | Check access   | Role assignments Roles Deny assignments Classic a                                    | oministrators  |
| Access control (IAM)                        | Classic admini | strators are only needed if you are still using Azure classic deployments            | We recommend using role assignments for all other pu |
| 🔷 Tags                                      |                |  |  |
| Diagnose and solve problems                 | Name ①         | ime or email   |  |
| Security                                    | Name           | 1  | Role   |
| 🗲 Events                                    |                | Shagun Bhatia (Guest)  | Co-administrator                                     |
| Cost Management                             |                | shagunbh@usc.edu<br>Sarahgin Shane (Guest)   | A charlenges   |
| <ol> <li>Cost analysis</li> </ol>           |                | sarahzic@usc.edu   | Co-administrator                                     |
| Cost alerts                                 | •              | Malavika Prabhakar (Guest)<br>malavika@usc.edu                                       | Co-administrator                                     |
| Budgets                                     |                | Christopher Shane<br>chrisshanee22 gmail.com#EXT#@chrisshanee22gmail.onmicrosoft.co. | Co-administrator                                     |
| <ul> <li>Advisor recommendations</li> </ul> |                | Amarbir Singh (Guest)<br>amarbirs@usc.edu  | Co-administrator                                     |
| Billing                                     |                | Shanice Williams (Guest)<br>shanicew@usc.edu   | Co-administrator                                     |
| Settings                                    |                | Christopher Samayoa (Guest)<br>csamayoa@usc.edu                                      | Co-administrator                                     |
| Programmatic deployment                     |                | Anthony Cassar (Guest)<br>acassar@usc.edu  | Co-administrator                                     |
| Billing properties                          |                | Pratyush Prakhar (Guest)   | Co-administrator                                     |
| Resource groups                             |                | Tejas Radey (Guest)<br>to ander Start and  | Co-administrator                                     |
| Preview features                            |                | Pratyush Prakhar (Guest)   | Co-administrator                                     |
| Usage + quotas                              |                | pratyushp010@gmail.com   |  |
| D. Ballalar                                 |                | dwaynero@usc.edu   | Co-administrator                                     |

| Microsoft Azure |
|-----------------|
|                 |

| Microsoft Azure                                 | ① Upgrade                  | ₽ Search         | resources, se  | ervices, and docs (G+/)          |             |                 |                              |                     | 2 <b>G</b> | •• ©       |              | Chrisshanee22@gm<br>DEFAULT D |         |
|---|----------------------------|------------------|----------------|----------------------------------|-------------|-----------------|------------------------------|---------------------|------------|------------|--------------|-------------------------------|---------|
| ne > Default Directory >                        |                            |                  |                |                                  |             |                 |                              |                     |            |            |              |                               |         |
| Users   All use<br>Default Directory - Azure Ac | rs (Prev<br>tive Directory | iew) …           |                |                                  |             |                 |                              |                     |            |            |              |                               | ×       |
|   | ~                          | + New user + 1   | New guest us   | er 🗋 Bulk operations 🗸           | 🕐 Refrest   | PReset password | 🛃 Multi-Factor Authenticatio | n 🗐 Delete user     | EE Col     | umns 🛛 🕕   | Preview infi | D Preview feature             | res ··· |
| All users (Preview)                             |                            |                  |                | - 1.4.1. <i>K</i>                |             |                 |                              |                     |            |            |              |                               |         |
| Deleted users (Preview)                         |                            | This page includ | is previews av | anable for your evaluation, view | previews -+ |                 |                              |                     |            |            |              |                               |         |
| Password reset                                  |                            | P Search users   |                | ty Add                           | ilters      |                 |                              |                     |            |            |              |                               |         |
| User settings                                   |                            | 15 users found   |                |                                  |             |                 |                              |                     |            |            |              |                               |         |
| Diagnose and solve problem                      | is                         | Name             | τu             | User principal name              | ↑↓ User ty  | pe              | Directory synced             | Identity issuer     |            | Company na | ne           | Creation type                 |         |
| vity  |                            | Amarbir !        | Singh          | amarbirs_usc.edu#EXT#@           | ch Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
| Sign-ins  |                            | Anthony          | Cassar         | acassar_usc.edu#EXT#@cl          | ri Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
| Audit logs                                      |                            | 🗌 📧 ben          |                | bcn_isi.edu#EXT#@chrissh         | a Guest     |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
| Bulk operation results                          |                            | Christoph        | ner Samayoa    | csamayoa_usc.edu#EXT#@           | c Guest     |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
| bleshooting + Support                           |                            | Christoph        | ter Shane      | chrisshanee22_gmail.com          | E Memb      | er              | No                           | chrisshanee22gmail/ | onmicrosc  |            |              |                               |         |
| New support request                             |                            | 🗌 😡 dwayne       |                | dwayne_dwaynerobinson.           | :o Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | Dr Dwayne I      | Robinson       | dwaynero_usc.edu#EXT#@           | c Guest     |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | 🗌 M Malavika     | Prabhakar      | malavika_usc.edu#EXT#@           | ch Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | PP Pratyush      | Prakhar        | pratyushp010_gmail.com#          | E Guest     |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | PP Pratyush      | Prakhar        | prakhar_usc.edu#EXT#@c           | hri Guest   |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | Sarahzin         | Shane          | sarahzic_usc.edu#EXT#@c          | hr Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | SB Shagun E      | Ihatia         | shagunbh_usc.edu#EXT#@           | c Guest     |                 | No                           | chrisshanee22gmail. | onmicrosc  |            |              | Invitation                    |         |
|   |                            | Shanice V        | Nilliams       | shanicew_usc.edu#EXT#@           | ch Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | TP Tejas Pan     | dey            | tpandey_usc.edu#EXT#@o           | hr Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | uuh 🔲            |                | uuh_usc.edu#EXT#@chris           | ih Guest    |                 | No                           | chrisshanee22gmail/ | onmicrosc  |            |              | Invitation                    |         |
|   |                            | -                |                |                                  |             |                 |                              |                     |            |            |              |                               |         |

### **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

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

Non-administrative group (no SSH access) for website management

#### 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       | MACHINE NAME: DS-Web01-         | MACHINE NAME: Dark-WK-01    |
|-----------------------------|---------------------------------|-----------------------------|
| PUBLIC IP: N/A              | Ubuntu                          | PUBLIC IP: N/A              |
| PRIVATE IP: 10.0.2.7        | PUBLIC IP: 52.191.161.183       | PRIVATE IP: 10.0.2.8        |
| OPEN PORTS: none externally | PRIVATE IP: 10.0.2.4            | OPEN PORTS: none externally |
|                             | OPEN PORTS: 80, 3306, 465, 587, |                             |
|                             | 443                             |                             |

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.

| Home > Azure Sentinel ><br>Azure Sentinel   Over<br>Selected workspace: Sentinelawdarkses<br>Selected workspace: Sentinelawdarkses<br>Selected workspace: Sentinelawdarkses<br>() Search (Ctrl+/) « | erview ····<br>≈<br>◯ Refresh ③ Last 24 hours ✓   |                                       |   |   | Home > Security Center > Secure Score Dashboard<br>Recommendations …<br>Showing subscription Airea walkorption 1'<br>↓ Download CSV report ♥ Guides & Feedback  | D   |   |  |   |  | ×                       |
|---|---|---------------------------------------|---|---|---|---|---|--|---|--|-------------------------|
| General Coverview Coys Cops Cops Cops Cops Cops Cops Cops Cop   | Age     Control     Contro     Control     Control     Control     Control     Contro | 776 2776                              | Notem by same<br>Else (c) Acres (b) Courd (for Reine (c) Courd<br>Alerts Alerts 7<br>, scorerreint<br>scorerreint<br>248.8K | d Ader Answer (a)      Recent Incidents      Median System security access was goated a- 1/2      Median Acure Resource was destroyed 1/2      Madum Acure Alema Maticious Modification 1/2 | Secure Score  | Recommendations status           (=)         6 completed controls         1           View         16 completed recommendations         2               | Resource health                         | Converting<br>4<br>Treathy<br>1<br>Tre explosite<br>5                                | Azure Security Benchmark  | mark is now the default policy<br>unity Center. The benchmark is th<br>y Center's recommendations. | he >                    |
| Notebooks     Entity behavior     Threat intelligence (Preview) Configuration     Data connectors     Analytics   | 14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00<br>14.00   |                                       | очков<br>36.8К<br>14.4К<br>спекта за<br>4.1К  | Medium Frield S91 logon detected 1 / 1<br>Medium Windows VML Login Falure 1 / 1<br>Data source anomalies  | Is the Secure Score experience clear to you?      Each security control before represents a security risk activity in the security restriction of the securety restriction of the security restriction of the security restre | Ves No you should mitigate. ing on the controls worth the most points. resources in a control. Learn more > us : 2 Selected Recommendation status : 2 S | elected Recommendation m                | aturity : All Severity : All   | Reset   | filters Group by con   | ×<br>ntrols: <b>O</b> n |
| Watchlist (Preview)     Autonation     Community     Settings   | ter 23  | 0.34 U.M                              | POTIDITIAL<br>MALCOOS<br>EVENTS<br>O  | Usage   | Resource type     Controls     Secure management ports     Remediate vulnerabilities  | e : All Response actions : All Contain<br>Max score<br>10<br>8<br>6   | Current Score                           | ent : All Potential score increase + 0% (0 points) + 15% (8 points) + 12% (6 points) | Unhealthy resources<br>None<br>3 of 3 resources<br>3 of 3 resources | Sort by max  | score V                 |
|   |   | · · · · · · · · · · · · · · · · · · · | ONORTUO   | Democratize MI for your SecOns  | Apply system updates     Manage access and permissions  | 6 4   | 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | + 0% (0 points)<br>+ 8% (4 points)   | None<br>1 of 1 resources  |  |                         |

|   | de 🖉 🔎 Searci  | h resources, services, and docs (G+/)                               |                            |                            | D 🖟 🤌 🍥           | ? 😳 malavika@u<br>DEFAULT DI | ISC.edu 🔕 |  |  |
|---|--|---|----------------------------|----------------------------|-------------------|------------------------------|-----------|--|--|
| Home > Azure Sentinel > Azure Sentinel<br>Azure Sentinel   Ana<br>Selected workspace: 'sentinellawdarksea | Azure Sentinel > Azure Sentinel         Azure Sentinel   Analytics         Selected workspace: 'sentinellawdarkseas' |   |                            |                            |                   |                              |           |  |  |
|   | + Create 🗸 💍 Refi  | resh 🔀 Analytics efficiency workbook (Preview) 🛛 🖞 Enable 🚫         | Disable 📋 Delete           |                            |                   |                              |           |  |  |
| Overview  | 📥 20   | Rules by severity   |                            |                            |                   | LEARN MORE                   |           |  |  |
| 🧬 Logs  | Active rules   | High (6) Medium (10) Low (4) Informational (0)                      |                            |                            |                   | About analytics rul          | es 🖸      |  |  |
| 🜰 News & guides   |  |   |                            |                            |                   |                              | ~         |  |  |
| Threat management   | Active rules Rule to   | emplates  |                            |                            |                   |                              |           |  |  |
| Incidents   | ₽ Search   | Severity : All Rule Type : All                                      | Status : All Tactics : All |                            |                   |                              |           |  |  |
| 🞽 Workbooks   |  |   |                            |                            |                   |                              |           |  |  |
| Hunting   | SEVERITY ↑↓  | NAME 1  | RULE TYPE 1                | STATUS ↑↓                  | TACTICS           | LAST MODIFIED ↑↓             |           |  |  |
| Notebooks   | High   | Special privileges assignment to new logins or object modifications | () Scheduled               | C Enabled                  | 🧚 🗘 🕐 🏬 +2 🛈      | 03/23/21, 12:42 PM           | ···· •    |  |  |
| 🥜 Entity behavior   | High   | Firewall Rule Was Deleted   | (Scheduled                 | Enabled                    |                   | 03/23/21, 12:42 PM           |           |  |  |
| O Threat intelligence (Preview)   | High   | The event logging service has shut down                             | Scheduled                  | 🕛 Enabled                  |                   | 03/23/21, 12:42 PM           |           |  |  |
| Configuration   | Medium   | Windows VMs Login Failure   | Scheduled                  | 🕛 Enabled                  | 2 00              | 03/23/21, 12:42 PM           |           |  |  |
|   | Medium   | Failed SSH logon detected   | Scheduled                  | 🕛 Enabled                  | » ()              | 03/23/21, 12:43 PM           |           |  |  |
| Data connectors   | Medium   | Azure Alerts Malicious Modification                                 | Scheduled                  | 🕛 Enabled                  | 📄 💲 🧐             | 03/23/21, 12:43 PM           | •••       |  |  |
| <ul> <li>Analytics</li> </ul>   | Medium   | Azure Resource was destroyed  | Scheduled                  | 🕛 Enabled                  | * Defense Evasion | 03/23/21, 12:43 PM           |           |  |  |
| Watchlist (Preview)   | Medium   | System security access was granted or revoked to an account.        | Scheduled                  | 🕛 Enabled                  |                   | 03/23/21, 12:43 PM           |           |  |  |
| 4 Automation  | <b>—</b>   |   | @ e+ +++                   | $\bigcirc$ $\sim$ $\cdots$ | ** **             | 00.01.01.07.00 MI            | *         |  |  |
| Community   | < Previous 1 - 2   | 0 Next >  |                            |                            |                   |                              |           |  |  |
| 🔅 Settings 🗸 🗸  |  |   |                            |                            |                   |                              |           |  |  |
| 4   |  |   |                            |                            |                   |                              | •         |  |  |

# **Sentinel Logic Example:**

#### Home > Azure Sentinel > Azure Sentinel >

| Analytics rule wiz                                   | zard - Edit existing rule  | Logs 🖈 …<br>SentinelUWDarksess  |
|--|--|---|
| Validation passed.                                   |  | New Query 1* * + 🛇 Feedback 😰 Queries   |
| Name<br>Description<br>Tactics<br>Severity<br>Status | Firewall Rule Was Deleted<br>Firewall Rule Was Deleted with the status of success or accepted<br>High<br>🕐 Enabled   | SentinelLAWDarkseas       ▶ Run       Time range: Set in query  |
| Analytics rule settings                              |  |   |
| Rule query   | //setting up an alert for every time a firewall rule is deleted<br>AzureActivity<br>  where OperationName == "Delete Firewall Rule" and ActivityStatus in ("Accepted", "Succeeded")<br>  project TimeGenerated, CallerJpAddress, ResourceGroup, ResourceId<br>  where TimeGenerated > ago(1d) //shows logs from the past day | Results       Chart       Columns       Red bookmark       Display time (UTC-07:00)       Group columns         Completed       TimeGenerated (Local Time)       CalleripAddress       ResourceGroup       ResourceId       V |
| Rule frequency                                       | Run query every 5 hours  | 3 3/17/2021, 51915.627 PM csamayoa@usc.edu 47.149.196.233 Darkseas, Firewall, ResoureGroup /subscriptions/e49db4c1-13b7-4571-aaf5-f994d66f766/resourcegro   |
| Rule period  | Last 1 day data  | 3 3/17/2021, 5:19:31.280 PM csamayoa@usc.edu Darkseas_Firewall_ResourceGroup /subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegro  |
| Rule threshold                                       | Trigger alert if query returns more than 0 results   |   |
| Event grouping                                       | Group all events into a single alert   |   |

# **Sentinel Logic Example:**

#### Home > Azure Sentinel >

| Analytics rule wizard<br>Failed SSH logon detected | - Edit existing rule  | Logs ☆ …<br>SentineILAWDarkseas                 | ×   |
|--|---|---|---|
| ✓ Validation passed.                               |   | 🧬 New Query 1* 🛛 × 🕂                            | ♡ Feedback 😂 Queries 🕞 Query explorer 🛛 🚳 🛄 ∽   |
| Conservation Contraction Interior Interior         | attions (Dention) Automated assesses Dention and easts  | P SentinelLAWDarkseas                           | 🕨 Run 🛛 Time range : Last 7 days 🌒 🛛 层 Save 🗸 🖄 Share 🗸 🕂 New alert rule 🗸 🏳 Export 🗸 🚀 Pin to dashboard 🛛 😇 Format query   |
| General Sectrule logic incidentis                  | eungs (Preview) Automated response Review and create  | Tables Queries Filter «                         | <pre>1 // Computers With Failed SSH Logons 2 // Lists computers with Failed SSH Logons. 3 // Lists computers with Failed SSH Logons. 4 Judge (Facility == 'authorize' and SysLogMessage has 'schdrauth' and SysLogMessage has 'authorization failure') on (Facility == 'auth' and ( 4 Judge (Facility == 'authorize') and SysLogMessage has 'schdrauth' and SysLogMessage has 'authorization failure') on (Facility == 'auth' and ( 4 Judge (Facility == 'authorize') and SysLogMessage has 'schdrauth' and SysLogMessage has 'authorization failure') on (Facility == 'auth' and ( 5 Judge (Facility == 'authorize') and ( 5</pre> |
| Analytics rule details                             |   | Search :<br>(▼ Filter) I≣ Group by: Solution ∨  | (SyslogMessage has 'Failed' and SyslogMessage has 'invalid user' and SyslogMessage has 'ssh2') or SyslogMessage has 'error: PAM: Authentication failure'))  |
| Name<br>Description                                | Failed SSH logon detected Failed SSH logon detected in 10 min windows                                   | Collapse all                                    | 5 summarize count() by Computer, HostIP, bin(TimeGenerated, 10m), ProcessID<br>6 where TimeGenerated > ago(14d) //shows logs from the past day  |
| Tactics  | Discovery     PreAttack   | Favorites                                       |   |
| Severity   | Medium  | You can add favorites by clicking on the 🖈 icon | Results Chart 🗓 Columns 🗸 👔 Add bookmark 🕓 Display time (UTC+00:00) 🗸 💿 Group columns   |
| Status   | ◎ Disabled  | Azure Sentinel                                  | Completed. Showing results from the last 7 days.  |
|  |   | ▶ LogManagement                                 | □ TimeGenerated [UTC] ▽ Computer ▽ HostiP ▽ ProcessiD ♡ count_ ♡  |
| Analytics rule settings                            |   | <ul> <li>Functions</li> </ul>                   | 3/23/2021, 150:00.000 PM         DS-Web01-Ubumtu         10.0.2.4         6,438         2   |
| Rule query   | // Computers With Failed SSH Logons   |   | >   |
|  | // Lists computers with failed SSH logons.<br>Svslog  |   | >   |
|  | where (Facility == 'authpriv' and SyslogMessage has 'sshd:auth' and SyslogMessage has 'authentication I |   | > 3/23/2021, 1:50:00.000 PM D5-Web01-Ubuntu 10.0.2.4 6,694 2  |
|  | SyslogMessage has 'ssh2') or SyslogMessage has 'error: PAM: Authentication failure'))                   |   | > 2/32/0011 5-50-00.00M DEL Ilburrhu 10.0.2.4 6.755 2   |
| Previous Save                                      |   |   | I         Page         1         of 214         ► ►I         50         ▼         items per page         1 - 50 of 10660 items  |

Home > Azure Sentinel > Azure Sentinel > Analytics rule wizard - Edit existing rule >

|  |   |  | FILL            |                               |                                   |  | ****<br>**** |                  |
|--|---|--|-----------------|-------------------------------|-----------------------------------|--|--------------|------------------|
| E Microsoft Azure 🕑 Upgrade              | ,   | es, services, and docs (G+/)                                 |                 |                               | Σ                                 | ] 🗣 🗘 🛞                                | ? 🙂 '        | nalavika@usc.edu |
| Home > Azure Sentinel > Azure Sentinel   |   |  |                 |                               |                                   |  |              |                  |
| Azure Sentinel   Inci                    | idents  |  |                 |                               |                                   |  |              | ×                |
| Selected workspace: 'sentinellawdarksea: | is'   |  |                 |                               |                                   |  |              |                  |
| Search (Ctrl+/)     «                    | C Refresh C Last 24 h   | ours 🗸 🧟 Actions 🔝 Security efficiency workbook (Previe      | ew) 😨 Cre       | eate automation rule (Pr      | eview)                            |  |              |                  |
| Overview                                 | <b>a</b> 8  | <b>※8 ₽</b> 0 ≅  | oen incidents b | y severity                    |                                   |  |              |                  |
| P Logs                                   | Open incidents  | New incidents Active incidents                               | ligh (2) Mediur | m (6) Low (0) Informational ( | 0)                                |  |              |                  |
| News & guides                            |   |  |                 |                               |                                   |  |              |                  |
| Threat management                        | Search by id, title, tags, or provide the search by id, tags, or prov | Severity : All Status : New, A                               | Active          | Product name : All            | Owner : All                       |  |              |                  |
|  | <ul> <li>Auto-refresh incide</li> </ul>   | nts  |                 |                               |                                   |  |              |                  |
| Workbooks                                | ↑↓ Incident ID ↑↓   | Title ↑↓   | Alerts          | Product names                 | Created time $\uparrow\downarrow$ | Last update time $~\uparrow\downarrow$ | Owner ↑↓     | Status ↑         |
| Hunting                                  | 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              |
| Notebooks                                | 277   | Azure Resource was destroyed                                 | 1               | Azure Sentinel                | 03/23/21, 12:43 PM                | 03/23/21, 12:43 PM                     | Unassigned   | New              |
| Entity behavior                          | 276   | Azure Alerts Malicious Modification                          | 1               | Azure Sentinel                | 03/23/21, 12:43 PM                | 03/23/21, 12:43 PM                     | Unassigned   | New              |
| Threat intelligence (Preview)            | 275   | Failed SSH logon detected                                    | 1               | Azure Sentinel                | 03/23/21, 12:43 PM                | 03/23/21, 12:43 PM                     | Unassigned   | New              |
| Configuration                            | 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              |
| Data connectors                          | 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              |
| Watchliet (Deaujour)                     | 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              |
| Automation                               | 4   |  |                 |                               |                                   |  |              |                  |
| Community                                | 4   |  |                 |                               |                                   |  |              | ,                |
| Settings                                 | < Previous 1 - 8  | Next >   |                 |                               |                                   |  |              |                  |

#### **Sentinel Logic Example:**

| 🕨 Run 🛛 Time range : Last hour 🛛 🖶 Save 🗸 🖄 Share 🗸 🕂 New alert rule 🗸 $\mapsto$ Export $\checkmark$ $2$ Pin to dashboard $\Rightarrow$ Format query   |                            |           |     |  |  |  |
|--|----------------------------|-----------|-----|--|--|--|
| 1 // Find reports of Windows accounts that failed to login.<br>2 // To create an alert for this query, click '+ New alert rule'<br>3 SecurityEvent   |                            |           |     |  |  |  |
| 4   where EventID == 4625<br>5   summarize logauth = count() by TargetAccount, Computer, _ResourceId   |                            |           |     |  |  |  |
| 6   where logauth >= 5   |                            |           | l i |  |  |  |
|  |                            |           |     |  |  |  |
|  |                            |           |     |  |  |  |
| Results Chart Dimensional Columns Columns (Dimensional Columns Columns) (Columns Columns) (Columns Columns) (Columns) (Columns |                            |           |     |  |  |  |
| Completed. Showing results from the last hour.   |                            |           |     |  |  |  |
| Total CPU O     Age of processed data O     Parallelism O       343 Milliseconds     less than a day     N/A   |                            |           |     |  |  |  |
| Data used for processed query ①         Number of workspaces ①         Request ID           0 KB         1         110df77a-8547-477f-a810-81831259d5a6  |                            |           |     |  |  |  |
| Time span of the processed qu., $\bigcirc$ Number of regions $\bigcirc$  |                            |           |     |  |  |  |
| iess than a day  |                            |           |     |  |  |  |
| TargetAccount 🖓 Computer 🖓 ResourceId  | $\nabla$                   | logauth 🖓 |     |  |  |  |
| V 🗌 Jason1\Administrator DCDARK.Darkseasbank.com /subscriptions/e49db4c1-13b7-4571-aaf5-f994d4df7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compu   | ute/virtualmachines/dcdark | 350       |     |  |  |  |
| TargetAccount Jason1\Administrator   |                            |           |     |  |  |  |
| Computer DCDARK.Darkseasbank.com   |                            |           |     |  |  |  |
| _ResourceId /subscriptions/el9db4c1-13b7-4571-aaf5-f994d4677616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compute/virtualmachines/dcdark   |                            |           |     |  |  |  |
| logauth 350  |                            |           |     |  |  |  |
| JASON1\Administrator DCDARK.Darkseasbank.com /subscriptions/e49db4c1-13b7-4571-aaf5-499d4d6f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compu   | te/virtualmachines/dcdark  | 37        |     |  |  |  |
| > DCDARK.Darkseasbank.com /subscriptions/e49db4c1-13b7-4571-aaf5-f994d46f7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.compu  | ute/virtualmachines/dcdark | 37        |     |  |  |  |
| darkseasbank/cassarADM DCDARK.Darkseasbank.com /subscriptions/e49db4c1-13b7-4571-aaf5-f994d4df7616/resourcegroups/darkseas_firewall_resouregroup/providers/microsoft.computers/micros      | ute/virtualmachines/dcdark | 30        |     |  |  |  |



# **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  $\leftarrow \rightarrow$  Webserver (through Firewall)
  - b. Webserver  $\leftarrow \rightarrow$  Mysql database
  - c. Employee  $\leftarrow \rightarrow$  Domain Controller (though Firewall)
  - d. Domain Controller  $\leftarrow \rightarrow$  Workstation
  - e. Workstation  $\leftarrow \rightarrow$  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             | <ol> <li>Enact as another customer</li> <li>Perform MITM to get user<br/>credentials</li> <li>Phishing to get user credentials</li> </ol>   | Users use<br>credentials and<br>security question  |  |  |
| Employee        | S, R             | <ol> <li>Enact as another employee</li> <li>Perform MITM to get credentials</li> <li>Phishing to get credential</li> </ol>  | Employee use<br>VPN which is to<br>log into the DC<br>using credentials  |  |  |
| PROCESS         |                  |   |  |  |  |
| Webserver       | S, T, R, I, D, E | <ol> <li>Someone can act as a webserver<br/>and access web server</li> <li>Webserver can claim it did not<br/>fulfill the request</li> <li>Overwhelming requests can<br/>make the webserver unavailable</li> <li>The web server can be tweaked<br/>and changed</li> </ol> | <ol> <li>Webserver<br/>has a static IP</li> <li>Logs from the<br/>server is sent<br/>to SIEM</li> <li>There is a<br/>firewall which<br/>prevents DOS</li> </ol>  |  |  |
| Firewall        | S, T, R, I, D, E | <ol> <li>Someone can act as a firewall</li> <li>Firewall can claim it did not fulfill<br/>the request</li> <li>Overwhelming requests can bring<br/>down the firewall</li> <li>The firewall rules can be tweaked<br/>and changed</li> </ol>                                | <ol> <li>Logs from<br/>firewall are<br/>being sent to<br/>SIEM</li> <li>Firewall rules<br/>are sent and<br/>can be<br/>changed only<br/>if employee<br/>has access to<br/>azure instance</li> </ol>  |  |  |
| SIEM            | S, T, R, I, D, E | <ol> <li>Someone can act as a SIEM and<br/>collect all the logs</li> <li>Overwhelming requests can<br/>make the webserver unavailable</li> <li>The SIEM can be tweaked and<br/>changed</li> </ol>   | <ol> <li>SIEM<br/>communicates<br/>with all the<br/>services using<br/>keys which<br/>are generated<br/>by Azure</li> <li>These keys<br/>autorotate</li> <li>SIEM access<br/>is limited to<br/>special<br/>employee who<br/>hace access</li> </ol> |  |  |

| Domain Controller                       | S, T, R, I, D, E | <ol> <li>Someone can act as a Domain<br/>Controller and access Jump box</li> <li>Domain Controller can claim it<br/>did not push a policy or access<br/>the box</li> <li>Overwhelming requests can<br/>make the webserver unavailable</li> <li>The Domain Controller can be<br/>tweaked and changed</li> </ol> | to azure<br>instance<br>1. Logs are sent<br>to SIEM<br>2. DC can only<br>be accessed<br>over VPN<br>using RDP by<br>selected<br>employee   |
|---|------------------|--|--|
| Workstation                             | S, T, R, I, D, E | <ol> <li>Someone can act as a<br/>workstation and access server</li> <li>Workstation can claim it did not<br/>fulfill the request</li> <li>The workstation can be tweaked<br/>and changed</li> </ol>   | <ol> <li>Logs are sent<br/>to SIEM</li> <li>SSH keys is<br/>needed to<br/>access<br/>webserver</li> </ol>  |
| DATA STORE                              |                  |  |  |
| Mysql Database                          | T, R, I, D       | <ol> <li>Someone can access the data<br/>from database</li> <li>Database can claim it did not<br/>fulfill the request</li> <li>Overwhelming requests can<br/>make it unavailable</li> <li>The Database can be tweaked<br/>and changed</li> </ol>   | <ol> <li>The database<br/>itself is<br/>encrypted</li> <li>Logs are sent<br/>to SIEM</li> <li>Database can<br/>only be<br/>accessed by<br/>webserver<br/>from specific<br/>IP</li> </ol> |
| DATA FLOW                               |                  |  |  |
| Customer←→Webserver                     | Т, І             | An attacker can intercept the data flow, read and modify the data  | TLS is being used  |
| Webserver ←→ Mysql                      | Т, І             | An attacker can intercept the data<br>flow, read and modify the data   | TLS is being used  |
| Employee ←→ DC                          | Т, І             | An attacker can intercept the data flow, read and modify the data  | TLS is being used  |
| DC $\leftarrow \rightarrow$ Workstation | Т, І             | An attacker can intercept the data flow, read and modify the data  | TLS is being used  |
| Workstation←→Webserver                  | Т, І             | An attacker can intercept the data flow, read and modify the data  | TLS is being used  |
| Webserver → SIEM                        | Т, І             | An attacker can intercept the data flow, read and modify the data  | TLS is being used  |
| Mysql → SIEM                            | Т, І             | 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



| Cipher Suites   |     |  |  |  |  |  |
|---|-----|--|--|--|--|--|
| #TLS 1.3 (sultes in server-preferred order)   | Ξ   |  |  |  |  |  |
| 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 (0xc02£) 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 |  |  |  |  |  |
|   |     |  |  |  |  |  |



| DarkSeas Bank - Web App Test   |     |     |  |  |  |  |  |  |  |
|--|-----|-----|--|--|--|--|--|--|--|
| < Back to My Scans   |     |     |  |  |  |  |  |  |  |
| Hosts 1 Vulnerabilities 23 History 1                                     |     |     |  |  |  |  |  |  |  |
| Filter     Search Vulnerabilities     Q     23 Vulnerabilities           |     |     |  |  |  |  |  |  |  |
| Sev V Name A Family A C  |     |     |  |  |  |  |  |  |  |
| Browsable Web Directories CGI abuses                                     | 1   | 0 / |  |  |  |  |  |  |  |
| HSTS Missing From HTTPS Server (RFC 6797) Web Servers                    | 1   | 0 / |  |  |  |  |  |  |  |
| GI abuses : XSS CGI abuses : XSS   | 3 1 | 0 / |  |  |  |  |  |  |  |
| MEDUM Web Application Potentially Vulnerable to Clickjacking Web Servers | 1   | 0 / |  |  |  |  |  |  |  |

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/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) l 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) 1\_ 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 l\_http-server-header: Apache/2.4.29 (Ubuntu) I\_http-title: Did not follow redirect to https://www.darkseasbank.com/ 443/tcp open ssl/http Apache httpd 2.4.29 ((Ubuntu)) l\_http-server-header: Apache/2.4.29 (Ubuntu) I\_http-title: DarkSeas Bank I ssl-cert: Subject: commonName=www.darkseasbank.com I Subject Alternative Name: DNS:www.darkseasbank.com | Not valid before: 2021-03-11T23:55:42 L\_Not valid after: 2021-06-09T23:55:42 I\_ssl-date: TLS randomness does not represent time | tls-alpn: 465/tcp closed smtps 3306/tcp closed mysql Device type: general purposelstorage-misclfirewall 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 05 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:<br>+ Target Hostname:<br>+ Target Port:  | 52.191.161.183<br>www.darkseasbank.com<br>443   |  |
| + SSL Info:<br>+ Start Time:  | Subject: /CN=www.darkseasbank.com<br>Altnames: www.darkseasbank.com<br>Ciphers: ECDHE-RSA-CHACHA20-POLY1305<br>Issuer: /C=US/0=Let's Encrypt/CN=R3<br>2021-03-23 17:48:42 (GMT-7)   |  |
| <pre>+ Server: Apache/2.<br/>+ Server: Apache/2.<br/>+ The anti-clickjac<br/>+ The X-XSS-Protect:<br/>+ The site uses SSL<br/>+ The X-Content-Typ<br/>+ Cookie PHPSESSID<br/>+ No CGI Directorie<br/>+ The Content-Encod<br/>+ Uncommon header '<br/>+ Apache mod_negoti<br/>tives for 'index' w<br/>+ Web Server return<br/>+ OSVDB-3268: /down<br/>+ OSVDB-3268: /img/<br/>+ OSVDB-3268: /img/<br/>+ Server leaks ind<br/>envmo + Cooco + Cooco</pre> | 4.29 (Ubuntu)<br>:king X-Frame-Options header is not present.<br>tion header is not defined. This header can hint to the<br>_ and the Strict-Transport-Security HTTP header is not of<br>e-Options header is not set. This could allow the user<br>created without the secure flag<br>is found (use '-C all' to force check all possible dirs<br>ing header is set to "deflate" this may mean that the is<br>'ton' found, with contents: list<br>iation is enabled with MultiViews, which allows attacke<br>were found: index.bak<br>ns a valid response with junk HTTP methods, this may can<br>hload/: Directory indexing found.<br>hload/: This might be interesting<br>/: Directory indexing found.<br>/: This might be interesting | user agent to protect against some forms of XSS<br>lefined.<br>agent to render the content of the site in a different fashion to the MIME type<br>erver is vulnerable to the BREACH attack.<br>rs to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alterna<br>use false positives. |

+ 1 host(s) tested



### Nikto Top Vulnerabilities

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

### **OpenVAS**

| Greenbone  |                  |              |            |                        |                 |              |           |                |                |                 |                     |                                |                        |
|--|------------------|--------------|------------|------------------------|-----------------|--------------|-----------|----------------|----------------|-----------------|---------------------|--------------------------------|------------------------|
| Dashboards   |                  | Scans Assets |            |                        | Resilience      |              | SecInfo   |                | juration Admi  | nistration      | Help                |                                |                        |
| ◎≣ ≝≣ ≣®★®≫ Ł⊳   |                  |              |            |                        |                 |              |           |                | Filter         |                 | \$00×0              | 🔻                              |                        |
| Information         Results         Hosts         Ports         Applications         Operating Systems         CVEs         Closed CVEs         TLS Certificates         Error Messages         User Tags           (0 of 0)         (1 of 1)         (1 of 2)         (1 of 1)         (0 of 0)         (1 of 1)         (0 of 0)         (0 of |                  |              |            |                        |                 |              |           |                |                |                 |                     |                                |                        |
| Host   |                  |              |            |                        |                 |              |           |                |                | N 11-2012VV     |                     |                                |                        |
| Vulnerability  |                  | <b>a</b>     | Severity V | QoD                    | IP              | Name         | Location  | Created        | Created        |                 |                     |                                |                        |
| SSL/TLS: Missing 'secure' Cookie Attribute   |                  |              |            |                        | 47              | 6.4 (Medium) | 99 %      | 52.191.161.183 | www.darkseasba | ink.com 443/tcp | Wed, Mar 24, 202    | Wed, Mar 24, 2021 12:35 AM UTC |                        |
| TCP timestamps   |                  |              |            |                        |                 | 4            | 2.6 (Low) | 80 %           | 52.191.161.183 | www.darkseasba  | ink.com general/tcp | Wed, Mar 24, 202               | 1 12:35 AM UTC         |
| (Applied filter: apply_c   | overrides=0 leve | els=hml row  | s=100 min_ | qod=70 first=1 sort-re | verse=severity) |              |           |                |                |                 |                     |                                | <  <  1 - 2 of 2  >  > |

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





• 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



University of Southern California

#### **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 emáil) 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.

