

# Bug Bounty & Documentation

S2Day12Bug.md

[Closing Ceremony](#)

GTST - GeezTech Security Tester®

by Nathan Hailu



Recall

# Last class Topic



# Topic

1. What is Bug Bounty
2. How to do Bug bounty
3. Bug bounty Platform overview
4. How to hack on bug bounty
5. Report Writing and Documentation
6. What is the next Step on Cyber Security field
7. Protocols - Assignment Presentation



# What is Bug Bounty?

- The name Bug Bounty, came from two words “BUG” and “Bounty”.
  - Bug is a A problem that caused on the logic of the code.
    - This can be the way they handle errors, or some Misconfigurations
  - Bounty is a payment
- SO Bug bounty is a security expert Job, which is finding a Bug on some program and getting paid for the report of the bug.
- It is Started by a company called Netscape.



# History

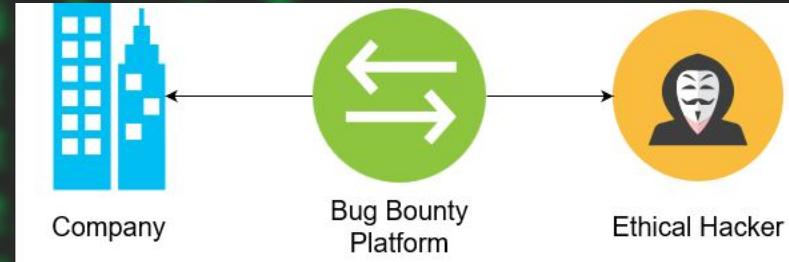
- Netscape is a browser software it, announced that if any user got any errors while using their browser software and if they report it , the company will pay them.
- Now a days, many websites,softwares are secured this is due to the involvement of Bug bounty programs.
- When a new company develop a platform, it will add it to a bug bounty program and many skilled security testers/hackers will try to get bug and report it, then that bug/vulnerability will be patched!
- The security researcher is called “Bug Bounty Hunter”/“Bug Hunter”



# What do you need ?

1. Programming language know-how
  - a. The Languages are based on the field you work(web or system hacking)
2. Hacking Skill
3. Tools
4. Patience
  - a. It is not simple As CTF, it is little bit hard to get vulnerabilities
5. Hard Working
  - a. Hackers try to get 1 website bug at least for a month
6. Always Learning mindset.

# Bug Bounty Platforms



- Bug Bounty Platforms are websites that help to connect the companies with the White Hat hackers AKA Security Researchers.
  - It will help to post any company websites to hack on
  - It will finish the payment between them.
  - It will validate if the report for the payment.
- There are a lot of bug bounty platforms, each with unique features.
- Example:
  - Hacker-One
  - Bug Crowd
  - Intigriti
  - Yes we Hack
  - Synack
  - ...
- Also some big companies have their own platforms that have registration for their products only.
- Lets see Hackerone...



# Hackerone

<https://www.hackerone.com/>

# hackerone

[SOLUTIONS](#)[PRODUCTS](#)[PARTNERS](#)[COMPANY](#)[HACKERS](#)[RESOURCES](#)[Login](#)[Contacted by a hacker?](#)[Contact Us](#)

## Peace of mind from security's greatest minds

Increase your resistance to attack by tapping the world's top ethical hackers. Understand your attack surface, hunt bugs, test apps, and fix vulnerabilities before anyone else knows they exist.

[How it Works](#)[Request a Demo](#)

Protecting the world's top innovators



Nintendo®



PayPal



HYATT

AT&T



## Hacktivity

See the latest hacker activity on HackerOne

Search Hacktivity

### Sort

Popular ▾ ▾

### Type

- All
- Bug Bounty
- Published
- Disclosed

### Filter

- Hackers I am following
- Collaborations

30		<a href="#">TikTok 2FA Bypass</a>	By amans to TikTok	Resolved	Medium	\$1,564.00	disclosed about 1 day ago
34		<a href="#">XSS at jamfpro.shopifycloud.com</a>	By kanthu to Shopify	Resolved	Medium	\$9,400.00	disclosed 2 days ago
13		<a href="#">Mystery with a leaked token and Reusability of email confirmation link leading to Account Takeover</a>	By gokulsk to Sorare	Resolved	Low	\$300.00	disclosed 21 hrs ago
40		<a href="#">Stored XSS in SVG file as data: url</a>	By irisrumtub to Shopify	Resolved	Medium	\$5,300.00	disclosed 4 days ago
5		<a href="#">CVE-2022-43551: Another HSTS bypass via IDN</a>	By kurohiro to Internet Bug Bounty	Resolved	Medium		disclosed 17 hrs ago
92		<a href="#">Github Apps can use Scoped-User-To-Server Tokens to Obtain Full Access to User's Projects in Project V2 GraphQL api</a>	By ahacker to GitHub	Resolved	High	\$20,000.00	disclosed 9 days ago
48		<a href="#">IDOR for changing privacy settings on any memories</a>	By mrhavit to TikTok	Resolved	High		disclosed 8 days ago
39		<a href="#">XSS at TikTok Ads Endpoint</a>	By s3c to TikTok	Resolved	High		disclosed 8 days ago
14		<a href="#">Stored XSS in Public Profile Reviews</a>	By vj1naruto to Judge.me	Resolved	None	\$250.00	disclosed 3 days ago
		<a href="#">Rails ActionView sanitize helper bypass leading to XSS using SVG tag</a>					

Programs Pentesters

## Directory

Find new hackable targets or contact information to report vulnerabilities you've already found.

 Search Directory

### Program features

- IBB ⓘ
- Offers bounties ⓘ
- High response efficiency ⓘ
- Managed by HackerOne ⓘ
- Offers retesting ⓘ
- Active program ⓘ
- Bounty splitting ⓘ

### Asset type

- Any
- CIDR
- Domain
- iOS: App Store ↗
- iOS: Testflight
- iOS: .ipa
- Android: Play Store ↗
- Android: .apk ↗
- Windows: Microsoft Store ↗
- Source code ↗
- Executable ↗
- Hardware/IoT ↗
- Other

Program	Launch date ↓	Reports resolved ↑	Bounties minimum ↑	Bounties average ↑	Star
 TD Bank Managed	01 / 2023	260	-	-	★
 S-Pankki Managed Retesting Bounty splitting	01 / 2023	81	\$150	\$300	★
 TRON DAO Retesting	01 / 2023	0	\$50	\$250-\$350	★
 Kiwi.com Managed Retesting	01 / 2023	177	\$100	\$200-\$256	★
 Hedera Hashgraph Managed Retesting Bounty splitting	01 / 2023	46	\$50	\$200-\$250	★
 Stanford University Managed	01 / 2023	1	-	-	★
 KKR-VDP Managed	01 / 2023	-	-	-	★
 8x8 Bounty Retesting Bounty splitting	01 / 2023	194	\$100	\$200-\$400	★
 McKesson Managed	01 / 2023	2	-	-	★

# Scope

Scope is the range u can hack on.

Scope can be in Bug type or Subdomain

There are two types:

1. In-scope: this is an included scope
2. Out-of-Scope: this is a place which you are not needed to hack.

Scopes			
In Scope			
Domain	online.s-pankki.fi	Critical	Eligible
	S-Bank netbank which provides netbank functionalities (accounts, payments, cards, loans, investments etc) to private customers.		
Domain	https://www.s-pankki.fi	Critical	Eligible
	S-bank public pages		
Domain	https://crosskey.io/stores/s-pankki/apis	Critical	Eligible
	S-Bank PSD2 interface.		
Domain	mobile.s-pankki.fi	Critical	Eligible
	S-mobile banking application interface.		
Domain	https://www.s-kaupat.fi/	Critical	Eligible
	S-Group online grocery store.		
	You do not need to have an account but to get access to all asset's functionality we prefer you create S-Kaupat account via "Kirjaudu" / "Log in".		
	In case you create S-Kaupat account please use info regarding HackerOne reference for example "firstname.lastname+ <a href="mailto:hackerone@mail.com">hackerone@mail.com</a> ". Notice that these S-Kaupat "HackerOne" accounts will be automatically removed after 6		

## Out-of-scope vulnerabilities

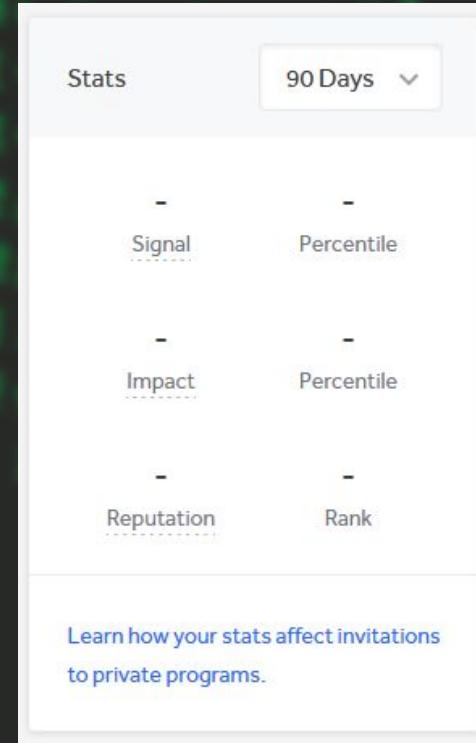
When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug.

The following issues are considered out of scope:

- Self-XSS and XSS without impact
- Clickjacking on pages with no sensitive actions
- Unauthenticated CSRF
- Attacks requiring MITM or physical access to a user's device
- Previously known vulnerable libraries without a working Proof of Concept
- Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS

# Profile

- ON any bug bounty program , you reports have to be valid as much as possible. If u do false things or invalid reports your, reputation will lower.
- Hacker1 also have a public and private programs the programs those are listed in directories are public programs. But as you reputation increases some companies will invite you for private hack.



# Reporting

## Submit Vulnerability Report

You're about to submit a report to U.S. Department Of Defense. Provide as much information as possible about the potential issue you have discovered. The more information you provide, the quicker U.S. Department Of Defense will be able to validate the issue.

By clicking "Submit Report," you are indicating that you have read, understand, and agree to the guidelines described in our [vulnerability disclosure policy](#) for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to DoD information systems, and consent to having the contents of the communication and follow-up communications stored on a U.S. Government information system.

1

**Weakness**  
Select the type of the potential issue you have discovered. Can't pick just one? Select the best match or submit a separate report for each distinct weakness.

Code Injection (CWE-94)  
Server-Side Request Forgery (SSRF) (CWE-918)  
SQL Injection (CWE-89)  
UI Redressing (Clickjacking) (CAPEC-103)  
Open Redirect (CWE-601)

Currently selected: None

Proof of Concept

2

**Proof of Concept**  
The proof of concept is the most important part of your report submission. Clear, reproducible steps will help us validate this issue as quickly as possible.

**Title\***  
A clear and concise title includes the type of vulnerability and the impacted asset.

**Description\***  
What is the vulnerability? In clear steps, how do you reproduce it?  
  
\*\*Description:\*\*  
  
## References  
  
Write Preview Parsed with Markdown

**Impact\***  
What security impact could an attacker achieve?  
  
Write Preview Parsed with Markdown

**Affected System Host(s)\***  
Prefer one entry per report. If multiple, please provide in a comma delimited format. Also, please only include the domain with the TLD and no protocol (http/https) or path beyond the domain name. (ex. www.foo.bar)

POC(proof of Concept): is a term given for showing a hacking step.

# Learning resources

- It also have a learning resource and web CTF's Prepared by hacker1 called "Hacker 101"

<https://www.hacker101.com/>

**h1** Announcements Getting Started Videos CTF Resources Discord



## LEARN TO HACK

Hacker101 is a free class for web security. Whether you're a programmer with an interest in bug bounties or a seasoned security professional, Hacker101 has something to teach you.

[Start Hacking!](#)

### Capture the Flag

Put your skills into practice with CTF levels inspired by the real world

[Check out CTF](#)

### Video Lessons

Learn to hack with our free video lessons, guides, and resources

[Explore free classes](#)

# Another Best Source



PortSwigger WebSecurity Academy.

Another Best Web Hacking Training Platform with Good Notes and Real World Labs.

<https://portswigger.net/web-security>



The screenshot shows the PortSwigger Web Security Academy homepage. At the top, there's a navigation bar with links for Dashboard, Learning path, Latest topics, All labs, Mystery labs, Hall of Fame, Get started, Get certified, and a LOGIN button. The main heading "Web Security Academy" is prominently displayed with a small flame icon. Below it, a sub-headline reads "Free, online web security training from the creators of Burp Suite". There are two large orange buttons: "Sign up" and "Login". At the bottom, there are three promotional sections: "Boost your career" (with a gear icon), "Flexible learning" (with a book icon), and "Learn from experts" (with a person icon). Each section includes a brief description and a link to "Produced by a world-class team - led by the author of The Web Application Hacker's Handbook".



# How to Hack on Bug Bounty Programs

- We still do same hacking steps.
- 1. Information Gathering
  - a. Use the methods we saw and try to understand the site.
  - b. Find Subdomains, Dont just hack on landing Page
- 2. Scanning
  - a. There are a lot of scanning types mainly on bug bounty you do subdomain enumerations.
  - b. This will increase our attack surface(the attacking scope)
- 3. Exploiting
  - a. Here you will use your web Hacking skill and test these Vulnerabilities on the subdomains you got.
  - b. This exploiting on Bug bounty is just used to test if there is vulnerability, we don't hack the site.
- 4. Reporting
- The other steps are not needed because We need to report ,not exploiting and taking advantage (they can be illegal).

# Subdomain enumeration tools

There are a lot of tools, for this purpose.

1. Amass:

```
(nathan㉿Nathan)-[~]
└─$ sudo apt install amass
[sudo] password for nathan:
Reading package lists... Done
```

2. Subfinder:

```
(nathan㉿Nathan)-[~]
└─$ sudo apt install subfinder
[sudo] password for nathan:
Reading package lists... Done
Building dependency tree... Done
```

Knockpy....

```
(nathan㉿Nathan)-[~]
└─$ amass enum -d example.com -o results.txt
example.com
www.example.com
```

```
(nathan㉿Nathan)-[~]
└─$ sudo subfinder -d insa.gov.et
```



projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions

[WRN] Developers assume no liability and are not responsible for any misuse or damage

[WRN] By using subfinder, you also agree to the terms of the APIs used.

```
└─$ sudo subfinder -d insa.gov.et
```

[projectdiscovery.io](http://projectdiscovery.io)

[WRN] Use with caution. You are responsible for your actions  
[WRN] Developers assume no liability and are not responsible for any misuse or damage.  
[WRN] By using subfinder, you also agree to the terms of the APIs used.

```
[INF] Enumerating subdomains for insa.gov.et
ethio-cer2t.insa.gov.et
www.rootca.insa.gov.et
signal.insa.gov.et
cds.insa.gov.et
sucp.insa.gov.et
insecocom.insa.gov.et
www.insa.gov.et
appointment.insa.gov.et
debo.insa.gov.et
```

inseccom.insa.gov.et  
www.insa.gov.et  
appointment.insa.gov.et  
debo.insa.gov.et  
exchangeserver.insa.gov.et  
mail.insa.gov.et  
www.ca.insa.gov.et  
www.iam.insa.gov.et  
smtp.cds.insa.gov.et  
erga.insa.gov.et  
www.cte.insa.gov.et  
www.ra.insa.gov.et  
testportal.insa.gov.et  
iam.insa.gov.et  
sdev.insa.gov.et  
smtp.sucp.insa.gov.et  
cychallenge.insa.gov.et  
crypto.insa.gov.et  
csam.insa.gov.et  
gmg.insa.gov.et  
ethiocert.insa.gov.et  
recruitment.insa.gov.et  
security.insa.gov.et  
skbs.insa.gov.et  
services.insa.gov.et  
elearning.insa.gov.et  
identity.insa.gov.et  
www.identity.insa.gov.et  
kbs.insa.gov.et  
cdev.insa.gov.et

<https://subdomainfinder.c99.nl>

# Subdomain Finder

Consider helping the project, check out our [Hall of Fame](#)

[07-01-2023 02:00AM UTC] We're currently maintaining our servers. The service may be unstable.

Domain (eg. example.com) [Start Scan](#)

**Private scan** *(This makes sure your scan will not be logged, published or indexed. Everything stays private.)*

Result of [insa.gov.et](https://subdomainfinder.c99.nl/scans/2023-02-04/insa.gov.et)  
<https://subdomainfinder.c99.nl/scans/2023-02-04/insa.gov.et>

Scan date: 2023-02-04 13:33:25  
Domain Country: Ethiopia (ET)   
Subdomains found: 29  
Most used IP: 196.188.171.243 (2x)

[Whois Check](#) [Check Status](#) [Copy to clipboard](#) [Download CSV](#) [Download JSON](#)

Subdomain	IP	Cloudflare
insa.gov.et	196.188.171.243	
www.insa.gov.et	196.188.171.243	
testportal.insa.gov.et	196.188.172.142	
ethiocert.insa.gov.et	213.55.96.13	
debo.insa.gov.et	196.188.171.246	
cychallenge.insa.gov.et	197.156.68.243	
elearning.insa.gov.et	196.188.172.131	
gmg.insa.gov.et	102.218.2.9	
mail.insa.gov.et	102.218.2.10	
iam.insa.gov.et	196.188.172.135	
www.iam.insa.gov.et	196.188.172.135	
crvoto.insa.gov.et	196.188.171.253	

Recent scans:

- insa.gov.et
- polarmods.com
- google.midtrans.com
- pnw.edu
- statueofliberty.org
- sellercenter.com
- studiodaily.com
- cbic.gov.in
- shope.net
- sellercenter.jumia.dz
- transformativeworks.org
- tokopedia.us
- cassovn
- rabbit.com
- now.jumia.dz
- wearego.com

# CMS(Content Management System)



- CMS is a software/framework that helps to build a website.
- This can make the website making journey simple, it is done by dragging and dropping.
- But some advanced features are not included.
- The most known CMS are Wordpress,Drupal,Joomla.
- It is not recommend beginners to hack on it because they are very updated and almost the simple vulnerabilities are already patched.
- BUT, if you saw a very old version of CMS then try to exploit it
- You can Get the Version and Type of CMS the website have, by using recon tools, like wappalyzer.



# CMS Pentest

- On CMS pentest, you focus more on Public Known Vulnerabilities and Misconfiguration rather than Bug on the CMS.
    - Because Finding New Vulnerability on the CMS means, Finding 0day Vulnerability.
  - As CMS Penetration Most of the time we do, Information Gathering about the System and Version, then we will Look for Exploits with that Specific Version CMS .
  - There are tools that can help us to Scan and enumerate the CMS's.
    - Wordpress - WPSCAN
    - Joomla - Joomscan
    - Drupal - Drupscale
  - These tools will enumerate the site for you.
  - In addition to the Misconfiguration, You will do manual Security check on the site, for Exposed data, Files rather than Deep Exploitation.

# Improving skill

- To have a Good Understanding on Concepts and to have Good Hacking skill, You can do the following.
  - All ways learn.
    - Sometimes it is the most overwhelming thing to learn always, but if you have a plan to be Good Bug Hunter 1 day, so be disciplined and keep learning.
  - Use Hacking Books.
    - There are Lot of Hacking Books, but specially the following are Good for understanding
      - Web Application Hackers Handbook
      - Web hacking 101
      - Real world Bug Hunting
      - Art of Exploitation
      - Practical Malware analysis
  - watch/read disclosed reports(POC - proof of Concept)
    - When you watch poc videos on youtube/ read poc from disclosed reports on hacker1 they will teach you a new way of attacking sites.
  - Follow Bug Hunters on social medias and use medium.com(app/site)
    - Bug hunters will share some hunting and exploiting techniques in their social media
    - Specially twitter is a Good Place.
    - Follow the hackers on Twitter, LinkedIn
  - Also begin with sites those are located in ethiopia, don't just start hacking on hacker1.
  - Don't waste your time by trying to hack a CMS website.





## Farah Hawa

@Farah\_Hawaa

noobiest of the noobs | content creator | SecOps @Bugcrowd | she/her | personal account

📍 Mumbai 🎵 youtube.com/c/farahhawa 📅 Joined March 2015

779 Following 32.4K Followers



## Jason Haddix

@jhaddix

Father, hacker, educator, gamer, & nerd. exCitrix, exRedspin, exFortify, exHP, exBugcrowd.

📍 Science & Technology 🌐 Colorado 🎵 jhaddix.com/links  
Born July 27 📅 Joined February 2009

7,090 Following 115.1K Followers

Followed by Mohsin Khan 🇮🇳, Sifat, and 24 others you follow



## Rana Khalil

@rana\_khalil

Pentester | OSCP | Youtube: [bit.ly/3o7lH0e](https://bit.ly/3o7lH0e) | Medium: [bit.ly/3pb2GuY](https://bit.ly/3pb2GuY) | HTB OSCP Preparation GitBook: [bit.ly/3qKFoMO](https://bit.ly/3qKFoMO) | Views are my own

📍 Ottawa, Canada 🎵 youtube.com/c/RanaKhalil101 📅 Joined March 2018

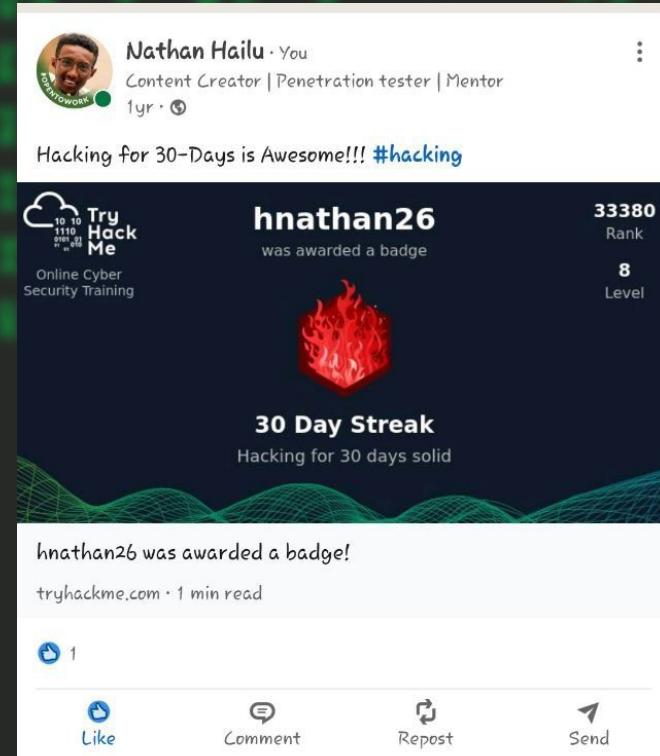
839 Following 34.7K Followers



NAHAMSEC

NAHAMSEC . COM

# Also Post your progress on Social Medias





**Nathan Hailu**

rexder26

It is just c0d4 n4m3 :) find me...

[Edit profile](#)

9 followers · 2 following

Geez Tech

Ethiopia

rexder26 / README.md



# Hi 🙌, I'm Natan Hailu



A Cyber Security Enthusiast and Content Creator.

- 💻 I'm currently working on **Web Penetration Testing**
- 📝 I'm currently learning **System Hacking**
- 🛠️ I'm looking to collaborate on **System hacking**
- ❤️ I'm looking for help with **OSCP, CEH, CBBH, CPTS**
- ✍️ I regularly Create Content on <https://www.youtube.com/@geeztech>
- 💬 Ask me about **Any Ethical Hacking Concepts**
- ✉️ How to reach me [natanhailu82@gmail.com](mailto:natanhailu82@gmail.com)
- ⚡ Fun fact I think am Funny and Serious at Same time

Connect with me:



Languages and Tools:



Certifications / Cyber-Security-Certificates-Note / HTB Certs / 7. Using The Metasploit Framework

## 7. Using The Metasploit Framework

### # Preface

- Why do we need to use Automation tools for vulnerability assessment
  - We dont have lot of time to pentest if the customer system uses lot of technologies
  - But it can make use tunnel vision ( If the tool cant do it , i cant too)

### Target

- On Metasploit we have targets, those are the OS and versions that the exploit work with, by default it is set by Automatic, but setting them to specific value can make our exploit to run properly.

### Payload

#### Staged

- it will call for the shellcode after exploiting because this will determine the system and download the shellcode and run it.
- it is like a medrek meri, it will go the stage and after seeing the program it will call the musician.
- it have / on metasploit.
- example:
  - windows/meterpreter/reverse\_tcp
    - this means the meterpreter will be sent and then the reverse\_tcp will go.
  - they are small in size

#### Encoders

```
msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=127.0.0.1
LPORT=4444 -b "\x00" -f perl -e x86/shikata_ga_nai
```

- to get the compatible encoders for a payload

```
msf6 exploit(windows/smb/ms17_010_永恒之蓝) > set payload 15
```

```
payload => windows/x64/meterpreter/reverse_tcp
```

Review: 0 note(s), 0 card(s) due Timer: Pomodoro (43166 minutes) 0 backlinks 492 words 3,179 characters

Today 680:35:25

Dec 2023 < TODAY >

SUN	MON	TUE	WED	THU	FRI	SAT
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

rexder26 Create 😊 Introduction to Active Directory.md

Preview Code Blame 63 lines (63 loc) • 6.35 KB Code 55% faster with GitHub Copilot

## Active Directory Overview

### Why Active Directory

- Active Directory (AD) is a directory
- It is a distributed, hierarchical structure of objects, such as users, groups, network devices, file shares, and more.
- AD is essentially a sizeable read-only database.
- A basic AD user account with proper security settings can be used to access resources on the network.

### Active Directory Functions

#### Structure

- A domain (forest) is a structure with multiple domains.
- It has many built-in organizational units (OUs).
- We can Create a Domain Browsing
- ![[Pasted image 202312010500]] But [copr.freightlogistics](#).

#### Terminology

#### Object

- An object can be defined as ANY type of entity, such as a user, group, or computer.

### GOBUSTER commands

```
for subdomains - for subdomain only: gobuster dns -d google.com -w ~/wordlists/subdomains.txt - for subdomain with ip: -i for directory - default: gobuster dir -u https://buffered.io -w ~/wordlists/shortlist.txt - for length: -l
```

- `gobuster dns -d inlanefreight.com -w /usr/share/SecLists/Discovery/DNS/namelist.txt`
- `whatweb --no-errors 10.10.10.0/24`

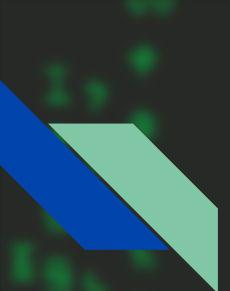
### awk tutorial = FOR filtering texts in column.

```
used to filter texts, it filters with default field separator "space"
```

- to print single column '{print \$column\_number}'
  - awk '{print \$1}' -> printing the 1st column, \$NF for last field
- to change the field separator -F "separator\_sign"
  - awk -F ":" '{print \$1}' -> the table is separated with : and printing the 1st column
- to add signs/space between two+ tables use "space/sign"
  - awk '{print \$1" "\$2}' -> we can use \t as tab, \n = new line between the " "
- if you want to use a pattern search awk can use pattern between '/'
  - awk '/^/ {print \$NF}' -> \$NF = Last field
- you can do bash scripting on awk
  - awk '{if(\$NF == "/bin/sh") print \$0}' file
- print the results if the first character is b or c
  - awk '\$1 ~ /^[b,c]/ {print \$0}' file

regex - start with = ^ - start with slash = ^/ - start with dot = ^.

'uniq' for removing duplicates , so use 'sort -u' this will sort and remove dups too



# Report Writing & Documentations

- After all of our Vulnerability Assessment, Red team Penetration Test or Blue Team Analysis we finally Do a Report As An Ethical hackers.
- This Report is the main thing that will be Delivered to our clients, to patch their system or to let them see their Vulnerable Side.
- Lets See How you will Write Your Good Report.



# Documentation

- When You do the Analysis/Pentest at first Place, Always Try to take notes on everything you found.(try to practice in CTF's you play)
  - The Credentials you found(username,password,tokens,id)
  - URLs/endpoints
  - Subdomains
  - Weird Behaviours
  - Scan results
    - IP
    - Subnets
    - Ports
  - Log files
  - Error Displays
  - Some Sensitive text Files
  - Commands and tools Used.
- You can use any Software you like to handle your notes.(Cherry Tree, Obsidian, Vscode, nano)

## Hack-Report-Template

1 Reference: 🔥 Rex Bug Hunting Methodologies 💀.

2 URL:

### 1. Recon Tasks

3 Subdomains enumeration

- 4  subfinder
- 5  findomain
- 6  websites
  - 7  virusTotal
  - 8  subdomainfinder
  - 9  dnsdumpster
- 10  amass - optional
- 11  assetfinder

12 DNS

- 13  dnseenum
- 14  dnsrecon
- 15  ldns-walk

16 IP Gather

- 17  Censys
- 18  Shodan
- 19  Securitytrials
- 20  fofa

## Information Gathered

Title: [YourTitle]

### Scope

- IP
  - [yourIPs]
- URL
  - [YourURLs]

### System Information

- OS:
  - [Your]
- Open Ports:
  - [Your]
- Server(+version):
  - [Your]

### Software Information

- Frameworks
  - [YourFrameworks]
- Plugins
  - [YourPlugins]



# Report Writing

- Report Writing is the last and Very Essential Phase as an Ethical Hackers( Security Analyst).
- On this Stage you will Convert your Documentation into Reports,
- **THIS WHAT THE CLIENT NEED, you are paid for this Document**
- Things Your Report have to have:
  - a. **Executive Summary**: Provide a high-level overview of the report
  - b. **Introduction**: Set the context for the report by explaining the scope and purpose of the assessment, including the systems, networks, or applications under review.
  - c. **Methodology**: Detail the techniques, tools, and procedures employed during the assessment.
  - d. **Findings**: Present a detailed analysis of the vulnerabilities, weaknesses, and security gaps identified during the assessment. Categorize the findings based on severity and potential impact. Include evidence and supporting documentation, such as screenshots or log extracts, to substantiate the findings.
  - e. **Risk Assessment**: Evaluate the identified vulnerabilities and weaknesses in terms of their potential impact on the organization's assets, operations, and reputation. Assign a risk rating or score to each finding to prioritize remediation efforts.( CVSS can help here)
  - f. **Recommendations**: Provide actionable recommendations to address each identified vulnerability or weakness.
  - g. **Conclusion**: Summarize the key findings, risks, and recommendations from the report. Emphasize the importance of proactive security measures and continuous improvement to protect the organization's assets.
  - h. **Appendices**: Include any additional information that supports the report, such as technical details, raw scan outputs, or any relevant legal or compliance requirements.

## 3 Executive Summary

TODO Customer Ltd. ("TODO Customer" herein) contracted TODO Candidate Name Network Penetration Test of TODO Customer's externally facing network to identify weaknesses, determine the impact to TODO Customer, document all findings in a clear and concise manner, and provide remediation recommendations.

### 3.1 Approach

TODO Candidate Name performed testing under a "Black Box" approach from , to without or any advance knowledge of TODO Customer's externally facing environment without identifying unknown weaknesses. Testing was performed from a non-evasive standpoint of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from TODO Candidate Name's assessment labs. Each weakness identified was identified and manually investigated to determine exploitation possibilities and escalation potential. Candidate Name sought to demonstrate the full impact of every vulnerability, up to internal domain compromise. If TODO Candidate Name were able to gain a foothold in the network, TODO Customer as a result of external network testing, TODO Customer allowed testing including lateral movement and horizontal/vertical privilege escalation to determine the impact of an internal network compromise.

### 3.2 Scope

The scope of this assessment was one external IP address, two internal network ranges, and the INSERT DOMAIN NAME Active Directory domain, and any other Active Directory domains that TODO Customer discovered if internal network access were achieved.

### In Scope Assets

Host/URL/IP Address	Description
TODO 10.129.X.X	TODO
172.16.139.0/24	TODO Customer internal network
172.16.210.0/24	TODO Customer internal network
TODO	TODO Customer internal AD domain
TODO other discovered internal domain(s)	TODO

## Creative way to Showcase your App

Lorum ipsum dolor sit amet, consectetur adipiscing elit. Temporibus commoc, voluptate quaeor lune quidem expedito eas a blanditibus sint modi est error verum facere eum at doloribus amet, nobis ut.



## Vulnerability

13-07-2023

Natan Hailu  
- Security Tester  
Phone Number: +251920047396  
Email: [nathanhailu82@gmail.com](mailto:nathanhailu82@gmail.com)  
Twitter: @hnathan26

### Summary

The Vulnerabilities I Got on Your System are high in Severity, If Some Unethical Security Persons Got this the damage would be Extremely Dangerous. Technical the Bug is Called "User Account TakeOver".

### Goals

1. Get SuccessFull Account Password reset Response
2. Try to change to Another user password

### Vulnerability Description ( Reproduction Steps - PoC )

#### I.Getting Orginal Success Result

- Goto the forgot password endpoint (<https://customer.com/forgotPassword>) and try with your real account.
- Here you will get the success response from the server as the following

```
{"success": "Success"}
```

## Table of Contents

<b>1 Document Control .....</b>	<b>4</b>
1.1 Team .....	4
1.2 List of Changes .....	4
<b>2 Executive Summary .....</b>	<b>5</b>
2.1 Overview .....	5
2.2 Identified Vulnerabilities .....	5
<b>3 Methodology .....</b>	<b>7</b>
3.1 Objective .....	7
3.2 Scope .....	7
3.3 User Accounts and Permissions .....	7
<b>4 Findings .....</b>	<b>1</b>
C1: Outdated System .....	1
H1: Directory Listing .....	1
H2: Blog Author User Infomation Disclosure .....	1
M1: Error page path disclosure .....	1
L1: Excessive Tenders data Exposure .....	1
<b>5 Disclaimer .....</b>	<b>2</b>
<b>A Appendix .....</b>	<b>2</b>
A.1 Words .....	2

## 2.2 Identified Vulnerabilities

#	CVSS	Description	Page
C1	9.8	Outdated System	8
H1	8.2	Directory Listing	10
H2	7.7	Blog Author User Infomation Disclosure	13
M1	6.3	Error page path disclosure	16
L1	3.7	Excessive Tenders data Exposure	18

### Vulnerability Overview

In the course of this penetration test **1 Critical**, **2 High**, **1 Medium** and **1 Low** vulnerabilities were identified:

## 3 Methodology

I Tried To examine all the functionality of the website, also Directories teh webserver accessing through Directory Bruteforcing.

### 3.1 Objective

The penetration testing engagement is to assess the security posture of the target system by identifying vulnerabilities and weaknesses that could potentially be exploited by malicious actors. Through a systematic and controlled approach, the objective is to simulate real-world attack scenarios and evaluate the effectiveness of existing security controls. The ultimate goal is to provide the client with actionable recommendations and insights to enhance their overall security defenses, mitigate risks, and protect their critical assets from potential threats.

### 3.2 Scope

The engagement began on **Feb 26, 2024** and concluded on **Feb 29, 2024**. The time taken to complete the assessment and deliver the final report was **1 Week**. The assessment focused on identifying vulnerabilities, weaknesses, and potential avenues for unauthorized access within the defined scope. It is important to note that the assessment was conducted within the agreed-upon boundaries and did not include any activities that could cause disruption or damage to the target systems.

#### Scope

System	Description
http://[REDACTED]	main domain

### 3.3 User Accounts and Permissions

#### Enumerated Users

- Yafet: [REDACTED]@m... negatu...ct
- Getane: [REDACTED]@m... negatu...ct

## 4 Findings

### C1: Outdated System

Score	9.8 (Critical)
Vector string	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Target	www. 
References	<a href="https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT01_2023-Outdated_Software">https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT01_2023-Outdated_Software</a>

#### Overview

The Website is using Joomla CMS, that is very old and outdated, it is using Joomla 1.5. the Current Version is Joomla 4.4.3.

#### Details

Outdated software can lead to a variety of different vulnerabilities, ranging from vulnerabilities with a low criticality to vulnerabilities causing compromization of the entire system. The severity and amount of these vulnerabilities in an outdated software system depends on the individual case. Usually, they rise with time as more and more vulnerabilities are found

#### Proof of Concept

- This Specific Version of Joomla(1.5) have a lot of CVE Reports, I was trying them, But some How they werent working, this means they are not working now but after some time an attacker can craft a very good Exploit for this Vulnerability and Do Very High Damanges From XSS upto Remote Code execution .

[+] Detecting Joomla Version  
[+] Joomla 1.5

[+] Core Joomla Vulnerability  
[+] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution  
EDB : <https://www.exploit-db.com/exploits/4212/>

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection  
CVE : CVE-2007-4781  
EDB : <https://www.exploit-db.com/exploits/4350/>

Joomla! 1.5.x - (Token) Remote Admin Change Password  
CVE : CVE-2008-3681  
EDB : <https://www.exploit-db.com/exploits/6234/>

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure  
CVE : CVE-2011-4909  
EDB : <https://www.exploit-db.com/exploits/33061/>

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting  
EDB : <https://www.exploit-db.com/exploits/33378/>

Joomla! 1.5.12 - read/exec Remote files  
EDB : <https://www.exploit-db.com/exploits/11263/>

Joomla! 1.5.12 - connect back Exploit  
EDB : <https://www.exploit-db.com/exploits/11262/>

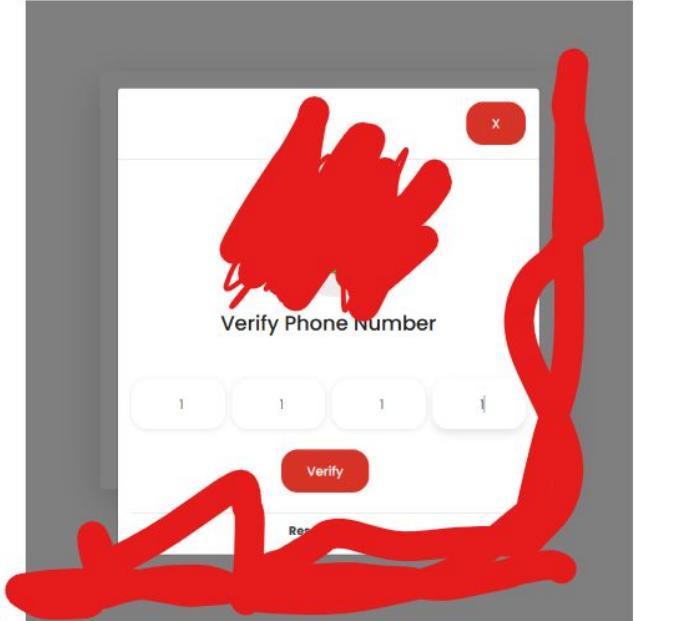
Joomla! Plugin 'tinybrowswer' 1.5.12 - Arbitrary File Upload / Code Execution (Metasploit)  
CVE : CVE-2011-4908  
EDB : <https://www.exploit-db.com/exploits/9926/>

Joomla! 1.5 - URL Redirecting  
EDB : <https://www.exploit-db.com/exploits/14722/>

Joomla! 1.5.x - SQL Error Information Disclosure  
EDB : <https://www.exploit-db.com/exploits/34955/>

#### Recommendation

It is recommended to keep all software components, including libraries and similar, on an up-to-date, stable and supported version. Every software and its components should be regularly checked for updates and new patches. It is recommended to implement an update management process to ensure no components are missed, and the checks are in time.



Now i will use Some web request interceptors(i used tool called burpsuite) and i will alter the response, before passing it to my browser. This works because as i told you it do client side validation.

#### ORIGINAL RESPONSE

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 13 Jul 2023 12:41:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Set-Cookie: csrf_cookie_name=40e8af6fc505b5c80ae827e6ac057ca1
   Max-Age=7200; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Set-Cookie: ci_session=e032uuumbms937rafinnsvq5lbjd763a; expi
   path=/; HttpOnly
9 Content-Length: 26
0 Connection: close
1 Content-Type: text/html; charset=UTF-8
2
3
4 {"error": "Incorrect OTP"}
```

#### - CHANGED RESPONSE

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 13 Jul 2023 12:41:49 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Set-Cookie: csrf_cookie_name=40e8af6fc505b5c8
   Max-Age=7200; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-reval
7 Pragma: no-cache
8 Set-Cookie: ci_session=e032uuumbms937rafinnsv
   path=/; HttpOnly
9 Content-Length: 26
0 Connection: close
1 Content-Type: text/html; charset=UTF-8
2
3
4 {"success": "Success"}
```

# Tools for Reporting

- There are some tools that can help you on Your reporting, they will Generate a report based on template you gave, you just need to add your documented informations and findings.

- Plextrac
- SysReptor
- WriteHat
- ...



The screenshot shows the SysReptor homepage. At the top, there's a green header with the text "SYSREPTOR" in large white letters and "Pentest Reports. Easy as Pie." below it. To the right is a cartoon illustration of a green Tyrannosaurus Rex wearing a white hard hat and holding a wrench. Below the header, a dark banner contains the text "Easy and customisable pentest report creator based on simple web technologies." followed by social media links for GitHub, LinkedIn, and Twitter, and a "Follow @sysreptor" button. Underneath the banner is a navigation bar with links to "Playground", "Ideas", "Questions", "Documentation", "Features and Pricing", "Installation", and "Buy SysReptor". A descriptive paragraph at the bottom explains that SysReptor is a fully customisable, offensive security reporting solution designed for pentesters, red teamers, and other security-related people, allowing them to create designs based on simple HTML and CSS, write their reports in user-friendly Markdown, and convert them to PDF with a single click, either in the cloud or self-hosted.



The screenshot shows the WriteHat homepage. It features a large, stylized logo where the letter 'H' in "WriteHat" is replaced by a white fedora hat icon. Below the logo, the text "Hack your reporting chain." is displayed in a smaller, sans-serif font. The background is black.



# What is the next Step on Cyber Sec?

- On This Stage, You have learnt Most Fundamental Cyber Security Concepts and Fields, Except Android, Cloud, Hardware, IoT Penetrations.
- You can Work/Hack with the Skills You have, You just need Practice and Experience.
- So To list out the Fields We learnt
  - Network penetration
  - System Penetration
  - Web penetration
  - Malware Analysis
  - Log Analysis
  - Blue Team Fields
  - Reverse Engineering
- So... From now on you will Choose the fields We saw in highlight and you will Learn more you will Practice do more CTF's on them and you can Sharpen Your Cyber Security Career and Future
  - You can Create Telegram groups and you can help each other, with the majors you choose.
- But in addition to the Job world, you might need some Skill Provings/ Certificates/Degree

...

- At this stage, You have taken all the GTST course based on the CEHv11.
- Now, you need to practice and Have a clear understanding on the concepts we covered.

## Course Outline

### 20 Modules That Help You Master the Foundations of Ethical Hacking and Prepare to Take the C|EH Certification Exam

#### Introduction to Ethical Hacking

Cover the fundamentals of key issues in the information security field, including the basics of ethical hacking, information security relevant laws, and standard procedures.

#### Foot Printing and Reconnaissance

Learn how to use the latest techniques and tools to perform footprinting and reconnaissance, a critical pre-attack phase of the hacking process.

#### Scanning Networks

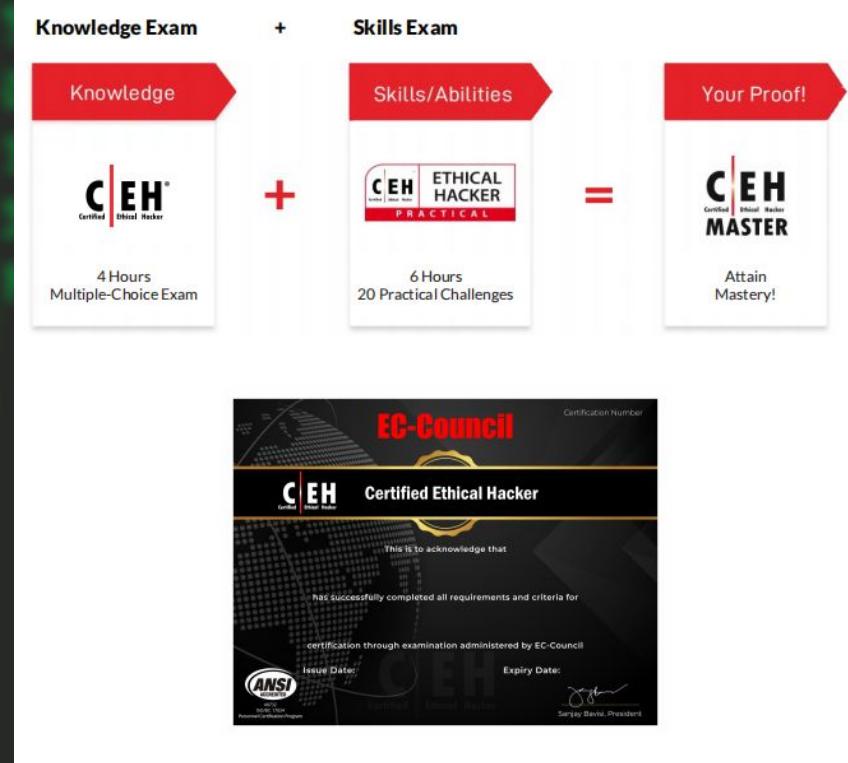
Learn different network scanning techniques and countermeasures.

#### Enumeration

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, and countermeasures.

LEARN	
<b>Module 05</b>	<b>Vulnerability Analysis</b> Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools.
<b>Module 06</b>	<b>System Hacking</b> Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.
<b>Module 07</b>	<b>Malware Threats</b> Learn different types of malware (Trojan, virus, worms, etc.), APT and fileless malware, malware analysis procedure, and malware countermeasures.
<b>Module 08</b>	<b>Sniffing</b> Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.
<b>Module 09</b>	<b>Social Engineering</b> Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
<b>Module 10</b>	<b>Denial-of-Service</b> Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
<b>Module 11</b>	<b>Session Hijacking</b> Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
<b>Module 13</b>	<b>Hacking Web Servers</b> Learn about web server attacks, including a comprehensive methodology used to audit vulnerabilities in web server infrastructure and countermeasures.
C EH v12	www.eccouncil.org/ceh
<b>Module 14</b>	<b>Hacking Web Applications</b> Learn about web application attacks, including a comprehensive methodology used to audit vulnerabilities in web applications and countermeasures.
<b>Module 15</b>	<b>SQL Injection</b> Learn about SQL injection attacks, evasion techniques, and SQL injection countermeasures.
<b>Module 16</b>	<b>Hacking Wireless Networks</b> Understand different types of wireless technologies, including encryption, threats, hacking methodologies, hacking tools, wireless security tools, and countermeasures.
<b>Module 17</b>	<b>Hacking Mobile Platforms</b> Learn mobile platform attack vector, android and iOS hacking, device management, mobile security guidelines, and security countermeasures.
<b>Module 18</b>	<b>IoT and OT Hacking</b> Learn different types of IoT and OT attacks, hacking methodologies, hacking tools, and countermeasures.
<b>Module 19</b>	<b>Cloud Computing</b> Learn different cloud computing concepts, such as containerization and server less computing, various cloud computing threats, hacking methodology, and cloud security techniques and tools.

- From Now on you can do any cyber security consulting, Bug bounty as a partime job
- Also if you need to be a professional Cyber Security expert, you have the know-how you just need to dig a little big and take the exam for certifications.
- You can learn master's degrees on some universities too.
- Certificates
  - CEH - it is expensive(92,056birr) - Now OLD
  - eJPT - 10,836birr
  - OSCP- 81,220birr
  - CompTIA(pentest+) - 20,643birr
  - HTB CPTS/CBBH/CDSA - 25,000birr
  - A+, Security+ are more theoretical
  - CISSP - is for Cyber Bosses



# Presentation Time.

- You will Share your slide on the screen, Try to Teach us about the protocol You Assigned.
- You have 10 mins
- We might have Questions
- Audiences
  - Take Notes
  - Learn From things they teach these protocols are protocols you will face on the cyber world

**GTSTv1 Is Completed Officially!** 🔥

Hope it was Fun

# Assessment Questions.

- There are 60 questions from our 2 month Class - 1:30 allowed
  - Includes from linux->bug bounty
- This will help you to test and know how much thing you have gathered from this course and helps me to know how much impactful i am.
- As a reward if you got greater 30% and total point of 60% above you will have a course completion certificate
  - “Geez Tech Security Testers Certificate”

