



DSci526: Secure Systems Administration

Final Project Briefs
Project Demonstrations
Review for Final Exam

Prof. Clifford Neuman

Lecture 14
28 April 2021
Online



Final Exam

The Final exam for Data Science 526 will be held

Monday May 10th, 2021

2PM to 4PM Pacific Time

(I will also allow it to be taken from 6PM – 8PM upon request)

Online

Exam will be Open Book / Open Note

It will be taken Electronically

We will Discuss Logistics and Review
near the end of Lecture



Agenda

- 1400-1405 Introduction and Announcements
- 1405-1440 Poly Road Project Brief (and discussion)
- 1440-1515 Market of Mystery Brief (and discussion)
- 1515-1525 Break
- 1525-1540 Poly Road Demonstration
- 1540-1555 Market of Mystery Demonstration
- 1555-1630 Class Discussion
 - Red-Team Hypotheses and Rebuttals
- 1630-1720 Review and Logistics for Final Exam



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam

Poly Road

By Group 1

Law Enforcement Assessment

- Dark market vendors are most concerned with arrest, not being hacked. Confidentiality is the overriding security concern.
- “Beyond a Reasonable Doubt” is a tough standard - limit the evidence available to meet that standard.
- Criminal networks must be selective about what they collect.
- Encryption is a must but not the only safeguard - Ross Ulbricht employed encryption.
- More incriminating evidence must be kept in a more secure protection domain.
- Criminal networks must constantly move. Move to new bullet proof server every two weeks.
- Production network is wiped every two weeks.
- Constantly improve your “development” system, not your production system.
- Deliverable is essentially a text file (stolen credit card info) - use end-to-end encrypted email.
- Customer Service doesn’t have to be all that good. Transaction history is deleted after two days.

Cloud Deployment

- Local Testing
 - Front End Application
 - Databases
 - Overall Functionality
- Azure Cloud
 - Storing of Dummy Criminal Data
 - Configuration Challenges
 - The migration to the cloud.

Cloud Deployment Con't

Why Azure?

Auditing, scalability, and feasibility

B2B Collaboration

Home > Sarahzin Directory >

Users | All users (Preview)

Sarahzin Directory - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Multi-Factor Authentication Delete user

«

- All users (Preview)
- Deleted users (Preview)
- Password reset
- User settings
- Diagnose and solve problems

Activity

- Sign-ins
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

Search users Add filters

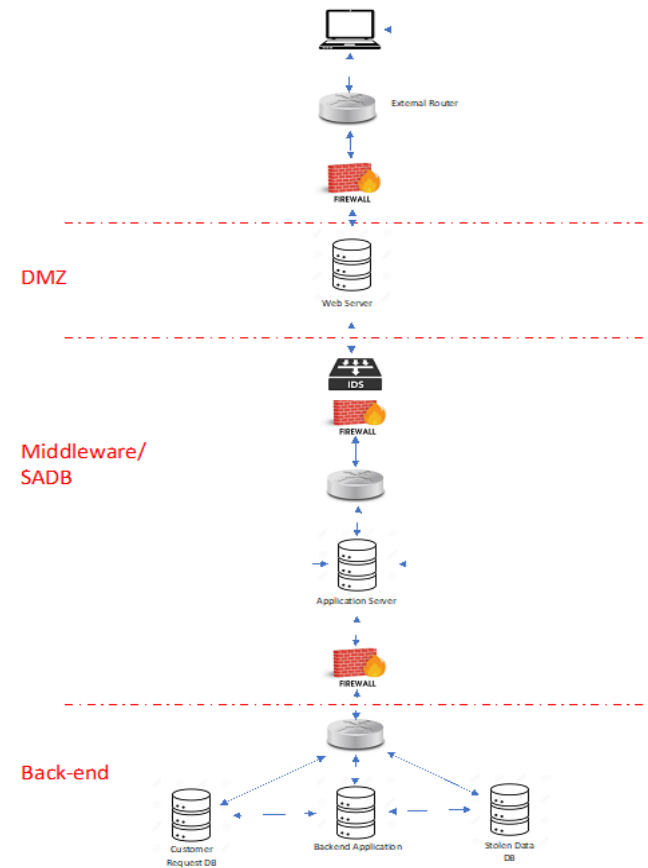
14 users found

	Name	User principal na...	User type	Directory synced	Identity issuer	Company name	Creation type
<input type="checkbox"/>	AA aambasth	aambasth_usc.edu#E...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	AT Abhishek Tatti	atatti_usc.edu#EXT#...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	AC Anthony Cassar	acassar_usc.edu#EXT#...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	CS Chris Shane	chrisshane22_gmail.c...	Member	No	chrisshane22gmail.onnr		
<input type="checkbox"/>	CS Christopher S...	csamayoa_usc.edu#E...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	HZ Hanzhou Zhang	hanzhou_usc.edu#E...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	JT jtsclubadiver	jtsclubadiver_gmail.co...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	LU Louis Uuh	uuh_usc.edu#EXT#@...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	MW MaryLiza Walk...	marywalk_usc.edu#E...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	PP Pratyush Prak...	prakhar_usc.edu#EXT#...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	SS Sarahzin Shane	sarahzic_usc.edu#EX...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	SB Shagun Bhatia	shagunbh_usc.edu#E...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	SH shagunb	shagunb_usc.edu#EX...	Guest	No	chrisshane22gmail.onnr		Invitation
<input type="checkbox"/>	TP Tejas Pandey	tpandey_usc.edu#EX...	Guest	No	chrisshane22gmail.onnr		Invitation

Network Diagram

- Layered Security
 - Application
 - DMZ(Webserver)
 - Back-End
- Traditional MySQL Database vs Azure MYSQL Databases
- Firewalls

Source: Jason's Assignment #2



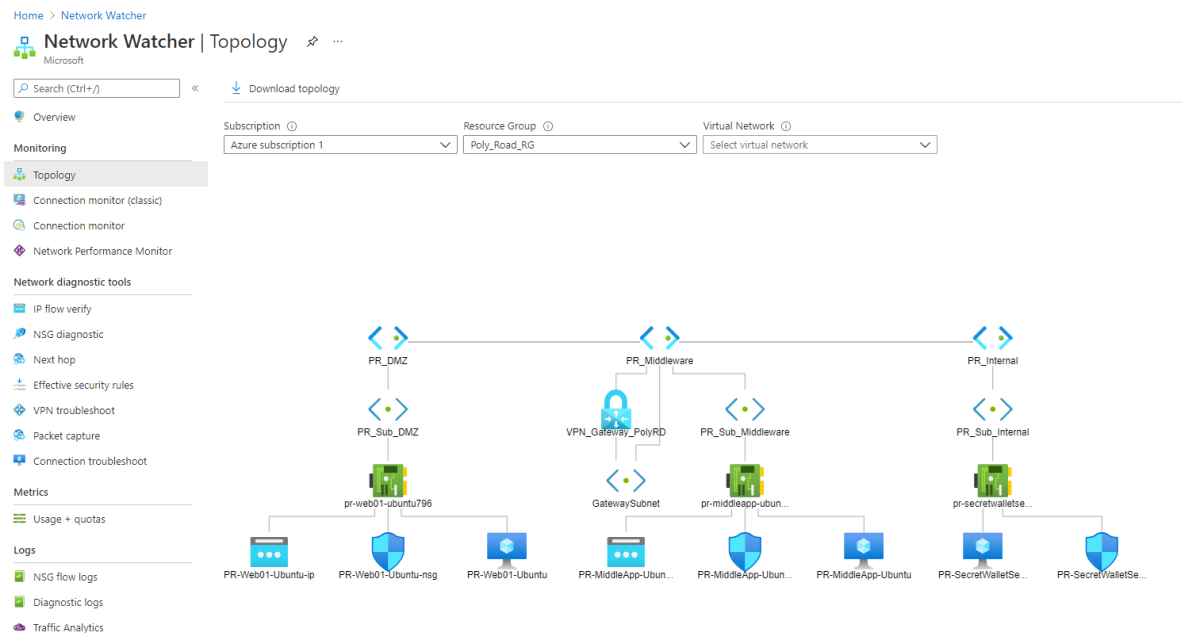
Network Components

- Azure Subnetting
 - Peering
 - Access Points
- Azure to VPN Client
 - OpenVPN
 - Certifications
- Protonmail

ProtonMail

- Overview
 - Hosted in Switzerland
 - End-to-end encryption
 - Uses asymmetric and symmetric encryption
- ProtonMail Bridge
 - Allows local client to use end-to-end encryption
 - Client/user authenticates to bridge
 - Bridges authenticates to ProtonMail via API (SRP Protocol)
 - Secure Remote Password (SRP) Protocol (RFC 2945) ensures that the user's password never leaves local machine

Network Topology (Azure)



Linux Hardening

- Kernel Configuration
 - Protection against SYN flood attacks
 - `echo "kernel.exec-shield = 2" > /etc/sysctl.d/50-exec-shield.conf`
 - Restricting access to the kernel logs
 - `echo "kernel.dmesg_restrict = 1" > /etc/sysctl.d/50-dmesg-restrict.conf`
 - Restricting access to kernel pointers
 - `echo "kernel.kptr_restrict = 1" > /etc/sysctl.d/50-kptr-restrict.conf`
 - Protect against IP spoofing
 - `echo "kernel.exec-shield = 2" > /etc/sysctl.d/50-exec-shield.conf`

Linux Hardening

- Monitoring System Events with AuditD

- Log every attempt to read/modify the `/etc/ssh/sshd_config` file:
 - `auditctl -w /etc/ssh/sshd_config -p warx -k sshd_config_modified`
- Log changes to `/etc/passwd`:
 - `auditctl -w /etc/passwd -p wa -k passwd_modified`
- Monitor `/etc/sudoers` for changes:
 - `auditctl -w /etc/sudoers -p wa -k sudoers_modified`
- Log all invocation of “useradd” command:
 - `auditctl -a always,exit -F exe=$(which useradd) -F arch=b64 -S execve -k useradd_executed`
- Log insertion and removal of kernel modules:
 - `auditctl -a always,exit perm=x -F auid!=-1 -F path=/sbin/modprobe -k modules_event`
 - `auditctl -a always,exit perm=x -F auid!=-1 -F path=/sbin/rmmod -k modules_event`

Firewall

- The Host-Based Firewall
 - Security Groups
 - Implicit-Deny
- Externally Managed Firewall
 - Costs(Currently not configured)
 - What about in the current industry?
- Azures Firewall
 - Network Segmentation
 - Easy Configuration
- Open Ports
 - Management ports(SSH)
 - Web Traffic(HTTP and TLS)
 - What would change in a real environment?

Database Management & Middleware (Abhishek Fill in)

The database running in **pr-customerdb-mysql VM in azure** is a **MYSQL database**. The Structure of the table is as follows:

- TABLE NAME: TRANSACTIONS
- ID - Primary key
- TRANSACTION_ID: Transaction id submitted by the customer, generated after successful payment
- EMAIL: The email address on which the user wants to receive the stolen credentials files.
- ITEM_ID: The item/list of stolen credentials selected by the customer.

INVENTORY:

- The inventory containing stolen credentials is not a database but is a folder of 3 files hosted on the PR-SecretWalletServer-Ubuntu VM in azure. Each of the files is associated with a product sold on the website.

MIDDLEWARE:

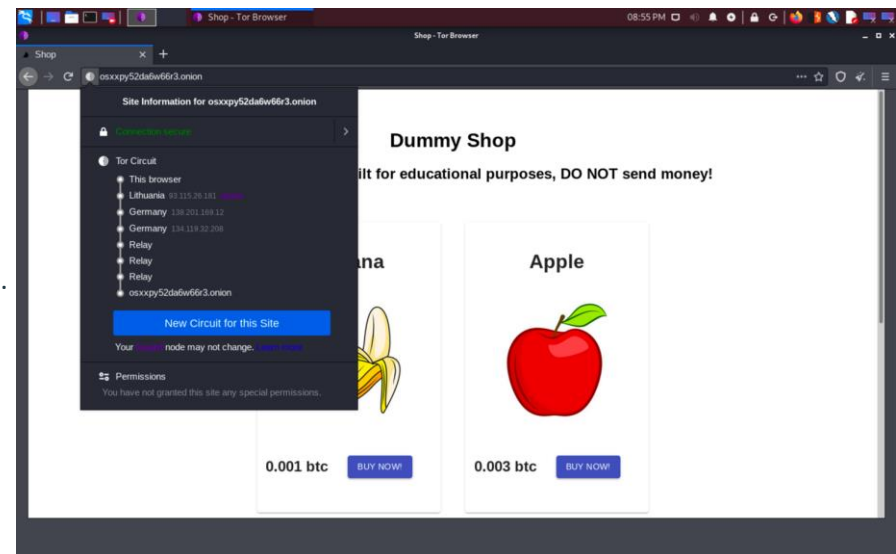
- The middleware will run as a python flask application and is hosted on PR-MiddleApp-Ubuntu VM in azure.
- This app provides an API endpoint for the frontend and will extract the fields from the header and store them in variables which can later be used to perform operations on the database.
- The biggest benefit of using the middleware is that it doesn't allow the web server to directly access your database thus provides a second layer of security against attacks like XSS or SQL injection.

Tor Implementation(Abhishek)

Onion address: osxpxy52da6w66r3.onion

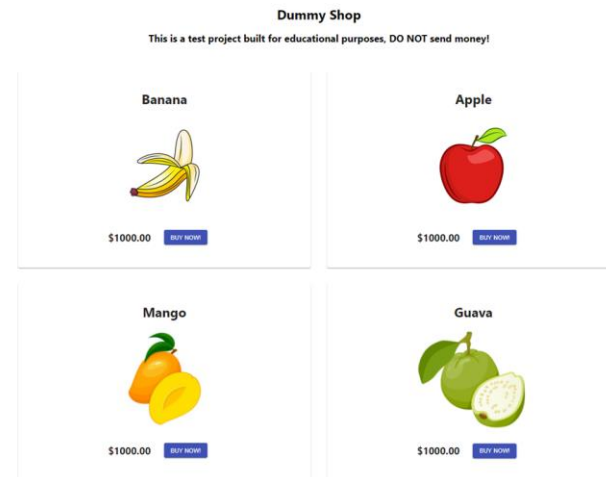
Advantages of Tor Network

- You can access the deep dark internet websites and blocked websites.
- You can hide your original Internet Protocol (IP) address.
- You will be able to access non-indexed pages in google, bing, Yandex etc search engines.
- It hides all the data regarding the source(which is you) and the destination.
- It also protects the information passed onto the network.



Front End Application(Ayush and Hanz)

- Because of the anonymity, our frontend only has two pages: index page and checkout page.
- The index page shows the price and the items that the customer can choose.
- We conceal the actual criminal information and only the people who know this website know what those items actually mean.



Front End Continued:

- The checkout.page shows the payment details
- Customers need to enter the item quantity, Bitcoin transaction ID and the email ID in order to finish the request.
- Frontend will send a POST request which includes the item ID, email address and transaction ID to <http://10.0.1.4:5000/> middleware.

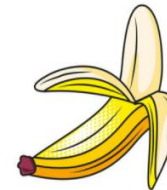
Dummy Shop

This is a test project built for educational purposes, DO NOT send money!

Payment Details

We only accept payment through Bitcoin

Address to send money to: Some value



Item: 1 dozen Bananas

Price: \$1000

Quantity:

Enter the Transaction ID:

Email ID:

[GO BACK](#)

[SEND REQUEST](#)

IDS or SIEM

- Why we chose not to include this in our project?
 - Non-Existent in current infrastructure project
 - Historically, online dark market vendors are most concerned with arrest.
 - Silk road was hacked numerous times and blackmailed.
 - Must weigh the value of identifying hackers versus the impact that collected data would have on a prosecution.
 - Better to constantly improve “development system” which is put into production every two weeks on different bullet-proof server.

Red Teaming and Penetration Testing

Active Reconnaissance Tools

- Nmap
 - `Nmap -sC -sV -vv -oA web01 13.66.168.190`
- Nikto
 - `Nikto -C all -h 13.66.168.190`
- Nessus
 - See report “Web01_iqi3bm.html”
- BurpSuite
 - See report “Burp_Suite_Report_2.html”

Nmap - Front End

```

# Nmap 7.91 scan initiated Fri Apr 23 13:13:21 2021 as: nmap -Pn -sC -sV -p- -oN frontend.txt 13.66.168.190
Nmap scan report for 13.66.168.190
Host is up (0.040s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 b2:ee:05:2c:3e:0e:e6:32:50:d5:67:91:26:04:87:ee (RSA)
|_ 256 03:0e:84:ca:79:d0:7e:a3:12:83:7f:dc:10:0b:10:8d (ECDSA)
|_ 256 ca:39:a9:22:2d:a0:ed:da:5b:1d:3a:ae:1d:a7:41:f4 (ED25519)
80/tcp    closed http
443/tcp   closed https
3000/tcp  open  ppp?
|_ fingerprint-strings:
|_   GetRequest:
|_     HTTP/1.1 200 OK
|_     Cache-Control: no-store, must-revalidate
|_     X-Powered-By: Next.js
|_     ETag: "10a5-Y07IPZnhRmNzLA9JbK4fK0nFU"
|_     Content-Type: text/html; charset=utf-8
|_     Content-Length: 4261
|_     Vary: Accept-Encoding
|_     Date: Fri, 23 Apr 2021 20:15:36 GMT
|_     Connection: close
|_     <!DOCTYPE html><html><head><style data-next-hide-fouc="true">body{display:none}</style><noscript data-next-hide-fouc="true"><style>body{display:block}</style></noscript><meta name="viewport"
|_     content="width=device-width"/><meta charset="utf-8"/><title>Shop</title><link rel="icon" href="/favicon.ico"/><meta name="next-head-count" content="4"/><noscript data-n-css=""></noscript><link
|_     rel="preload" href="/_next/static/chunks/webpback.js?ts=1619208936538" as="script"/><link rel="preload" href="/_next/static/chunks/main.js?ts=1619208936538" as="script"/><link rel="preload" href="/_next/
|_     static/chunks/pages/_app.js?ts=1619208936538" a
|_   HTTPOptions:
|_     HTTP/1.1 200 OK
|_     Cache-Control: no-store, must-revalidate
|_     X-Powered-By: Next.js
|_     ETag: "10a5-YE0VazuvJnK1K0D19fX3wq5SA"
|_     Content-Type: text/html; charset=utf-8
|_     Content-Length: 4261
|_     Vary: Accept-Encoding
|_     Date: Fri, 23 Apr 2021 20:15:36 GMT
|_     Connection: close
|_     <!DOCTYPE html><html><head><style data-next-hide-fouc="true">body{display:none}</style><noscript data-next-hide-fouc="true"><style>body{display:block}</style></noscript><meta name="viewport"
|_     content="width=device-width"/><meta charset="utf-8"/><title>Shop</title><link rel="icon" href="/favicon.ico"/><meta name="next-head-count" content="4"/><noscript data-n-css=""></noscript><link
|_     rel="preload" href="/_next/static/chunks/webpback.js?ts=1619208936783" as="script"/><link rel="preload" href="/_next/static/chunks/main.js?ts=1619208936783" as="script"/><link rel="preload" href="/_next/
|_     static/chunks/pages/_app.js?ts=1619208936783" a
|_   Help, NCP:
|_     HTTP/1.1 400 Bad Request
|_     Connection: close
|_   1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
|_   SF:Port3000-TCP:V=7.91X1=74D=4/234Time=60832AE0P=x86_64-ggole-darwin17.7.
|_   SF:0hr(GetRequest:1180,"HTTP/1.1x20200x200K\r\nCache-Control:x20no-sto
|_   SF:re,x20must-revalidate\r\nX-Powered-By:x20Next.js\r\nETag:x20"10a5-
|_   SF:ry07IPZnhRmNzLA9JbK4fK0nFU"\r\nContent-Type:x20text/html;x20charset
|_   SF:utf-8\r\nContent-Length:x204261\r\nVary:x20Accept-Encoding\r\nDate:V
|_   SF:x20Fri,x2023,x20Apr,x202021x2020:15:36x20GMT\r\nConnection:x20close
|_   SF:\r\n\r\n<!DOCTYPEx20html><html><head><stylex20data-next-hide-fouc="t
|_   SF:rue">body{display:none}</style><noscriptx20data-next-hide-fouc="true
|_   SF:\x20style=body{display:block}/><style></noscript><metax20name="viewpor
|_   SF:t:x20content="width=device-width"/><metax20charset="\utf-8"/><tit
|_   SF:le=Shop</title><linkx20rel="icon"x20href="/favicon.ico"/><metax
|_   SF:20name="next-head-count"x20content="4"/></noscript><linkx20data-n-css=""
|_   SF:\x20noscript><linkx20rel="preload"x20href="/_next/static/chunks/w
|_   SF:ebback.js?ts=1619208936538"\x20as="script"/><linkx20rel="preload
|_   SF:\x20href="/_next/static/chunks/main.js?ts=1619208936538"\x20as=""
|_   SF:script"/><linkx20rel="preload"x20href="/_next/static/chunks/pages
|_   SF:/_app.js?ts=1619208936538"\x20a"hr(Help,2F,"HTTP/1.1,x20400,x20Bad
|_   SF:x20Request\r\nConnection:x20close\r\n\r\n")hr(NCP,2F,"HTTP/1.1,x2040
|_   SF:0,x20Bad,x20Request\r\nConnection:x20close\r\n\r\n")hr(HTTPOptions,118
|_   SF:0,"HTTP/1.1,x20200,x200K\r\nCache-Control:x20no-store,x20must-revali
|_   SF:date\r\nX-Powered-By:x20Next.js\r\nETag:x20"10a5-YE0VazuvJnK1K0D19
|_   SF:fX3wq5SA"\r\nContent-Type:x20text/html;x20charset=utf-8\r\nContent-
|_   SF:length:x204261\r\nVary:x20Accept-Encoding\r\nDate:x20Fri,x2023,x20A
```

NIKTO

Frontend Server

```
Last login: Sat Apr 24 13:14:40 on ttys002
shagunbhatia@usc-guestwireless-upc-newsc6351 ~ % nikto -host 13.66.168.190:3000
- Nikto v2.1.6
-----
+ Target IP:          13.66.168.190
+ Target Hostname:    13.66.168.190
+ Target Port:        3000
+ Start Time:         2021-04-24 13:17:52 (GMT-7)
-----
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Next.js
+ Server leaks inodes via ETags, header found with file /, fields: 0x10a5 0xDw4gg3p4++t+SOWAAPAAT2Ac66Mg
+ 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 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
+ Uncommon header 'refresh' found, with contents: 0;url=/dXKqfPBq
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Nessus



Report generated by Nessus™

Web01

Fri, 23 Apr 2021 07:33:09 PDT

TABLE OF CONTENTS

[Hosts Executive Summary](#)

- [13.66.168.190](#)

Hosts Executive Summary

[Collapse All](#) | [Expand All](#)

13.66.168.190



Nessus

Severity	CVSS v3.0	Plugin	Name
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	10662	Web mirroring

Burp Suite

Burp Scanner Report



Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			Total
		Certain	Firm	Tentative	
Severity	High	0	0	0	0
	Medium	0	0	0	0
	Low	1	0	0	1
	Information	23	2	0	25

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Burp Suite

Contents

1. Unencrypted communications

2. Cross-origin resource sharing

- 2.1. <http://13.66.168.190:3000/>
- 2.2. http://13.66.168.190:3000/_next/static/chunks/main.js
- 2.3. http://13.66.168.190:3000/_next/static/chunks/pages/_app.js
- 2.4. http://13.66.168.190:3000/_next/static/chunks/pages/_error.js
- 2.5. http://13.66.168.190:3000/_next/static/chunks/pages/index.js
- 2.6. http://13.66.168.190:3000/_next/static/chunks/polyfills.js
- 2.7. http://13.66.168.190:3000/_next/static/chunks/react-refresh.js
- 2.8. http://13.66.168.190:3000/_next/static/chunks/webpack.js
- 2.9. http://13.66.168.190:3000/_next/static/development/_buildManifest.js
- 2.10. http://13.66.168.190:3000/_next/static/development/_ssgManifest.js
- 2.11. <http://13.66.168.190:3000/robots.txt>

3. Cross-origin resource sharing: arbitrary origin trusted

- 3.1. <http://13.66.168.190:3000/>
- 3.2. http://13.66.168.190:3000/_next/static/chunks/main.js
- 3.3. http://13.66.168.190:3000/_next/static/chunks/pages/_app.js
- 3.4. http://13.66.168.190:3000/_next/static/chunks/pages/_error.js
- 3.5. http://13.66.168.190:3000/_next/static/chunks/pages/index.js
- 3.6. http://13.66.168.190:3000/_next/static/chunks/polyfills.js
- 3.7. http://13.66.168.190:3000/_next/static/chunks/react-refresh.js
- 3.8. http://13.66.168.190:3000/_next/static/chunks/webpack.js
- 3.9. http://13.66.168.190:3000/_next/static/development/_buildManifest.js
- 3.10. http://13.66.168.190:3000/_next/static/development/_ssgManifest.js
- 3.11. <http://13.66.168.190:3000/robots.txt>

4. Input returned in response (reflected)


5. Frameable response (potential Clickjacking)

- 5.1. <http://13.66.168.190:3000/>
- 5.2. <http://13.66.168.190:3000/robots.txt>

1. Unencrypted communications

Next

Summary

	Severity:	Low
	Confidence:	Certain
	Host:	http://13.66.168.190:3000
	Path:	/

Issue description

The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. Unencrypted connections have been exploited by ISPs and governments to track users, and to inject adverts and malicious JavaScript. Due to these concerns, web browser vendors are planning to visually flag unencrypted connections as hazardous.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Please note that using a mixture of encrypted and unencrypted communications is an ineffective defense against active attackers, because they can easily remove references to encrypted resources when these references are transmitted over an unencrypted connection.

Issue remediation

Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.

2. Cross-origin resource sharing

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user.

Even if an allowed domain is not overtly malicious in itself, security vulnerabilities within that domain could potentially be leveraged by an attacker to exploit the trust relationship and attack the application that allows access. CORS policies on pages containing sensitive information should be reviewed to determine whether it is appropriate for the application to trust both the intentions and security posture of any domains granted access.

Issue remediation

Any inappropriate domains should be removed from the CORS policy.

3. Cross-origin resource sharing: arbitrary origin trusted

Issue background

An HTML5 cross-origin resource sharing (CORS) policy controls whether and how content running on other domains can perform two-way interaction with the domain that publishes the policy. The policy is fine-grained and can apply access controls per-request based on the URL and other features of the request.

Trusting arbitrary origins effectively disables the same-origin policy, allowing two-way interaction by third-party web sites. Unless the response consists only of unprotected public content, this policy is likely to present a security risk.


If the site specifies the header `Access-Control-Allow-Credentials: true`, third-party sites may be able to carry out privileged actions and retrieve sensitive information. Even if it does not, attackers may be able to bypass any IP-based access controls by proxying through users' browsers.

Issue remediation

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

4. Input returned in response (reflected)

Summary

	Severity:	Information
	Confidence:	Certain
	Host:	http://13.66.168.190:3000
	Path:	/robots.txt

Issue detail

The name of an arbitrarily supplied URL parameter is copied into the application's response.

Issue background

Reflection of input arises when data is copied from a request and echoed into the application's immediate response.

Input being returned in application responses is not a vulnerability in its own right. However, it is a prerequisite for many client-side vulnerabilities, including cross-site scripting, open redirection, content spoofing, and response header injection. Additionally, some server-side vulnerabilities such as SQL injection are often easier to identify and exploit when input is returned in responses. In applications where input retrieval is rare and the environment is resistant to automated testing (for example, due to a web application firewall), it might be worth subjecting instances of it to focused manual testing.

5. Frameable response (potential Clickjacking)

There are 2 instances of this issue:

- /
- /robots.txt

Issue description

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Note that some applications attempt to prevent these attacks from within the HTML page itself, using "framebusting" code. However, this type of defense is normally ineffective and can usually be circumvented by a skilled attacker.

You should determine whether any functions accessible within frameable pages can be used by application users to perform any sensitive actions within the application.

Issue remediation

To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself. Note that the SAMEORIGIN header can be partially bypassed if the application itself can be made to frame untrusted websites.

Vulnerability Management

- Unencrypted Communication
- Cross-end Resource Sharing
- Clickjacking Attack possible
- API Security headers Missing

Frontend Server

Last login: Sat Apr 24 13:14:48 on tty002
shagunbhatia@huc-guestwireless-upc-news6351 ~ N niko -host 13.66.168.190:3000
- Nikto v2.1.6

• Target IP: 13.66.168.190
• Target Hostname: 13.66.168.190
• Target Port: 3000
• Start Time: 2021-04-24 13:17:52 (GMT-7)

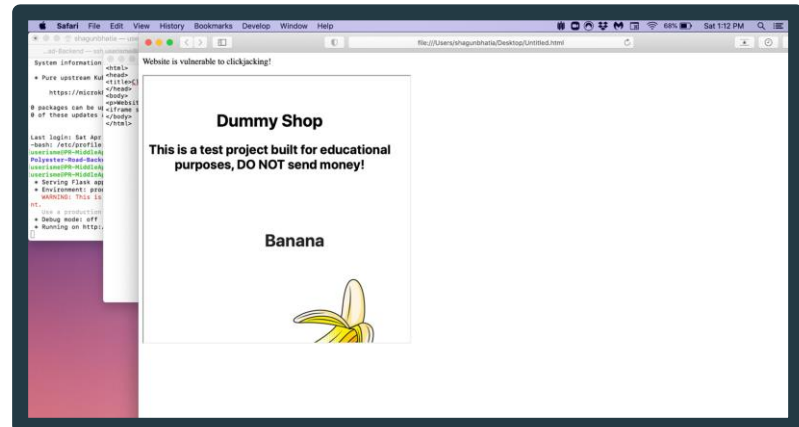
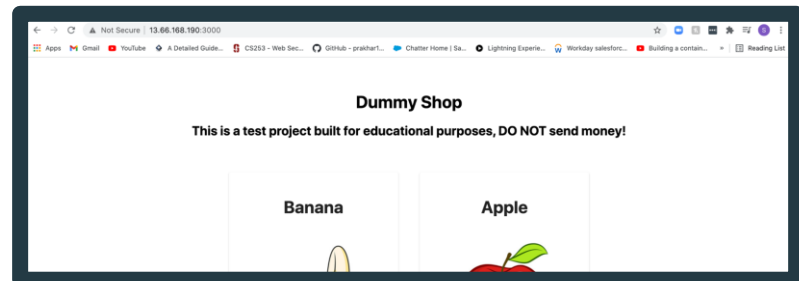
• Server: No banner retrieved
• Retrieved x-powered-by header: Next.js
• Server leaks inodes via ETags, header found with file /, fields: 0x10a5 0xb2c63b3a+1+50NAAPAT72ac6Mg
• The anti-clickjacking X-Frame-Options header is not present.
• The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
• The 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
• Unknown header 'refresh' found, with contents: 0x101d004cP8q
• No CGI Directories found (use '-C all' to force check all possible dirs)

Middleware server

shagunbhatia@huc-guestwireless-upc-news6351 ~ N niko -host 13.66.135.19:5000
- Nikto v2.1.6

• Target IP: 13.66.135.19
• Target Hostname: 13.66.135.19
• Target Port: 5000
• Start Time: 2021-04-24 13:16:12 (GMT-7)

• Server: Werkzeug/1.0.1 Python/3.6.9
• 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 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



Risk Assessment

The Top Risks

1. Unencrypted Communication : The site does not show any sensitive information you just select the package you want to buy and give email id
2. The site collects logs of the transaction for short time interval and later delete the information
3. Middleware application is public facing but it whitelist the ip that it can accept the communications from

Conclusion

Any Questions?



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam



Market of Mystery

**Use Your riddleBITS
Buy Something Shady**

Team 2 Project 2
26 April 2021
DSci 526
Spring

Market of Mystery



Team Members

Aditya Goindi -

Amarbir Singh - Deployment

Carol Varkey – Middleware/DBs/Deployment

Dwayne Robinson - Pen Test

Marco Gomez - FWs/SSL/Deployment

Yang Xue - Frontend/Deployment

Alejandro Najera - IDS/Honeypot

Azzam Alsaeed - EVERYTHING

Doug Platt - IDS/Honeypot

Malavika Prabhakar - IDS/Honeypot

Shanice Williams - FW Rules

Whole Team - Pen Testing

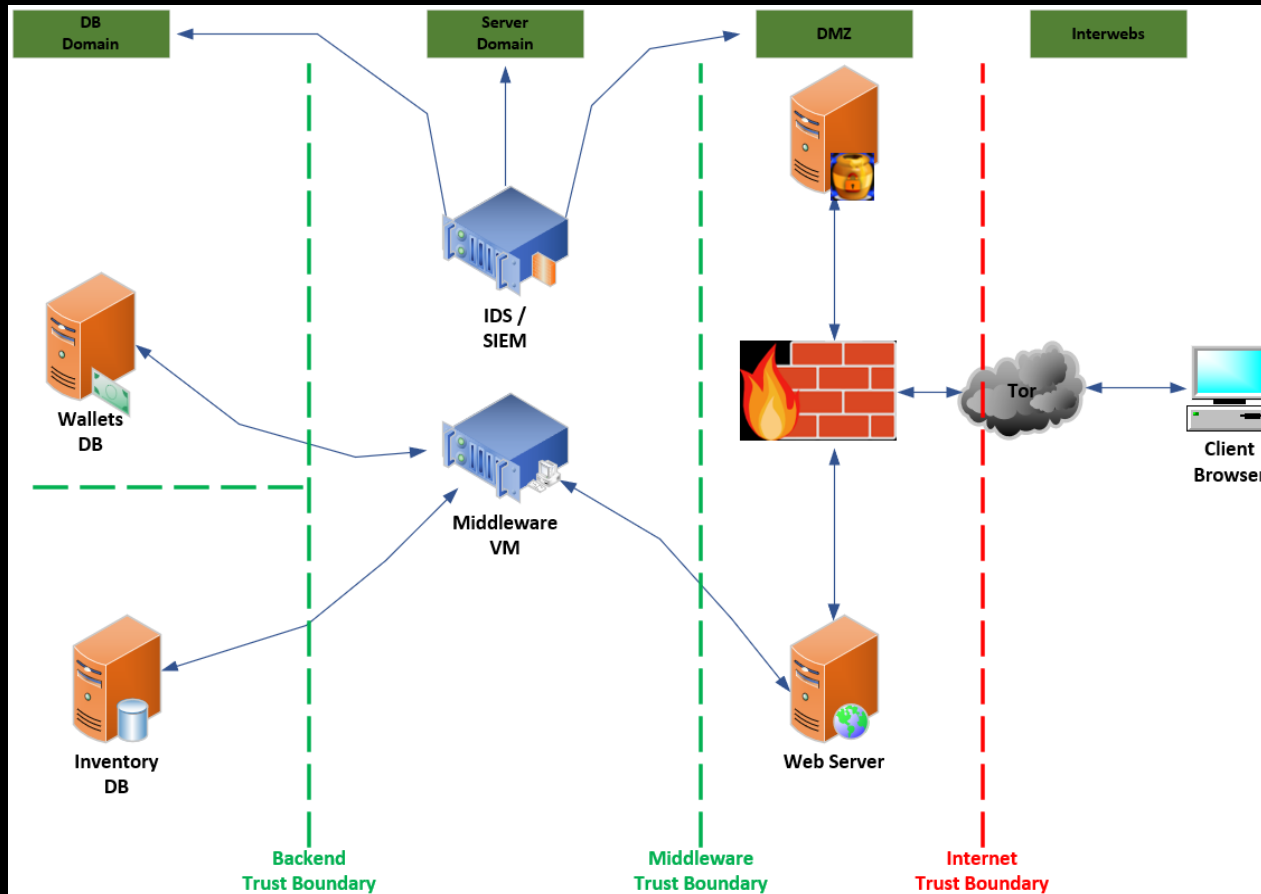
Market of Mystery



High Level System Description

The system is designed to allow us as the seller of stolen goods to sell to confirmed buyers while protecting, limiting, and hiding the amount of information we collect and maintain. A buyer is required to enter the Tor Network to view our website. As buyer(s) initially peruse our website, they must confirm to consent to the use of the website, they are 18 years old or older, and not affiliated with law enforcement to gain entry into the Market. Once in, the buyer can scan what we have for sale such as: OnlineFlix, MoneyPal, NoTube, and various other Stolen Goods. For payment, the buyer will input their riddleBIT[®]™ (not really TM, but we want it to sound official) address and it will be verified to ensure they have enough riddleBITS. Once the transaction is complete the buyer will be able to download the purchase and with an encryption key decipher the product.

Market of Mystery



Market of Mystery



Network and Server Architecture

DMZ Domain – Frontend

- > Developed using React next.js framework and the Material UI Library
- > Users' input as requests and ask the middleware for a response
- > Consists of 4 pages: Index, Homepage, Item, and Transaction Page

Market of Mystery



Network and Server Architecture cont.

Index: Our welcome page greets the user/buyer, and they are required to agree to the content to get into the market product detail page.

Homepage: Our homepage will list all the products' information from the database. Customers can scan and choose what they want. After customers click the "BUY" button, they will be redirected to the item page.

Marketplace of Mystery

☐ I agree with the terms and conditions of the website. I agree that I am 18 years of age or older and not affiliated with law enforcement

PROCEED

tr7j6fetvnrk7tpgmcaaxkwbu2k6t7y3kawoh7u2ypxdfbl6ssweqd.onion

Marketplace of Mystery

I agree with the terms and conditions of the website. I agree that I am 18 years of age or older and not affiliated with law enforcement

PROCEED

You have not agreed with the content!

OK

Marketplace of Mystery

Name: Carrot Type: Multiple Service Quantity: 10 Price: 29 BUY	Name: Zoodle Type: Multiple Service Quantity: 10 Price: 28 BUY	Name: NoTube Type: Streaming Service Quantity: 10 Price: 97 BUY	Name: Minisoft Type: Multiple Service Quantity: 10 Price: 36 BUY
Name: SocialIn Type: Social Service Quantity: 10 Price: 59 BUY	Name: Sahara Type: Payment Service Quantity: 10 Price: 24 BUY	Name: GitStand Type: Storage Service Quantity: 10 Price: 7 BUY	Name: FriendsBook Type: Social Service Quantity: 10 Price: 13 BUY

Market of Mystery



Network and Server Architecture cont.

Item: The item page will show the specific product's description and here the buyer enters the pre-shared "Bit String" (riddelBIT address) to try to buy the chosen product. The Frontend will use Axios to send the product information and Bit String to the middleware to check the validation.

Marketplace of Mystery

Name: Zoozle
Type: Multiple
Quantity: 10
Price: 28

Enter Bit String *

BUY

Marketplace of Mystery

[HOMEPAGE](#)

Name: HackedMail
Type: Email
Quantity: 10
Price: 5

Enter Bit String *

Bit String can't be empty!

OK

Market of Mystery



Network and Server Architecture cont.

Transaction: After the middleware check, it will return the result to the transaction page. If the Bit String (riddelBIT address) is wrong, customers will be shown Transaction failed information. Else, customers will see Transaction Success with a button to download the files that they bought from the middleware and a button to download the decryption tool, which can be used to decrypt the files.

Marketplace of Mystery

Name: CloudStore
Type: Storage
Quantity: 10
Price: 38

Transaction Failed

[HOMEPAGE](#)

Marketplace of Mystery

Name: GitStand
Type: Storage
Quantity: 10
Price: 7

Transaction Successful

YfMxXgYH5Ebq3yvVhm_hN3m0LBINWbuUZrHQqbdLH8=

DOWNLOAD

DECRYPTION TOOL

[HOMEPAGE](#)

Market of Mystery

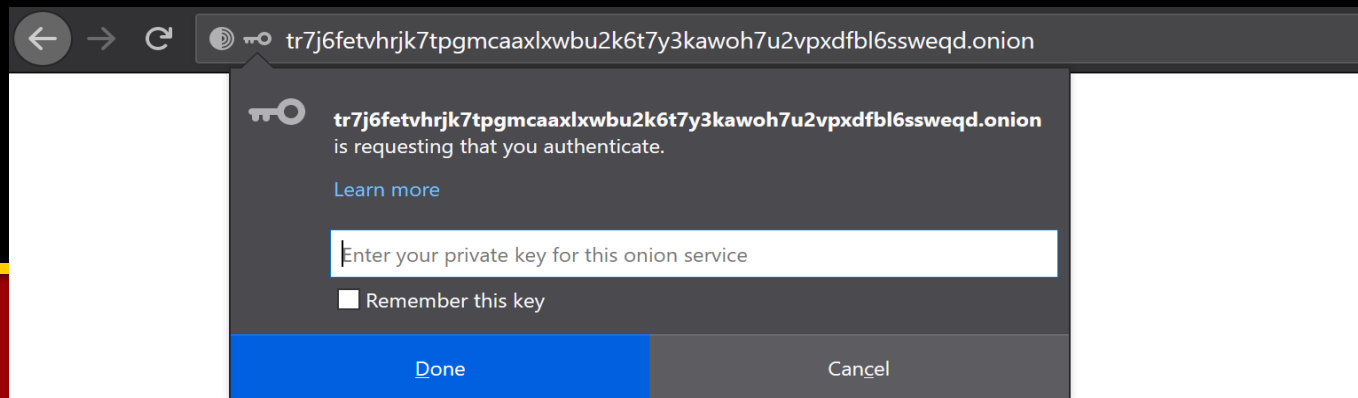


Network and Server Architecture cont.

DMZ Domain – Tor/Web Server

- > Running a Tor client service on our web server virtual machine
- > Running a Nginx web server
- > Using the latest version of Tor, which has longer URLs and stronger cryptography
- > Configured to use client authorization, so clients can only connect if they have a unique private key.

URL- `tr7j6fetvhrjk7tpgmcaaxlxwbu2k6t7y3kawoh7u2vpxdfbl6ssweqd.onion`





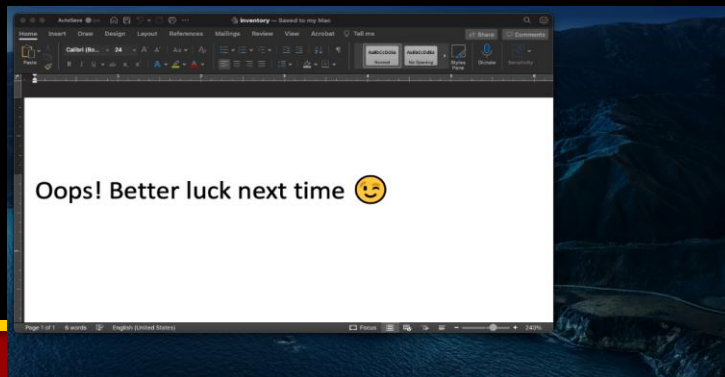
Market of Mystery

Network and Server Architecture cont.

DMZ Domain – HoneyTraps, HoneyWall, and HoneyNet

HoneyTraps: Canarytokens

We used canary tokens as a means of knowing if and when an attacker manages to get past our defenses. These tokens are basically honey traps scattered around the web server, with alluring names such as “inventory.docx” and “transactions.pdf” which draw the attacker into opening them.



Canarytoken triggered

ALERT

A DNS Canarytoken has been triggered by the Source IP 66.75.177.5. Please note that the source IP refers to a DNS server, rather than the host that triggered the token.

Basic Details:

Channel	DNS
Time	2021-04-24 02:21:08 (UTC)
Canarytoken	veahpnttbbkg1lzfj8ybd3j
Token Reminder	Token triggered: PDF file placed in webserver /home/honestt/marketplace_mystery/.git/logs
Token Type	adobe_pdf
Source IP	66.75.177.5

Canarytoken Management Details:

Manage this Canarytoken [here](#)

More info on this token [here](#)

Market of Mystery



Network and Server Architecture cont.

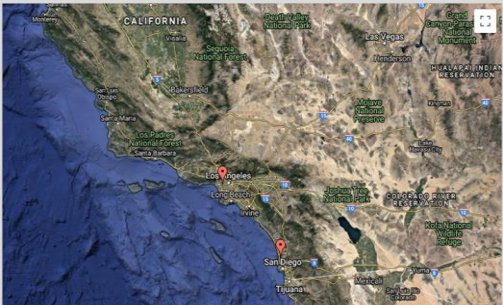
DMZ Domain – HoneyTraps, HoneyWall, and HoneyNet

HoneyTraps: Canarytokens cont.

History for Canarytoken:
veahpnntbbkeglizj8ybhd3j

Heads Up! Click the incident items for more info.

Incident Map



Incident List

Date	IP	Channel
2021 Apr 24 02:21:09.183841 (UTC)	66.75.177.41	DNS
2021 Apr 24 02:21:09.046266 (UTC)	66.75.177.4	DNS
2021 Apr 24 02:21:08.801977 (UTC)	66.75.177.44	DNS
2021 Apr 24 02:21:08.797487 (UTC)	66.75.177.5	DNS
2021 Apr 24 02:21:08.651659 (UTC)	66.75.177.44	DNS
2021 Apr 24 02:21:08.649204 (UTC)	66.75.177.5	DNS
2021 Apr 24 02:21:08.527828 (UTC)	66.75.177.44	DNS
2021 Apr 24 02:21:08.072592 (UTC)	66.75.177.5	DNS

Incident List

Date: 2021 Apr 24 02:21:08.649204 (UTC) IP: 66.75.177.5 Channel: DNS

Export

Geo Info

Country	US
City	Los Angeles
Region	California
Organisation	AS20001 Charter Communications Inc
Hostname	Isaica-dns-cac-302.socal.rr.com

Yot

Known Exit Node	False
-----------------	-------

Basic Info

Memo	Token triggered: PDF file placed in webserver /home/honestt/marketplace_mystery/glt/logs
------	--

Market of Mystery



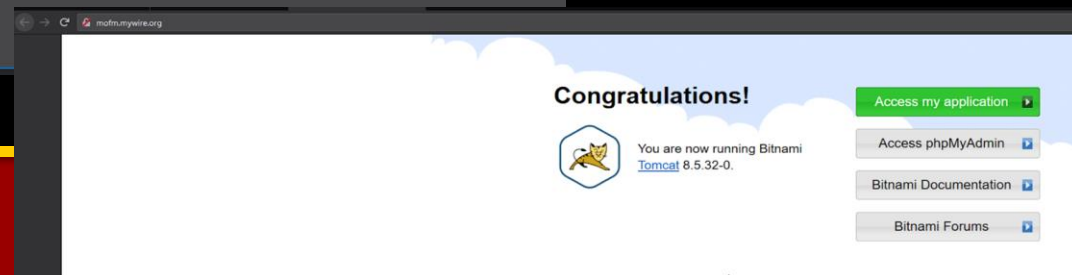
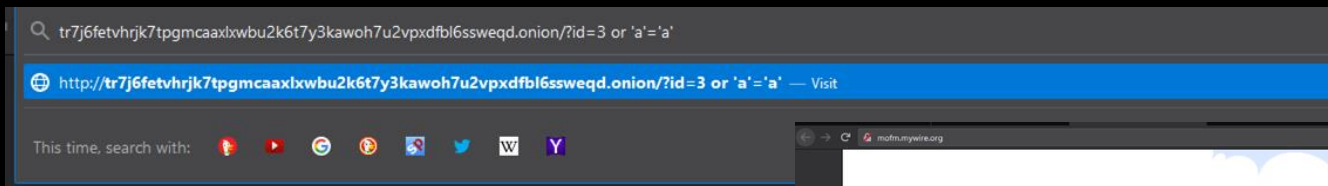
Network and Server Architecture cont.

DMZ Domain – HoneyTraps, HoneyWall, and HoneyNet

HoneyWall: Modsecurity

> An open source application that can be used with Apache, IIS, or Nginx, and allows for protection from a variety of attacks against web applications. It also provides for the capability to monitor traffic, log it, and either block or redirect malicious traffic

> OWASP CRS - activated rules will redirect to the honeypot





Market of Mystery

Network and Server Architecture cont.

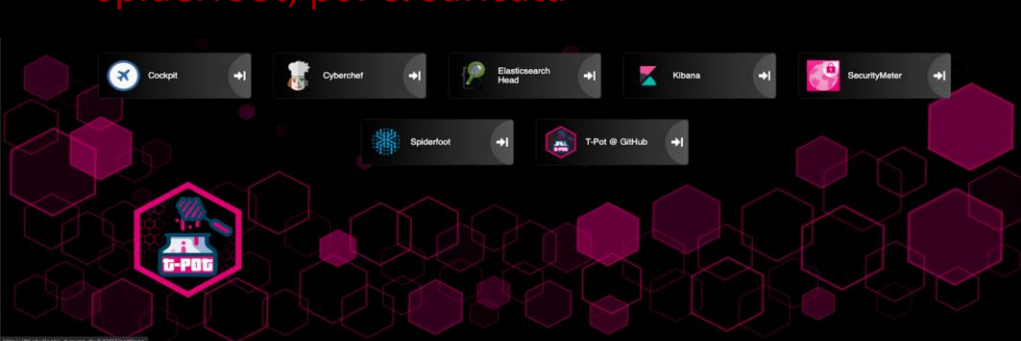
DMZ Domain – HoneyTraps, HoneyWall, and HoneyNet

HoneyNet: HoneyPots

tPot – HoneyNet

Honeypots: adbhoney, ciscoasa, citrixhoneypot, conpot, cowrie, dicompot, dionaea, elasticpot, heralding, honeysap, honeytrap, mailoney, medpot, rdp, snare & tanner

Tools: cockpit, cyberchef, ELK, fatt, elasticsearch head, ewsposter, nginx / heimdall, spiderfoot, p0f & suricata

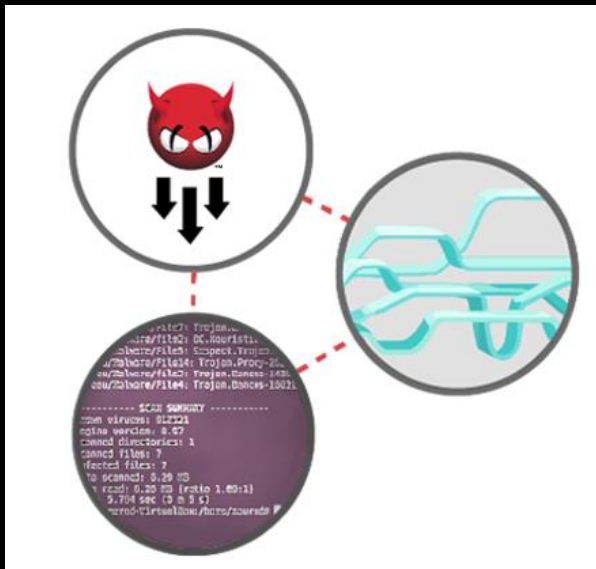




Market of Mystery

Network and Server Architecture cont.

Server Domain – IDS/SIEM



Host Antivirus – ClamAV

- > Opensource
- > Command Line Scanner
- > Automatic database updates
- > Scalable multithreaded daemon

```
File Edit View Search Terminal Help
ubuntu@ubuntu:~$ clamscan --infected --remove --recursive /home/ubuntu/Desktop/

----- SCAN SUMMARY -----
Known viruses: 2226383
Engine version: 0.102.2
Scanned directories: 14
Scanned files: 62
Infected files: 0
Data scanned: 9.72 MB
Data read: 4.66 MB (ratio 2.09:1)
Time: 11.842 sec (0 m 11 s)
ubuntu@ubuntu:~$ _
```

Market of Mystery



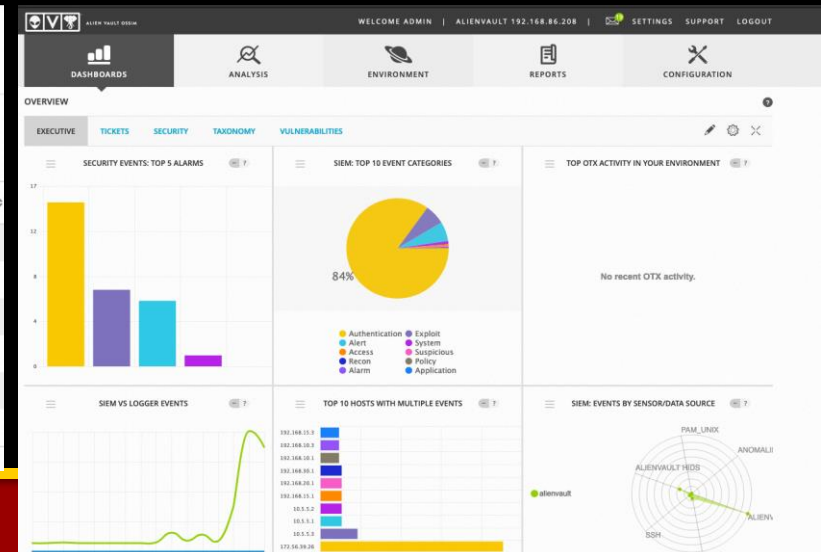
Network and Server Architecture cont.

Server Domain – IDS/SIEM

Intrusion Detection

AlienVault OSSIM – The AlienVault Open Source Security Information Management (OSSIM) SIEM Server provides asset management, vulnerability assessment, intrusion detection, behavioral monitoring and SIEM event correlation to our environment.

OVERVIEW AGENTS AGENTLESS EDIT RULES CONFIG HIDS CONTROL						
AGENT CONTROL SYSCHECKS AGENT.CONF						
Automatic HIDS deployment is only available for assets with a Windows OS defined in the asset details pages. If you are unable to deploy a HIDS agent to a Windows machine, you may need to update the OS field on the asset details.						
Search						
AGENT INFORMATION						
ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/local
001	Inventory_DB	InventoryDB	192.168.15.1	192.168.15.1	-	Active
2	MOM_DB	MomDB	192.168.10.1	192.168.10.1	-	Active
3	Webserver	Webserver	10.5.5.1	10.5.5.1	-	Active
4	Middleware	Middleware	10.5.5.2	10.5.5.2	-	Active
5	Tpot_HoneyNet	tPotHoneyNet	10.5.5.4	10.5.5.4	-	Active
SHOWING 1 TO 6 OF 6 AGENTS						



Market of Mystery



Network and Server Architecture cont.

Server Domain – Middleware

The Middleware VM runs 2 Python Flask Apps to support API calls between the frontend web server and backend databases. The apps include:

- > Wallet App

Interact with Wallets DB VM. App validates the transaction. Upon confirmation, encryption key for stolen credentials file is generated using the Fernet symmetric encryption method (from the Python cryptography package)

- > Inventory App

Interact with Inventory DB VM. App creates the encrypted stolen credentials file in memory (to not store in the VM itself). Returns the encrypted stolen credentials file and Decryptor Tool.

Market of Mystery



Network and Server Architecture cont.

DB Domain – Databases

The following 2 DB VM's all have installed MySQL Server:

- > MoM DB VM: Contains the Wallets DB Table

Database of stand in valid/available riddleBIT addresses', and their associated balances. Involved in the operations of the middleware Wallet App for returning data in making determinations of if the transaction is valid.

- > Inventor DB VM: Contains the Inventory DB Table

Database of dummy stolen credentials including Source Type, Source Name, Identifier, and Password encrypted with AES object encryption. Involved in operations of the middleware Inventory App in managing the credentials used in a given transaction.

Market of Mystery



Network and Server Architecture cont.

DB Domain – Databases

Protections in Place

- > Containment architecture separated these database tables into separate VMs to support isolation of their operations
 - > Utilized MySQL's Secure Installation Utility
 - > DBs both have a specified user accounts, given only the necessary grant privileges and reachable from their corresponding middleware app's address
 - > Used MySQL-supported AES object encryption for the Inventory Database Table (tradeoffs with other database encryption methods)
 - > Configured SSL/TLS encrypted connections between the MySQL database servers and middleware app clients

Market of Mystery



Risk Assessment/Vulnerability Analysis

Database-Related Risks

Database Encryption

There was much difficulty in applying whole disk encryption post VM instance creation. We decided that Object encryption would suit us better. We decided to activate the MySQL AES-256 encryption for the Inventory DB. This protected it while it was in use and at rest. Thus, if the hardware was stolen or taken by the authorities, they would not be able to decrypt our DB and the transactions.

We are accepting the risk to not have whole disk encryption since we had an OS hardened to Level II from the start.

Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

Database-Related Risks

AES Encryption Key

As this key is stored in the middleware and used in commands sent from the middleware to databases, we identified viable risks in entities possibly having visibility into our AES key that can further compromise the effectiveness of the object encryption put in place.

Mitigation: Configured SSL/TLS to support secure encrypted traffic between the MySQL Database Servers and Middleware App Clients.

We are accepting the tradeoff of having object encryption at rest and runtime which requires us to have the key stored in the middleware compared to the risk of having a whole disk encryption which results in the system being in unencrypted state while running.

Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

TOR-Related Risks

We decided to not implement SSL for web traffic as we are relying on Tor clients to encrypt all communications between them.

- > However, the traffic between the web server and Tor client as well as between the user's web browser and Tor client is on plain http. As this no-encrypted communication happens inside a single machine, we decided to accept this risk.

- > We have implemented a public-private key system to allow public access to Tor services. However, we cannot control if a legitimate user gives their private key away or their key is stolen. So even though we are limiting access to only certain individuals, we still risk other individuals acquiring the necessary keys.

Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

Information Flow-Related Risks

System Wide Information Flow Control

Mitigation

Firewall rules were placed onto each DB instance to control the flow of information. We controlled what information was allowed on each port and which protocol was allowed to flow on that interface. After all of the system required information was allowed all other ports and protocols were DENIED.

Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

Pen Testing

Mozilla Observatory: XSS, clickjacking, CORS, non-encrypted communication, inline javascript/CSS etc.

- > Remediated most of these vulnerabilities by setting proper policies and headers on our web server. We are relying on Tor for non-encrypted communication

Pentest-tools: CVE-2018-16843, CVE-2018-16844, CVE-2019-9511, CVE-2019-9513 etc.
Our version of Ubuntu came standard with an old version

- > We installed the latest version of Nginx from the vendor itself and the vulnerability scanner did not detect any high or medium level vulnerabilities again



Market of Mystery

Risk Assessment/Vulnerability Analysis cont.

Pen Testing

Another minor vulnerability that was found was that server version information was visible in the response. This might be helpful for an attacker in information gathering.

> Turn off server tokens that way our server does not give out any version information.

Probely & ImmuniWeb

Probely

Hello!

Probely finished scanning and found the following vulnerabilities.

Severity	Count
HIGH	0
MEDIUM	0
LOW	1

[View findings details](#)

Your final score

A

Tested on: Today, 04:21 CET
Server IP: 136.52.90.13
Reverse DNS: 136-52-90-13.googlefiber.net
Location: Mountain View
Client: Desktop Browser

[Refresh test](#) [Download report](#)

Test Type	Issues Found
Software Security Test	NO ISSUES FOUND
GDPR Compliance Test	2 ISSUES FOUND
PCI DSS Compliance Test	1 ISSUE FOUND
Content Security Policy Test	NO ISSUES FOUND
HTTP Headers Security Test	NO ISSUES FOUND

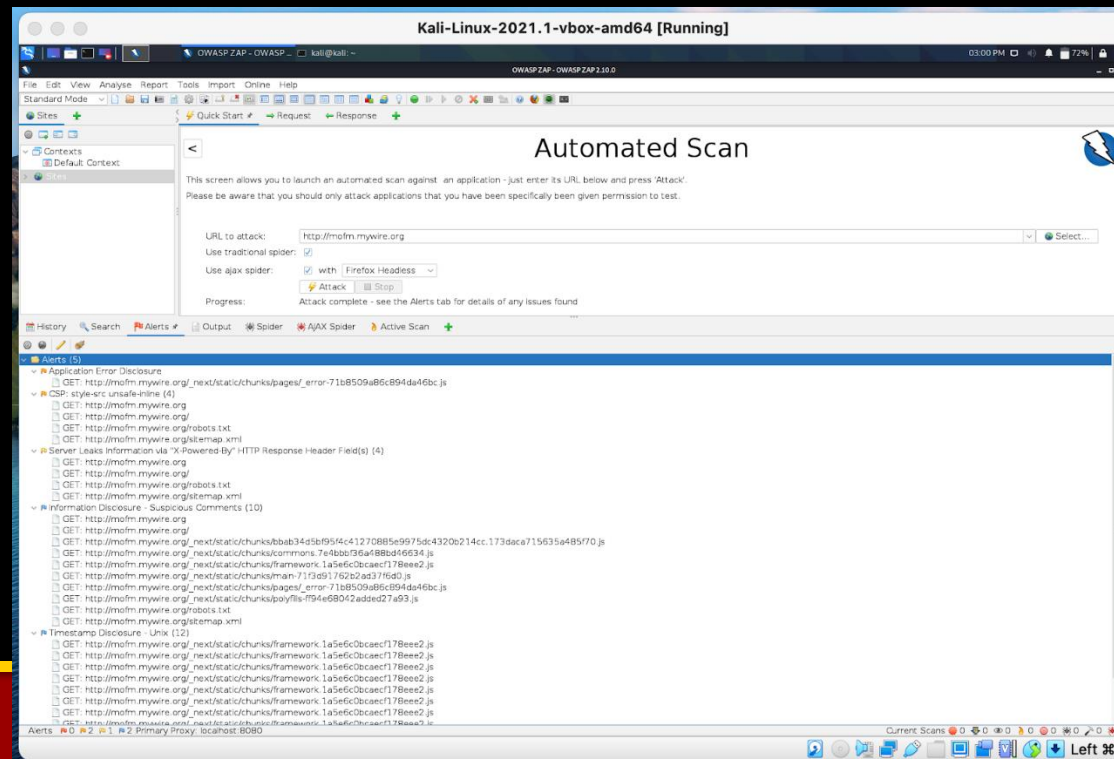


Market of Mystery

Risk Assessment/Vulnerability Analysis cont.

Pen Testing

OWASP ZAP



Market of Mystery

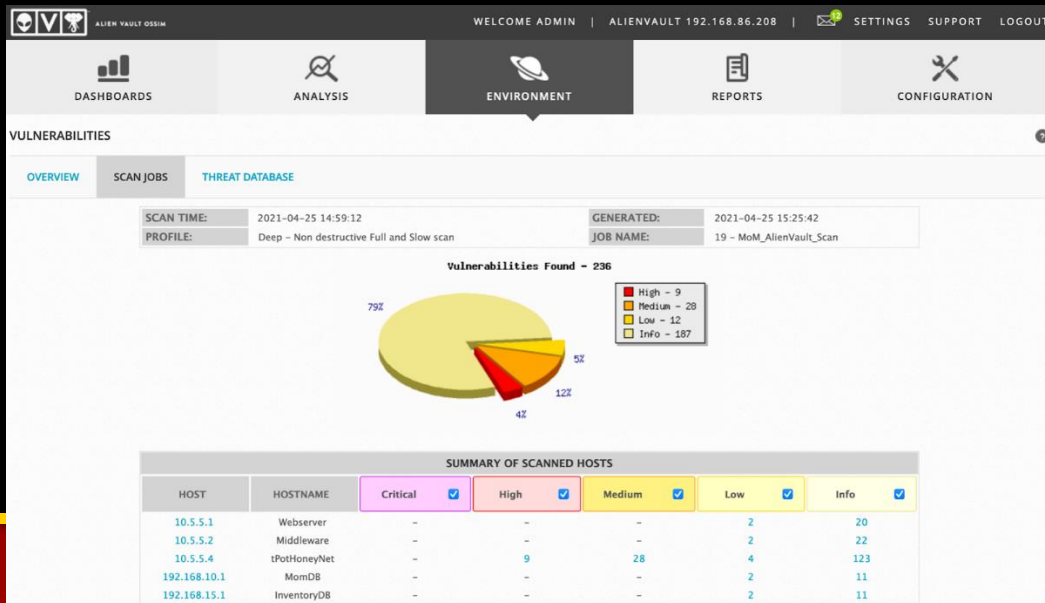


Risk Assessment/Vulnerability Analysis cont.

Pen Testing

AlienVault OSSIM

Scheduled internal scans to discover host vulnerabilities in our LAN & DMZ networks



Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

Pen Testing

Intruder

We scanned the site with a COTS web vulnerability scanner, producing the positive results from mediation of prior scans and diligence from the firewall team. Ironically, the 1 High alert was from our firewall / IDS blocking some scanning.

Differences Since Last Scan					
New Issues Discovered		Previous Issues Resolved		Direction of Travel	
Critical	0	Critical	0	↕	0
High	1	High	0	▲	1
Medium	4	Medium	0	▲	4
Low	3	Low	0	▲	3

Market of Mystery



Risk Assessment/Vulnerability Analysis cont.

Pen Testing

CWE Vulnerabilities

Vulnerabilities listed below we have accepted due to our HoneyPot implementation.

- > CWE-20

The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

- > CWE-693

The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product.

- > CWE-326

Inadequate Encryption Strength



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam

Challenge for 2nd Project



- 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.



Agenda

1400-1405 Introduction and Announcements

1405-1440 Poly Road Project Brief (and discussion)

1440-1515 Market of Mystery Brief (and discussion)

1515-1525 Break

1525-1540 Poly Road Demonstration

1540-1555 Market of Mystery Demonstration

1555-1630 Class Discussion

- Red-Team Hypotheses and Rebuttals

1630-1720 Review and Logistics for Final Exam



Final Exam

The Final exam for Data Science 526 will be held

Monday May 10th, 2021

2PM to 4PM Pacific Time

(I will also allow it to be taken from 6PM – 8PM upon request)

Online

Exam will be Open Book / Open Note

It will be taken Electronically

We will Discuss Logistics and Review
near the end of Lecture



Material for Final Exam

- The exam is comprehensive
 - But the emphasis will be on material since the mid-term exam.
- There will be at least one question related to one of the group projects.
 - Structured so that your answer will be about the parts of the group project that you contributed to the most.
- There will be a scenario question (hypothetical or from the news)
 - I will send all students the scenario to consider by Wednesday May 5th.

Selected Slides for Review



- This is not all the material you need to know, but it includes some of the slides from the semester that provide a framework for material that may be included.
- You should review ALL of:
 - The lecture slides
 - The readings linked from the lecture slides
 - Either as assigned for the future week, or as included in the current weeks discussion.
 - I suggest you download these to your computer for reference during the exam since you are not permitted to access the internet (other than for submission or asking questions of the instructor) during the time that you are taking the exam.
 - You may refer to any documents that you have downloaded, or physical notes in your possession.
 - Especially important will be the NIST documents that were discussed in lecture.



Course Outline

- Introduction to Secure System Administration
- Generation of Security Requirements
- NIST Best Practices – Linux System Administration
- Composition of systems and protection domains
- Configuration Management, System Updates
- Adversarial Security – Pen Testing – Red Teaming
- Virtualization and Cloud Security
- Incident Response Planning
- Network Administration
- Network Monitoring and Attack Forensics
- Security Incident Event Management
- Group Project Testing and Debrief
- Accreditation and acceptance testing

Introduction to Secure System Administration



- Secure
 - Ability to correctly implement relevant policy
- System
 - A computer?
 - A network?
 - The combination of all system components implementing a particular function
- Administration
 - Selection of components (purchases of products)
 - Architecture – how the pieces fit together
 - Installation and configuration
 - Security Testing
 - Operation
 - Monitoring
 - Repair and Maintenance
 - Threat response



Information Flow and Containment

- Understand your applications
Information Flow:
 - What is to be protected
 - Against which threats
 - Who needs to access which apps
 - From where must they access it
- Do all this before you invest in the latest products that salespeople will say will solve your problems.



System Administration

- What must be administered:
 - User accounts – Least Privilege
 - Software
 - Servers
 - Storage
 - Network (next slide)
 - Keys
 - Monitoring
 - Logs and Audit
- Core principles
 - Minimization



Network Administration

- Creation of network protection domains
 - Firewalls
 - VLANs
 - VPNs for access
 - Ipsec
 - Wireless Management
- Network Monitoring
- Network Admission Control

SIEM Monitoring - Forensics



- Network Attack Administration (SIEM)
- Network Monitoring and Attack Forensics

Accreditation and acceptance



-
- Determining when it is OK to bring your system live
 - Certification for government agencies
 - Periodic audits
 - Certification for customers or upstream parties
 - E.g. PCI Compliance

Administration vs Development



- Different stages in system life cycle
 - Administration is concerned with installation, interconnection, configuration, operation, and decommissioning
 - Administration is concerned with the environment
 - Development addresses the architecture of the system (or part of a system)
 - Depends on assumptions
- Security fails when environmental assumptions are violated.
 - Let's brainstorm on examples of such assumptions that led to security failures when they no longer held.



A Reasonable Outline(1)

- Motivation and Principles
 - Written altruistically, but in reality, the goals are to protect your organization.
 - Mentions Classes of Data and Consequences
 - E.g. Some Material from NIST Risk Management Framework
 - Acknowledgement of the threat environment
 - E.g. The Global System Environment (from GIACS)



A Reasonable Outline(1)

- Description of System (applicability)
 - Inventory: Systems, Devices, Data
- Motivation and Principles
 - Written altruistically, but in reality, the goals are to protect your organization.
 - Mentions Classes of Data and Consequences
 - E.g. Some Material from NIST Risk Management Framework
 - Acknowledgement of the threat environment
 - E.g. The Global System Environment (from GIACS)
- High level assignment of responsibilities



A Reasonable Outline(2)

- Security Requirements and Metrics
 - What is to be protected against what threats
 - Consequences to organization of breaches
 - Required level of protection to each class of asset
 - Required approaches to providing that protection
 - Metric regarding strength of mechanisms to be applied.
- Physical and Personnel Security Constraints
 - Who will have access
 - Access controls on physical systems

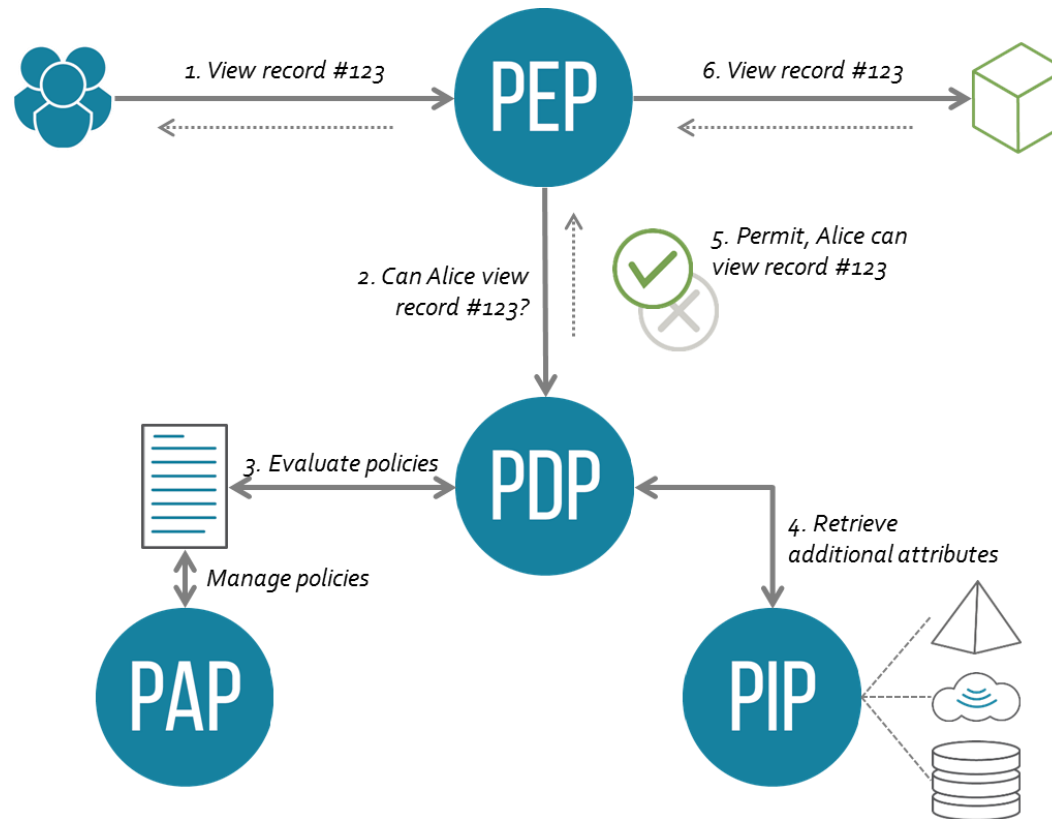


A Reasonable Outline(3)

- Requirements on Specific Categories of Controls
 - Access Control
 - Training
 - Audit
 - Configuration Management
 - Identity Management
 - Incident Response
 - Maintenance
 - Vendor Requirements
 - Media Protection
 - Personnel Security
 - Physical Protection
 - Risk Assessment
 - Security Assessment
 - Sys and Comm Protection
 - Integrity
 - Software Requirements



Points of Policy



- By Axiomatics - Axiomatics, CC BY 3.0, <https://commons.wikimedia.org/w/index.php?curid=48397652>



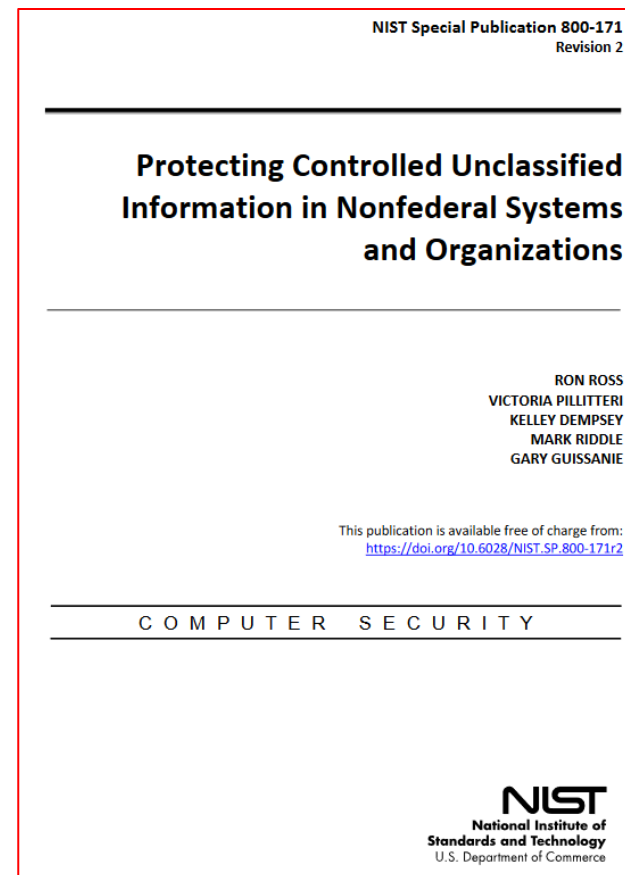
Network Administration

- Creation of network protection domains
 - Firewalls
 - VLANs
 - VPNs for access
 - Ipsec
- Define required characteristics
 - Where is encryption required
 - This is policy and administration

Reading for Next Week



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





Host Administration

Many security issues today are the result of poor system administration.

- Failure to implement least privilege
 - Poor management of user accounts
 - Mismanagement of remote access
 - Managing permissions incorrectly
 - Allowing vulnerable programs to run
 - Not keeping required programs up to date
 - Misconfiguration of applications
- Not just Linux, but many server machines are implemented on Linux, so that is our focus



Configuration Management

A process for consistently establishing and maintaining the characteristics of the components of a system relevant for the proper functioning of a system.

- Proper functioning includes:
 - Security
 - Updates and security patches.
 - Detection and prevention of unauthorized changes.
- Components includes all system assets:
 - Hardware
 - Software
 - Credentials
 - Licenses
- Characteristics includes:
 - Accounts
 - Settings
 - Policies.



Purpose of CM

- To Maintain Consistency of a system and its attributes with a technical baseline over the systems life.
- CM is part of system's security assurance cycle.
- Reduce the management workload for a collection of systems.
- Reduce the attack surface of a collection of systems by reducing the differences between individual systems within the collection.

Ethical Hacking Methodology





Response Planning

What are you responding to?

- All failures, security or reliability
- Some parts of the plan will be similar
- Other parts will depend on the nature of the failure

We start with Disaster Recovery

Then we move onto intrusion response

Secure Network Administration



- Secure Host Administration provides fine-grained control of access to a host's resources.
- Secure Network administration assists in controlling access at a coarse level of granularity
 - Not to records or files, but to computers and subnets.
 - At most, limits access to services (by port)
 - Confines access to zones
 - Is a second line of defense, and useful as stop-gap when vulnerabilities in host infrastructure are discovered.

Network Administration Guidance



- Manage access of devices to Network
 - See discussion earlier by Christopher Samayoa
- Use firewalls to contain access
 - Distributed Host Based may be okay and more effective for some environments – embedded even better.
 - Disallow by default
 - Open a flow only when defined by application/system architecture.
- VLAN's good, but unless enforced by network hardware or encryption, subverted hosts can circumvent.

Elements of Secure Network Administration



- Policy
 - Tells you what access is authorized
 - Should follow analysis of application information flow requirements.
 - Can also specify flows that are disallowed.
- Containment
 - Many tools to contain information.
 - Not all are effective.
 - Most available tools support DAC, but MAC is more effective.
- Monitoring
 - Important to discover unintended paths that are exploited
 - Important to discover insider threats



Network Containment Tools

- Firewall
 - Network, Host, Embedded, Application
- Virtual Private Network
 - Encrypted Tunnels between zones
- IPSec
 - Encryption and Integrity between hosts
- Virtual LANS
 - Layer 2 separation
- Encryption
 - Supports other forms of containment



Firewalls

- Network Based
 - Protects (or not) entire network. Chewy on inside.
 - Statefull vs stateless
 - Limited basis on which to make decisions.
 - Though some support deep packet inspection
- Host Based
 - Controls access to resources on single host
- Embedded
 - On interface card, but managed separately
- Distributed
 - Single policy (next) implemented at multiple PEP
- Application
 - No routing of packets, just recreation of application messages.
Examples: DNS, Web, Email – configuration.

Traditional Intrusion Detection System

- A device or software application that monitors a network or system for malicious activity and policy violations.
- In the past, Intrusion Detection systems were described as:
 - Network-based IDSs
 - Host-based IDSs
 - Distributed IDSs – sometimes described as Hybrid
- Today, all SIEM systems are distributed.

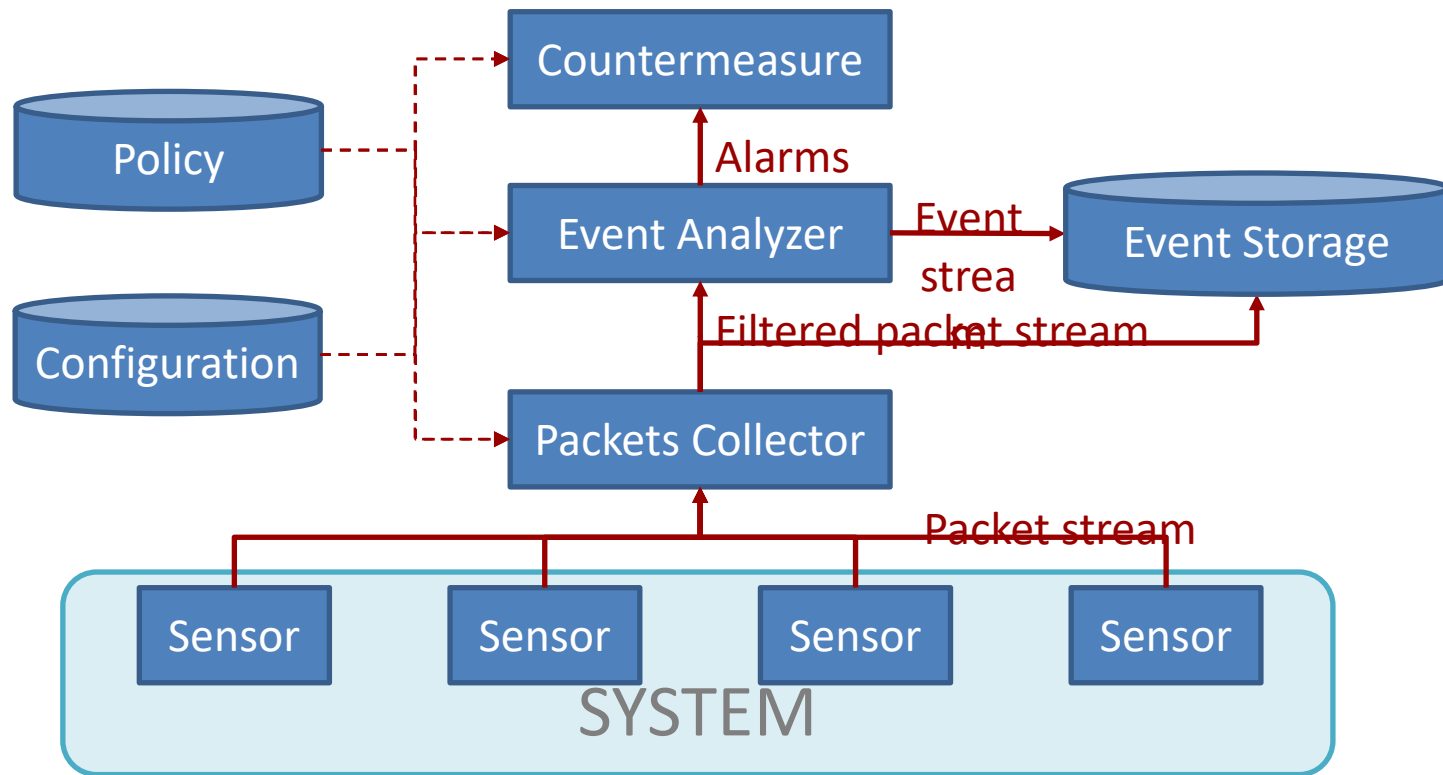
Traditional Network-based IDS



- Deploying sensors at strategic locations
 - E.G., Packet sniffing via *tcpdump* at routers
- Inspecting network traffic
 - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
 - Look into the data portions of the packets for malicious command sequences
- May be easily defeated by encryption
 - Data portions and some header information can be encrypted



Network-based IDS





Authorization Process: Accreditation

- Accreditation works in two ways within the authorization process
- 1. Accreditation of components or subsystems being bought requires less acceptance testing.
- 2. ATO is an accreditation. Once system receives ATO, it is accredited that all of the organization will recognize this system's ability to operate securely for a defined environment.

Accreditation and Acceptance Testing in Industry



- Industries also must perform some sort of testing on products they buy
- However, industries typically put more emphasis on functionality and availability than security (Microsoft acceptance testing example)
- Accreditation in industry is related to who a company will purchase from
- Acceptance Testing in industry used more as a way to validate a contract and provide payment



Accreditation in Industry

- Industries tend to buy from established companies that have proven to provide products that work
- Example: Microsoft Office
- However, this also applies to when companies need new software built for them.



Accreditation in Industry

- Software purchase agreements are made whenever a company is purchasing software.
- Accreditation comes into play in a couple of ways.
 1. Company might only be willing to buy software from an accredited source
 2. Company might give me leeway on a contract given to an accredited source (in how much acceptance testing is needed before

Acceptance Testing in Industry



- Companies often provide contracts to a different company to build something they need.
- Acceptance Testing is used to:
 - 1. Keep the company on contract on track
 - 2. Provide a concrete way to test the product, if it does not pass the tests the company won't get paid the full amount



Trust No-One

Zero-trust is not a specific technology, rather it is a justified application of paranoia, i.e that you cannot implicitly trust users, devices, or processes acting on behalf of users.

- You must reverify decisions on which access is based.
 - E.g. access to a network segment does not mean a device or packet is authorized, just because it made it past a firewall.
 - Authentication and access control to be applied on each access.
 - Plain-old network protection domains is not enough.
- Assume nothing

But in practice, we all trust something



Administering Zero Trust

- User Administration – Identity Management
 - Centralized administration – (trusted)
- Configuration Management
 - Devices
 - Assessing system health (you are trusting this)
 - Admission
 - Authentication / Attestation – (trust points)
 - Software – Trusted Computing – Attestation
- Network Administration
- SOC / SIEM
- Fine Grained Access Control
 - Least Privilege (least trust)

NIST 800-207



- A zero trust architecture (ZTA) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement. ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level. Many organizations already have elements of a ZTA in their enterprise infrastructure today. Organizations should seek to incrementally implement zero trust principles, process changes, and technology solutions that protect their data assets and business functions by use case.

Final Exam Summer 2016 Q1



1. Monitoring. (40 points)

- a) List the kinds of data and the sources for each kind of data that is useful in assessing the current state of security of a system. By system I am including all computers, software and network components that are used to provide a function or service. (15 points)
- b) Describe any technical issues you see with the ability to collect, and the coverage of (what is visible from) the data you described in part (a), and suggest ways to address the issues you identify. (15 points – answer on back of page)
- c) Describe any issues regarding the accuracy and authenticity of the data that you will be collecting as described in part (a). Which data is more vulnerable, and discuss steps you can take to provide greater confidence that you are observing the events that occur. (10 points)

Final Exam Summer 2016 Q2



2. Configuration Management and Virtualization (40 points)

Configuration management is an important function in the administration of computer systems.

- a) List items that are included in the term “configuration” that is being managed by an organization. (10 points)
- b) List the benefits that are recognized through effective configuration management. (15 points)
- c) Explain how virtualization might be used to facilitate better configuration management in a system. (10 points)
- d) Explain how the use of virtualization can make configuration management more difficult. (5 points)

Final Exam Summer 2016 Q3



3. Recovery and response plans (15 points)

a) Two steps among those in disaster recovery planning as described in lecture include

i) Determining the impact on the business (Business impact analysis BIA), and

ii) Identifying critical business functions.

Explain why these steps might be especially important for the definition of an intrusion response plan. (15 points)

b) In recent hacks of the Democratic National Committee's computer systems, discuss what steps might not have been properly defined or implemented in their recovery plan, for which such deficiency might have contributed to the subsequent breaches of the computer systems of the Hillary Clinton Campaign and the Democratic Congressional Campaign committees. (5 points)