



**EncryptEdge Labs**

# **Cybersecurity Analyst Internship**

## **Task Report**

atalmamun@gmail.com

Task No: 29



Copyright © 2024 EncryptEdge Labs. All rights reserved

Credit: Offensive Security



## Table of Contents

<b>1.0 EncryptEdge Labs Internship Task Report</b>	<b>3</b>
<i>1.1 Introduction</i>	3
<i>1.2 Objective</i>	3
<i>1.3 Requirements</i>	4
<b>2.0 Phase 1: Incident Response Execution</b>	<b>4</b>
<i>2.1 Incident Handling Fundamentals</i>	5
<i>2.2 Responding to Remote System Attacks</i>	5
<i>2.3 Malware Incident Response Exercise</i>	6
<i>2.4 Perimeter Compromise Simulation</i>	6
<i>2.5 Independent Malware Incident Challenge</i>	7
<b>3.0 Phase 2 – CVE Analysis and Remediation</b>	<b>7</b>
<i>3.1 Overview of CVEs</i>	8
<i>3.2 WinRAR Vulnerability – CVE-2023-38831</i>	8
<i>3.3 Windows Search Exploit – CVE-2023-36884</i>	9
<i>3.4 Log4Shell Vulnerability – CVE-2021-44228</i>	9
<i>3.5 PrintNightmare Exploit – CVE-2021-34527</i>	10
<i>3.6 Detecting Ransomware Variants (REvil)</i>	10
<b>4.0 Phase 3 – Integrated Incident Simulation and Reporting</b>	<b>11</b>
<i>4.1 Comprehensive Incident Simulation</i>	11
<i>4.2 Final CVE Review and Proactive Measures</i>	13
<b>5.0 Lab Completion Screenshots: Proof of Completion</b>	<b>14</b>
<i>5.1 Incident Response</i>	14
<i>5.2 CVEs and Emerging Threats</i>	20



## 1.0 EncryptEdge Labs Internship Task Report

### 1.1 Introduction

The Capstone Project titled “*Integrated Incident Response and Emerging Threats Defense*” is designed to demonstrate practical knowledge and hands-on skills acquired throughout the cybersecurity internship program. This project simulates real-world cyber incidents and requires a complete incident response cycle, from detection to recovery. It also includes the identification and mitigation of emerging threats through the analysis of recent Common Vulnerabilities and Exposures (CVEs). By engaging with a series of guided labs and simulations, the project emphasizes critical thinking, technical investigation, and professional reporting—core skills for any cybersecurity analyst.

### 1.2 Objective

The primary objective of this capstone project is to provide hands-on experience in:

- Executing full-cycle incident response (IR) processes including identification, containment, eradication, and recovery.
- Investigating and mitigating known vulnerabilities using up-to-date CVE data.
- Strengthening detection and prevention strategies to minimize the risk of future cyber threats.
- Developing clear, actionable, and professional documentation of cybersecurity incidents and mitigation strategies.



### **1.3 Requirements**

To successfully complete the capstone project, the following requirements must be met:

- Completion of all assigned modules in the RangeForce platform, covering both incident response and CVE-based threat mitigation.
- Accurate documentation of each exercise, including indicators of compromise (IoCs), detection and containment steps, tools used, and strategic recommendations.
- Submission of a comprehensive incident simulation report and CVE defense summary.
- Inclusion of screenshots as proof of lab completions and key milestones.
- Use of appropriate tools such as a text editor or word processor for reporting and a screenshot tool to capture evidence of task execution.

### **2.0 Phase 1: Incident Response Execution**

This phase focuses on applying fundamental and advanced incident response (IR) techniques through interactive lab modules. Each task simulates a real-world security incident and provides hands-on experience with detection, containment, eradication, and recovery processes. Documentation of each exercise includes the use of tools, identified Indicators of Compromise (IoCs), and recommended mitigation strategies.



## 2.1 Incident Handling Fundamentals

### **Objective:**

To understand the full incident response lifecycle, including the key stages: identification, detection, containment, eradication, recovery, and post-incident reporting.

### **Activity Summary:**

I completed the “**Incident Handling**” module in the RangeForce platform. This foundational lab introduced the theoretical and practical aspects of handling incidents effectively in an enterprise environment.

### **Deliverable – Summary:**

The incident response lifecycle is a structured approach to managing cybersecurity incidents. The **detection phase** involves identifying unusual or malicious activity through alerts and log analysis. **Containment** limits the spread of an attack by isolating affected systems. **Eradication** focuses on removing the threat from the environment, and **recovery** ensures that systems are restored to normal operations securely. Post-incident activities involve documenting lessons learned and improving response plans for future incidents.

## 2.2 Responding to Remote System Attacks

### **Objective:**

To detect and respond to an unauthorized remote system attack using appropriate tools and methodologies.

### **Activity Summary:**

I completed the “**Remote System Attacks**” module. The lab simulated a scenario where an attacker gained unauthorized access to a remote system. I was tasked with identifying the indicators of compromise and containing the threat.

### **Deliverable – Summary:**

During the lab, I detected IoCs such as unusual login attempts, command execution via reverse shells, and suspicious network traffic. I used command-line tools and log analysis to identify the compromised host and isolate it from the network. Containment



actions included disabling affected user accounts and blocking the attacker's IP address at the firewall. A key lesson learned was the importance of monitoring remote access logs and setting up alerts for anomalous behavior.

### 2.3 Malware Incident Response Exercise

**Objective:**

To investigate and neutralize a malware infection, documenting detection methods, IoCs, and containment techniques.

**Activity Summary:**

I completed the "**Malware Incident Response Exercise**" module. The lab involved analyzing a compromised host suspected of malware infection and taking necessary actions to eliminate the threat.

**Deliverable – Summary:**

I identified malware-related IoCs such as rogue processes, registry modifications, and persistence mechanisms. Tools like process monitors and antivirus scanners were used for detection. I terminated malicious processes and removed registry entries to contain the infection. Mitigation strategies included deploying endpoint protection software, conducting system-wide scans, and ensuring regular patch management. In a corporate setting, user education and strict email filtering would help prevent such incidents.

### 2.4 Perimeter Compromise Simulation

**Objective:**

To detect and defend against a perimeter breach, followed by implementing stronger security controls.

**Activity Summary:**

I completed the "**Perimeter Compromise Challenge**" module. This simulated an attack on the network perimeter, where vulnerabilities in external services were exploited.



### **Deliverable – Summary:**

The initial detection involved observing failed login attempts and port scans. I used firewall logs and intrusion detection system (IDS) alerts to identify the attack vector. The containment involved blocking suspicious IPs and tightening firewall rules. Post-event, I recommended updating perimeter device firmware, applying network segmentation, and configuring intrusion prevention systems (IPS) to monitor traffic proactively.

## **2.5 Independent Malware Incident Challenge**

### **Objective:**

To apply incident response skills independently in a complex malware attack scenario.

### **Activity Summary:**

I completed the “**Malware Incident Response Challenge**” module without step-by-step guidance, simulating a real-world independent response scenario.

### **Deliverable – Summary:**

IoCs identified included command-and-control (C2) traffic, unauthorized scheduled tasks, and modified system files. I contained the malware by isolating the system, eradicating malware artifacts, and restoring clean configurations. The main challenge was pinpointing the malware’s persistence mechanism, which I overcame by analyzing startup scripts and scheduled tasks. This exercise reinforced the importance of thorough system inspection and using layered defenses.

## **3.0 Phase 2 – CVE Analysis and Remediation**

This phase focuses on identifying, analyzing, and mitigating real-world vulnerabilities (CVEs) affecting widely used software and operating systems. Each module highlights a specific vulnerability, its impact, and appropriate remediation techniques. Through hands-on exercises, I learned how to assess risks, detect exploits, and implement long-term mitigation strategies in alignment with security best practices.



### **3.1 Overview of CVEs**

#### **Objective:**

To understand the purpose and structure of CVEs and the importance of CVSS scores in assessing vulnerability severity.

#### **Activity Summary:**

I completed the “**CVE Overview**” module in RangeForce. The module explained how CVEs are documented, categorized, and scored using the Common Vulnerability Scoring System (CVSS).

#### **Deliverable – Summary:**

The CVSS rating system evaluates vulnerabilities based on several factors, including access complexity, required privileges, and potential impact on confidentiality, integrity, and availability. Scores range from 0.0 (low severity) to 10.0 (critical). High and critical vulnerabilities require immediate attention as they can be exploited remotely or lead to system compromise without user interaction.

### **3.2 WinRAR Vulnerability – CVE-2023-38831**

#### **Objective:**

To analyze and mitigate a critical vulnerability in WinRAR that allows arbitrary code execution.

#### **Activity Summary:**

I completed the “**CVE-2023-38831 WinRAR - Arbitrary Code Execution**” module. This vulnerability allows attackers to craft malicious archive files that execute hidden payloads when opened.

#### **Deliverable – Summary:**

I analyzed the exploit by inspecting the behavior of specially crafted .RAR files. The detection involved monitoring file execution paths and identifying embedded scripts. Mitigation steps included updating WinRAR to the latest patched version and using endpoint protection tools to flag suspicious archive behavior. As a preventive measure,



users should avoid opening unknown archive files and administrators should enforce file-type filtering on email gateways.

### **3.3 Windows Search Exploit – CVE-2023-36884**

**Objective:**

To investigate and remediate a remote code execution vulnerability related to Windows Search functionality.

**Activity Summary:**

I completed the “**CVE-2023-36884 Windows Search - Remote Code Execution**” module. The lab demonstrated how a specially crafted shortcut or document could trigger execution of malicious code via the Windows Search protocol.

**Deliverable – Summary:**

Detection was performed by analyzing the use of search-ms URI handlers in document files. The mitigation strategy involved disabling vulnerable protocol handlers via Group Policy and applying Microsoft’s security patch. To prevent future exploitation, it’s essential to monitor for abnormal usage of URI schemes and restrict user permissions on endpoint devices.

### **3.4 Log4Shell Vulnerability – CVE-2021-44228**

**Objective:**

To investigate the Log4Shell vulnerability affecting Java-based applications and deploy mitigation strategies.

**Activity Summary:**

I completed the “**CVE-2021-44228 Log4Shell**” module, which simulated the exploitation of a logging library to perform remote code execution (RCE).

**Deliverable – Summary:**

The detection involved examining logs for suspicious JNDI strings and LDAP callbacks.



I mitigated the risk by updating the Log4j library to a secure version and removing vulnerable classes. To prevent re-exploitation, I recommended continuous vulnerability scanning, proper input validation in applications, and using a Web Application Firewall (WAF) to block exploit attempts.

### **3.5 PrintNightmare Exploit – CVE-2021-34527**

**Objective:**

To analyze and remediate a vulnerability in the Windows Print Spooler service that enables privilege escalation.

**Activity Summary:**

I completed the “**CVE-2021-34527 PrintNightmare**” module, where the lab simulated a local privilege escalation scenario through the print spooler.

**Deliverable – Summary:**

I detected exploit attempts by monitoring for abnormal spooler activity and privilege changes. Containment involved disabling the print spooler service where unnecessary and applying security patches from Microsoft. I also recommended implementing strict privilege management and auditing all print-related services in the environment.

### **3.6 Detecting Ransomware Variants (REvil)**

**Objective:**

To detect and respond to ransomware activities, focusing on REvil variants.

**Activity Summary:**

I completed the “**REvil Detection and Response**” module, which provided insights into detecting and responding to ransomware behavior.

**Deliverable – Summary:**

Detection techniques included monitoring file encryption patterns, command-line activity, and creation of ransom notes. I practiced isolating infected systems and



recovering data from backups. For proactive defense, I suggested implementing real-time endpoint monitoring, network segmentation, and frequent user training on phishing awareness.

## **4.0 Phase 3 – Integrated Incident Simulation and Reporting**

This phase integrates all previously learned incident response (IR) and vulnerability management concepts into a comprehensive incident simulation. The goal is to demonstrate a coordinated response to a multi-vector attack affecting both the network perimeter and internal applications. It also includes a strategic review of vulnerabilities (CVEs) with long-term defense recommendations.

### **4.1 Comprehensive Incident Simulation**

#### **Objective:**

To simulate a coordinated response to a multi-faceted cyber attack, applying the full incident response lifecycle—detection, containment, eradication, and recovery—across affected systems and services.

#### **Activity Summary:**

Using insights from prior modules, I simulated a complex attack involving both network intrusion and application-layer exploitation. The attack vectors included unauthorized remote access, exploitation of known CVEs (e.g., Log4Shell and PrintNightmare), and lateral movement to compromise internal systems.

#### **Deliverable – Simulated Incident Report:**

- Detection:**

Initial signs of compromise were detected via abnormal network traffic and user behavior anomalies. IDS alerts and log correlation revealed access attempts on



exposed web services and unusual PowerShell activity.

- **Containment:**

The compromised systems were isolated from the network. Access controls were tightened, malicious accounts were disabled, and suspicious IP addresses were blocked at the firewall.

- **Eradication:**

Malware components were removed, vulnerable software was updated or replaced, and persistence mechanisms (e.g., scheduled tasks, registry modifications) were eliminated.

- **Recovery:**

Clean system backups were restored, user passwords were reset, and services were brought back online in a phased manner after verification. Logs were monitored post-recovery for reinfection attempts.

- **Lessons Learned:**

The simulation highlighted the importance of early detection, centralized logging, timely patching, and effective containment policies. A coordinated response across IT, security, and incident response teams is essential to minimize damage and downtime.

- **Recommendations for Enhancing Organizational Defenses:**

- Implement automated alerting for critical vulnerabilities.
- Apply Zero Trust principles across internal networks.
- Conduct regular security awareness training and red team exercises.
- Maintain a tested and documented incident response plan.



### 4.2 Final CVE Review and Proactive Measures

#### Objective:

To reflect on the CVEs addressed during the project and develop proactive strategies for long-term security posture improvement.

#### Deliverable – CVE Defense Summary:

CVE	Vulnerability Type	Mitigation Steps	Proactive Measures
CVE-2023-38831 (WinRAR)	Arbitrary Code Execution	Updated WinRAR, restricted archive file execution	Educate users on safe file handling, use sandbox environments
CVE-2023-36884 (Windows Search)	Remote Code Execution	Disabled vulnerable protocols, applied patches	Audit protocol usage, restrict URI handling via GPO
CVE-2021-44228 (Log4Shell)	Remote Code Execution	Upgraded Log4j, monitored logs for JNDI payloads	Regular dependency scanning, input sanitization
CVE-2021-34527 (PrintNightmare)	Privilege Escalation	Disabled Print Spooler where unnecessary, patched systems	Least privilege enforcement, restrict service usage
REvil Ransomware	Ransomware	Detected via behavior analysis, isolated system, restored from backup	Endpoint detection & response (EDR), frequent backups, phishing awareness



## 5.0 Lab Completion Screenshots: Proof of Completion

This section includes screenshots captured during the completion of each lab exercise as evidence of active participation, successful execution, and critical milestones achieved throughout the capstone project. Each screenshot reflects either the final step of a module, key configurations made, indicators of compromise (IoCs) identified, or successful mitigation applied.

### 5.1 Incident Response

The screenshot shows a web-based training interface for 'RangeForce'. The top navigation bar includes tabs for 'Instructions' and 'Feedback'. The main content area is titled 'Incident Handling' and features a circular 'The IR Lifecycle' diagram. The diagram is divided into five quadrants: 'Plan & Prepare' (top), 'Detection & Reporting' (right), 'Assessment & Decision' (bottom), and 'Responses' (left). Arrows indicate a clockwise flow between these phases. In the center of the circle is the text 'Incident Response Process'. Below the diagram, a list of '5 main steps of incident response' is provided:

1. Plan and Prepare: Establish an information security incident management policy and ensure your IR team has the necessary tools/experience to handle a security incident.
2. Detection and Reporting: Your team must have the ability to monitor security events in order to detect, alert, and report on potential security incidents.
3. Assessment and Decision: The data must be analyzed, and someone must assess the situation to determine if it is, in fact, an incident otherwise known as a "true positive".
4. Responses: Containment, eradication, and recovery.
5. Lessons Learnt: Post-incident reporting and monitoring are required to make systematic improvements to the organization's management of information.

A progress bar at the bottom left indicates '33%' completion. On the right side, there are buttons for 'BACK', 'RESUME LATER', and 'END'.



RangeForce

portal.rangeforce.com/play/68173bd7e2420da137849a8f

## Incident Handling

Instructions Feedback

**Respond to an Incident**

An alert has been detected, indicating that **Meterpreter** is present on a host:

This is how the alert appears in the SIEM:

Time	Agent	Agent name	Technique(s)	Description	Level	Rule ID
Sept 11, 2021 @ 18:22:01.988	001	windows10		Windows Defender: Antivirus platform detected potentially unwanted software 0	12	62123

Table JSON Rule

agent_ip	192.168.0.5
agent_name	windows10
agent_id	001
manager_name	server
rule_firstrule	1
rule_mail	true
rule_level	12
rule_pc1_dts	5.1, 5.2, 10.6.1, 11.4
rule_ipaa	164.312.8
rule_tac	A1.2, C0.2, CC7.3, C08.1, C08.8
rule_description	Windows Defender: Antivirus platform detected potentially unwanted software 0
rule_groups	windows, windows_Defender
rule_id	62123
rule_ipc_800_53	9.3, A1.6, S1.4
rule_gpt13	4.2
rule_gpt2	H.20.7.4
decoder_name	windows_EventChannel
location	EventChannel

Next objective

RangeForce

portal.rangeforce.com/play/68175f9c03694a1628bf5f789

## Remote System Attacks

Instructions Topology Feedback

**Triage Alert**

To begin, log in to **Splunk** with the following credentials:

- Username: admin
- Password: rangeforce

Navigate to **Search & Reporting > Alerts** and you should see a **Crypto Mining Detected** alert.

Clicking on the alert will display the **events** that triggered it.

**Crypto Mining Detected**

Triggered to a crypto mining pool detected.

Enabled: Yes	Trigger Time: 2023-04-17 05:59:12 UTC
App: Prevention	Action: Add to Triggered Alerts
Prevention: Pools: Owned by admin	Condition: Per Result
Modified: Unknown	Editor: Edit
Alert Type: Real-time	

Trigger History

20 per page

TriggerTime	Actions	View Results
2023-04-17 05:59:12 UTC		

Next step

splunk-enterprise

Home

Incognito (2)

Hello, Administrator

Apps Manage

Search & Reporting

Fortinet FortiGate App for Splunk

Find more apps

Common tasks

- Add data
- Search your data
- Visualize your data
- Add team members
- Manage permissions

BACK RESUME LATER END POP OUT VTA



The screenshot displays two windows from the RangeForce platform:

**Remote System Attacks** window:

- Module info:** Network Perimeter, Alert Monitoring, Triage Alert, Investigation, Root Cause Analysis, Remediation.
- Triage Alert:** A step in the process.
- Instructions:**
  - Log in to Splunk:
    - Username: admin
    - Password: rangeforce
  - Go to [Search & Reporting > Alerts](#).
  - Click on the [Crypto Mining Detected alert](#).
    - Analyze the events that triggered the alert.
    - Answer the questions.
- What is the source type of the events that triggered the alert?**  
fortigate\_utm
- What is the IP address of the system that triggered the alert?**  
answer
- What is the name of the system in the DMZ that triggered the alert?**  
answer

**Next step**

**Splunk Enterprise** window (Search results):

```
sourcetype="fortigate_utm" subtype="ips" attack="Crypto.Mining.Pool.Connection"
2 events (1/17/20 12:00:00:00 AM to 5/4/25 12:41:14.895 PM)
No Event Sampling
```

i	Time	Event
>	May 4 12:41:14 10.255.255.101 date=2025-05-04 time=05:41:14 devname="primaryrouter-FGT-A" devid=367 eventtime=1746362473851568000 tz="-0700" logid=0419016384" type="utm" subtype="ips" eventtype="alert" vd="VDMH-A" severity="high" srip=22.1.0.100 srccountry="United States" dstip=8.8.8.88 srcintrole="undefined" dstintf="port2" dstintrole="undefined" sessionid=363 action="detect" service="DNS" policyid=2 attack="Crypto.Mining.Pool.Connection" srport=47255 dstport=53 direction="tackid=9991 profile="cryptominer" incidentserialno=201326598 msg="custom: Crypto.Mining.Pool.Connection@30 craction=8192 crlevel="high" host = 10.255.255.101   source = udp:514   sourcetype = fortigate_utm	
>	May 4 12:41:14 10.255.255.101 date=2025-05-04 time=05:41:14 devname="primaryrouter-FGT-A" devid=367 eventtime=1746362473854841901 tz="-0700" logid=0419016384" type="utm" subtype="ips" eventtype="alert" vd="VDMH-A" severity="high" srip=22.1.0.100 srccountry="United States" dstip=8.8.8.88 srcintrole="undefined" dstintf="port2" dstintrole="undefined" sessionid=364 action="detect" service="DNS" policyid=2 attack="Crypto.Mining.Pool.Connection" srport=60769 dstport=53 direction="tackid=9991 profile="cryptominer" incidentserialno=201326599 msg="custom: Crypto.Mining.Pool.Connection@30 craction=8192 crlevel="high" host = 10.255.255.101   source = udp:514   sourcetype = fortigate_utm	

**Website Defacement Attacks** window:

- Module info:** Defacement Attack Overview, Investigation, Remediation.
- Defacement Attack Overview:** A step in the process.
- Instructions:**

The MITRE ATT&CK description of **Defacement**:

Adversaries may **modify** visual content available **internally** or **externally** to an enterprise network, thus affecting the integrity of the original content. Reasons for Defacement include delivering messaging, intimidation, or claiming (possibly false) credit for an intrusion. Disturbing or offensive images may be used as a part of Defacement in order to cause user discomfort or to pressure compliance with accompanying messages.

Effective detection of Defacement requires vigilant monitoring of various aspects. Below are some key indicators to watch for in order to identify and respond to potential attacks:

  - Application Log Content:** Monitor for third-party application logging, messaging, and/or other artifacts that may modify visual content available internally or externally to an enterprise network.
  - File Creation:** Monitor for newly constructed visual content for internal or external enterprise networks.
  - File Modification:** Monitor for changes made to files for unexpected modifications to internal and external websites for unplanned content changes.
  - Network Traffic Content:** Monitor and analyze traffic patterns and packet inspection associated with protocol(s) that do not follow the expected protocol standards and traffic flows, e.g., unauthorized, gratuitous, or abnormal traffic patterns attempting to access internal and external websites and services. Consider correlating with application monitoring for indication of unplanned service interruptions or unauthorized content changes.

**Note:** For more information about this type of attack, visit the MITRE ATT&CK technique for **Defacement**.

One memorable, albeit lighthearted, instance of a website defacement attack occurred in 2010 on the Spanish Presidency website. In this case, the image of the then Spanish Prime Minister Jose Luis Rodriguez Zapatero was replaced with that of the comedic character Mr. Bean, played by actor Rowan Atkinson. This incident was seen as a humorous jab at Mr. Zapatero, due to the long-standing joke in Spain about his resemblance to Mr. Bean.

Although the defacement did not disrupt the functionality of the website, it served to embarrass the Prime Minister and momentarily alter the public's perception of the site. This is a prime example of how website defacements, even non-malicious ones, can have significant impacts on the target entity's public image and credibility.

**Next objective**



# EncryptEdge Labs

This screenshot shows the RangeForce interface. On the left, there's a sidebar with icons for Recycle Bin, cmd, Google Chrome, PowerShell, and Virtual Teaching Assistant. A progress bar indicates 33% completion. The main window displays a Microsoft Outlook login page with fields for Domain/User name and Password, and a 'sign in' button. To the right of the login screen is a vertical toolbar with buttons for BACK, RESUME LATER, END, POP OUT, and VTA. At the bottom, a taskbar shows icons for Windows, Search, Google Chrome, and VITA, along with system status indicators.

This screenshot shows the RangeForce interface again. The sidebar and progress bar are identical to the first screenshot. The main window now displays a website for 'commsuratetechnology.com'. The page features a cartoon illustration of a man with a speech bubble that says 'WE ❤ MICRO TRANSACTIONS'. Below the illustration, there's a 'Reveal solution' button and a 'Next step' button. The right side has a vertical toolbar with the same set of buttons as the first screenshot. The taskbar at the bottom is also present.





The image displays three side-by-side browser windows:

- Left Window (EncryptEdge Labs):** Shows a "Cybersecurity Analyst: Task 2" page. It includes a "Screenshot Tools" section, a "Project Breakdown" section with "Phase 1: Incident Response Execution" (Objective: Introduce core IR techniques), and a "Step-by-Step Breakdown" section detailing tasks for Incident Handling Fundamentals, Responding to Remote System Attacks, Malware Incident Response Exercise, and Perimeter Compromise Simulation.
- Middle Window (ChatGPT):** Shows a conversation with AI. The user asks for a report template and ChatGPT responds that practical exercises for the capstone project are to be done on RangeForce Labs. It also lists "RangeForce Labs Modules Breakdown" for Phase 1 (Incident Response Execution) and Phase 2 (CVE Analysis and Remediation).
- Bottom Window (RangeForce):** Shows an "Incident Handling" module under "Security Incidents". It defines terms like Security Incident, Security Alert, and Security Event. It notes that a security event is a log message related to security, while a security alert is flagged by a SIEM solution. A security incident is a validated threat. The module provides examples of login failures and firewall events as security events. It also discusses the difference between a security breach (unauthorized access/exploitation) and a security incident (verified compromise). A progress bar indicates 16% completion.



A screenshot of the RangeForce platform interface. On the left, there's a sidebar with navigation links: Dashboard, Training, My Skills, Catalog, Completed Modules, Assessment Results, Leaderboard, and Profile. The main content area has a dark background with a blue header bar. The header bar contains the text "Theme: Incident Response". Below the header, there's a summary box with the following details: Course length (4 hours 55 minutes), Progress (green bar), and Teams (Blue team). A yellow "Save course" button is at the bottom right of this box. Underneath, there are tabs for Overview, Prerequisites, and Outcomes. The Overview tab is selected and displays a brief description: "Venture into the crucial domain of Incident Response with this course. Engaging learners with the essentials of incident handling, this course unfolds the journey from identifying to mitigating and recovering from cyber incidents, fostering a well-rounded understanding and resilience in facing cybersecurity threats." Below this, there's a section titled "Course modules" with filters for Difficulty (All difficulties), Duration (All durations), Type (All types), and Teams (All teams). The first module listed is "Incident Handling", described as Foundational, 10m long, and associated with Red team, Blue team, and Purple team. Below it is a partial view of the "Remote System Attacks" module.

## 5.2 CVEs and Emerging Threats

A screenshot of the RangeForce platform interface, specifically a module titled "CVE Overview". On the left, there's a sidebar with "Module info" sections: "What are CVEs" (checked), "CVE Severity Score" (checked), and "CVE Reporting and Response". A progress bar shows 66% completion. The main content area has a dark background with a white header bar. The header bar contains the text "CVE Overview". Below the header, there are tabs for Instructions and Feedback. The Instructions tab is active and contains a section titled "CVE Severity Score" with two bullet points: "Integrity (I) – Partial (P): The attacker is able to alter some files or data on the system." and "Availability (A) – Complete (C): The attacker is able to cause the system to become completely unavailable as a result of exploiting the vulnerability." Below this, it says "There are multiple versions of CVSS. At the time of writing this module, the latest version is CVSS 3.1. CVSS 3 scores are assigned thusly:" and lists a table of severity levels and base scores. The table is as follows:

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- Answer the questions.

In the CVSS vector string AV:N/AC:L/Au:N/C:P/I:C/A:C, what is the level of compromise for Integrity?



c

What is the severity of a vulnerability with CVSS score 10.0?



Critical

### Hints

Ask for a hint (3 left)

Next objective



The screenshot shows the 'CVE Overview' module in RangeForce. On the left, a sidebar lists 'Module info' items: 'What are CVEs' (checked), 'CVE Severity Score' (checked), 'CVE Reporting and Response' (checked), and 'Conclusion' (unchecked). A progress bar at the bottom of the sidebar is at 100%. The main content area is titled 'CVE Reporting and Response'. It contains a text block about responsible disclosure and security verification, followed by a list of methods to find vulnerabilities. Below this is a question asking for the expected relative URL of a security.txt page, with the answer '/.well-known/security.txt' entered in the input field. A 'View conclusion' button is visible at the bottom right.

The screenshot shows the 'CVE Overview' module in RangeForce. The sidebar is identical to the previous screenshot. The main content area is titled 'Conclusion'. It contains a text block about establishing a good CVE information flow. Below this is a 'Feedback (optional)' section with a rating scale from 'Bad experience' to 'Excellent experience' and a link for 'Any additional feedback?'. A 'Submit' button is visible at the bottom right.



The screenshot shows the RangeForce interface with a dark theme. On the left, a vertical sidebar lists various modules: Module info, Recycle Bin, Google Chrome, cmd, PowerShell, Virtual Teach..., This PC, and trading\_sys... A progress bar indicates 0% completion for the 'Module info' section. The main content area displays the following information:

**CVE-2023-38831 WinRAR - Arbitrary Code Execution**

**Module info**

- Vulnerability Overview
- Examine the Sample

**Instructions** **Feedback**

**CVE-2023-38831** is a file extension spoofing vulnerability, discovered in **RARLabs WinRAR versions before 6.23**. It leads to an arbitrary code execution when a user attempts to open a benign file within a ZIP archive. By modifying archives in a special way, adversaries are able to exploit the vulnerability and launch a malicious script instead of the intended file. The vulnerability has been exploited in the wild from April through August 2023.

In this module, you will learn about the vulnerability and its exploitation by examining a malicious sample that was rendered nonfunctional.

- CVSS Base Score: 7.8 HIGH
- CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**Get started**

On the right side of the interface, there are several buttons: BACK, RESUME LATER, END, POP OUT, and VTA. The bottom status bar shows the time as 2:28 PM and the date as 5/4/2023.

The screenshot shows the 'Vulnerability Overview' section of the module. The progress bar now shows 50% completion. The main content area contains the following questions and answers:

**Vulnerability Overview**

Answer the questions.

In which version of WinRAR was the vulnerability fixed? (format: x.xx)

6.23

Provide one example of malware families that were distributed with the exploitation of this vulnerability.

DarkMe

Who was the target group in this campaign?

Healthcare professionals and researchers

Traders, stock brokers, crypto-traders

Government agencies and military organizations

Everyday computer users and gamers

How were the archives modified by the adversary to exploit the vulnerability?

By adding additional metadata to the archive to mislead analysis tools

By encrypting the archive to hide its true purpose

By including a directory and file with the same name and a trailing space

By altering the file permissions of the archive to grant unauthorized access

**Next objective**

On the right side, there are buttons: BACK, RESUME LATER, END, POP OUT, and VTA. The bottom status bar shows the time as 2:33 PM and the date as 5/4/2023.



RangeForce +/-

portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

This PC Module info

Module info Virtual Teaching Assistant

Module info Instructions Feedback

CVE-2023-36884 Windows Search - Remote Code Execution

Administrator: PowerShell

PS C:\Users\ComtechAdmin\Desktop\maldoc\Overview\_of\_UWCs\_UkraineInNATO\_campaign\word>

Directory: C:\Users\ComtechAdmin\Desktop\maldoc\Overview\_of\_UWCs\_UkraineInNATO\_campaign\word>

Mode	LastWriteTime	Length	Name
d----	5/5/2025 10:02 AM	-----	media
d----	5/5/2025 10:02 AM	-----	temp
d----	5/5/2025 10:02 AM	-----	rels
---	6/30/2023 5:21 AM	44146	afchunk.rtf
---	1/1/1988 12:00 AM	22924	document.xml
---	1/1/1988 12:00 AM	22924	document.xml
---	1/1/1988 12:00 AM	5344	numbering.xml
---	1/1/1988 12:00 AM	3108	settings.xml
---	1/1/1988 12:00 AM	32213	styles.xml
---	1/1/1988 12:00 AM	843	webSettings.xml

PS C:\Users\ComtechAdmin\Desktop\maldoc\Overview\_of\_UWCs\_UkraineInNATO\_campaign\word>

Maldoc Analysis

What is the name of the .rtf file embedded in the maldoc?  afchunk.rtf Ask for a hint (1 left)

What is the URL of the file loaded via SMB?  answer POP OUT

What is the URL of the file loaded via HTTP?  answer VTA

Hint Next objective

10:15 AM 5/5/2025

RangeForce +/-

portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

This PC Module info

Module info Virtual Teaching Assistant

Module info Instructions Feedback

CVE-2023-36884 Windows Search - Remote Code Execution

Administrator: PowerShell

PS C:\Users\ComtechAdmin\Desktop\maldoc\Overview\_of\_UWCs\_UkraineInNATO\_campaign\word> rtobj.exe -all -o .\afchunk.rtf -p 13.1 - http://decalage.info/python/oletools

THIS IS WORK IN PROGRESS - Check updates regularly!

Please report any issue at https://github.com/decalage/oletools/issues

```
-----
```

File: ".\afchunk.rtf" - size: 44146 bytes

id: Index [OLE Object]

0 | 0000260Eh [Not a well-formed OLE object]

1 | 00003E6Bh [Format\_Id: 2 (Embedded)]  
  | 0000260Eh [OLE Link]  
  | data size: 3584  
  | MD5 = 'ed15c3b36a83206fdf1bb013b91575'  
  | CLSID: 8809640C-F192-11D4-A65F-0049963251E5  
  | SAX XML Reader: 5.6 (msxml.dll)

Saving raw data in object #0  
saving object to file .\afchunk\_rtf-object\_0000260E.raw  
raw file size: 44146  
Saving file embedded in OLE object #1:

File Explorer Word

File Home Share View

...> This PC > Desktop > maldoc > Overview\_of\_UWCs\_UkraineInNATO\_campaign > word

Name	Date modified	Type	Size
Desktop	5/5/2023 10:02 AM	File/folder	
Downloads	5/5/2023 10:02 AM	File/folder	
Documents	5/5/2023 10:02 AM	File/folder	
Pictures	5/5/2023 10:21 AM	Rich Text Format	44 KB
afchunk.rtf	5/5/2023 10:21 AM	Rich Text Format	44 KB
afchunk_rtf_object_00003E6Bh.bin	5/5/2023 10:18 AM	BIN File	4 KB
afchunk_rtf_object_0000260E.raw	5/5/2023 10:18 AM	RAW File	3 KB
document		XML Document	23 KB
fontTable.xml		XML Document	3 KB
numbering.xml		XML Document	6 KB
settings.xml		XML Document	4 KB
styles.xml		XML Document	32 KB
webSettings.xml		XML Document	1 KB

Maldoc Analysis

What is the name of the .rtf file embedded in the maldoc?  Ask for a hint (1 left)

What is the URL of the file loaded via SMB?  POP OUT

What is the URL of the file loaded via HTTP?  VTA

Hint Next objective

10:22 AM 5/5/2025



RangeForce x +

portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

Virtual Teaching Assistant

### CVE-2023-36884 Windows Search – Remote Code Execution

Instructions Feedback

Module info

This PC pestudio

Recycle Bin

cmd

Google Chrome

File Share View Picture Tools

This PC Desktop maldoc Overview

Name

5/5/2023 10:24 AM

sha256: DF658C0FCE44D9D0DE8156CAE3F4F0614F31AFCAC701F9234C9BA653D0D665ED

group (0) technique (0) value (18)

group (0)	technique (0)	value (18)
-	-	MSHTML_C7\file001.url
-	-	WordDocument.8
-	-	WordDocument.8
-	-	WMF
-	-	EMF
-	-	EMF+
-	-	EMF+@
-	-	RTF
-	-	OLE
-	-	OLEV
-	-	OLEV
-	-	EMF+@
-	-	EMF+
-	-	System
-	-	System
-	-	System
-	-	Calibri
-	-	Arial

Next objective

10:34 AM 5/5/2023

RangeForce x +

portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

Virtual Teaching Assistant

### CVE-2023-36884 Windows Search – Remote Code Execution

Instructions Feedback

Module info

This PC pestudio

40%

File Share View Picture Tools

This PC Desktop maldoc Overview

Name

5/5/2023 10:24 AM

sha256: DF658C0FCE44D9D0DE8156CAE3F4F0614F31AFCAC701F9234C9BA653D0D665ED

group (0) value (18)

group (0)	value (18)
-	MSHTML_C7\file001.url
-	WordDocument.8
-	WordDocument.8
-	WMF
-	EMF
-	EMF+
-	EMF+@
-	RTF
-	OLE
-	OLEV
-	OLEV
-	EMF+@
-	EMF+
-	System
-	System
-	System
-	Calibri
-	Arial

**Maldoc Analysis**

- Extract the word document (maldoc) from the zip archive.
  - File: maldoc.zip
  - Password: infected
- Identify and extract the malicious .rtf file from the maldoc.
- Extract and analyze the OLE objects embedded in the .rtf file.
- Extract URLs from the OLE objects.
- Answer the questions.

What is the name of the .rtf file embedded in the maldoc?

afchunk.rtf

Ask for a hint (1 left)

What is the URL of the file loaded via SMB?

\\10.234.239.26\share1\MSHTML\_C7\file001.url

What is the URL of the file loaded via HTTP?

http://74.50.94.156/MSHTML\_C7/start.xml

Hints

Ask for a hint (1 left)

Next objective

10:35 AM 5/5/2023



RangeForce x + portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

Virtual Teaching Assistant

Module info

- Campaign and Threat Actor Overview
- Maldoc Analysis
- Attack Chain Overview
- Vulnerability Overview
- Mitigation & Security Updates

40%

### CVE-2023-36884 Windows Search - Remote Code Execution

Instructions Feedback

#### Attack Chain Overview

adversaries in their attacks.

Below is a simplified chain (less details, misses some steps) derived from the attack chain created by research team at Volexity and a spreadsheet created by a vulnerability analyst Will Dormann.

A simplified attack chain description:

Next objective

10:41 AM 5/5/2025

RangeForce x + portal.rangeforce.com/play/681885b379e7a0d2b9d22f60

Virtual Teaching Assistant

Module info

- Campaign and Threat Actor Overview
- Maldoc Analysis
- Attack Chain Overview
- Vulnerability Overview
- Mitigation & Security Updates

80%

### CVE-2023-36884 Windows Search - Remote Code Execution

Instructions Feedback

#### Attack Chain Overview

The threat actor uses a Microsoft Word document (VULN\_19\_1.docx) containing a malicious macro to exploit the CVE-2023-36884 vulnerability to evade the Mark of the Web (MotW) defenses and allow code execution.

- 1111.htm and 2222.chm go through a set of steps of adding additional files (omitted for simplicity) via iframes and end up loading ex001.zip/file001.vbs from the adversary's SMB server.
- file001.vbs is loaded from the IE cache. It loads and executes the final payload (backdoor similar to RomCom).

Answer the questions.

In which Windows service is the CVE-2023-36884 vulnerability exploited?

Windows search

Which security measure is evaded by the threat actor with the exploitation of CVE-2023-36884?

Mark of the Web (Motw)

Connection to which file triggers the automated generation of tailored files in the adversary's SMB server? (file name)

file001.url

What HTML element does the threat actor predominantly use to load scripts and files in this attack chain?

iframe

Next objective

10:46 AM 5/5/2025



# EncryptEdge Labs

RangeForce

Virtual Teaching Assistant

## CVE-2023-36884 Windows Search - Remote Code Execution

Module info

- Campaign and Threat Actor Overview
- Maldoc Analysis
- Attack Chain Overview
- Vulnerability Overview**
- Mitigation & Security Updates
- Conclusion

100%

### Vulnerability Overview

Per Will Dorman's analysis of the attack chain:

- Adversary loads `[victim_ip]_[hex]_file001.zip` from their SMB server with `[victim_ip]_[hex]_file001.search-ms` but stops the execution of `search-ms` before the MotW comment is added. Contents of the ZIP archive on initial download are some dummy `1111.txt` and `2222.txt` files.
- The archive is replaced in the SMB server and `search-ms` is executed the second time. The files (inside the archive) loaded in the second try are `1111.htm` and `2222.chm`.
- `1111.htm` is loaded from the ZIP archive before the MotW comment is added to the file.

It is worth noting that this method of running the file before the MotW stamping is unreliable. The race is not won every time and fails quite often. However, it is doable as before the patch, approximately a 20-second delay was observed between the file extraction and the MotW stamping for files loaded with `search-ms`. Furthermore, the files would be extracted in a predictable temporary location of `C:\Users\<username>\AppData\Local\Temp\Temp_1\[victim_ip]_[hex]_file001.zip`. The adversary then could easily access the files with `\<computer_name>\$<username>\AppData\Local\Temp\Temp_1\[victim_ip]_[hex]_file001.zip\1111.htm`. Note that the victim's computer name, username, and IP address were already known to the adversary from the earlier stages of the attack chain.

Answer the question below.

What are the two main issues that allow the exploitation of the vulnerability?

Executables embedded into Office documents via the AltChunks method do not trigger security measures.

There is a long delay between file extraction and MotW application for files loaded with `search-ms`.

The MotW tag is never stamped on files loaded from remote SMB servers.

Archives are extracted in a predictable temporary location.

Files loaded with `search-ms` do not get the MotW tag stamped on them by default.

Next objective

10:46 AM 5/5/2025

RangeForce

## Theme: CVEs and Emerging Threats

RANGE FORCE

Dashboard Training My Skills Catalog Completed Modules Assessment Results Leaderboard Profile

Search for courses and modules Q

Course length 2 hours 40 minutes

Progress

Teams Blue team

Save course

Overview Prerequisites Outcomes

Get hands-on experience and learn about the impact of some of the recent and notable CVEs out there. Learn how to identify and analyze some of the most common variants of ransomware using various detection tools and techniques.

Course modules

Difficulty Duration Type Teams

All difficulties All durations All types All teams Clear

**CVE Overview**  
Novice 15m Purple team

**CVE-2023-38831 WinRAR - Arbitrary Code Execution**  
Novice 20m Blue team



**EncryptEdge Labs**

**This Internship Task report was developed on [May, 05, 2025]**

**By:**

**atalmamun@gmail.com**