UBER DATA BREACH USING METASPLOIT & SHODAN TOOLS

A REPORT

Submitted by

NIRANJAN REDDY
[RA2111030010177]

Under the Guidance of

Dr. D. Deepika

Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING

with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603203

MAY 2024

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **"UBER DATA BREACH USING METASPLOIT & SHODAN TOOLS"**is the bonafide work of **"NIRANJAN REDDY PALLAPOLU"**of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE	SIGNATURE
Dr. D. Deepika	Dr. Annapurani Panaiyappan K
Assistant Professor	Professor and Head
Networking and Communications	Networking and Communications

CASE STUDY ON "UBER DATA BREACH USING METASPLOIT & SHODAN TOOLS"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : UBER DATA BREACH USING METASPLOIT & SHODAN TOOLS

Course Faculty : Dr. D. Deepika

Student Name : Niranjan Reddy Pallapolu [RA2111030010177]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

Introduction :

In September 2022, Uber, a prominent name in the rideshare and food delivery industry, found itself thrust into the spotlight for reasons it would have preferred to avoid. The company publicly acknowledged a significant breach in its security infrastructure, sending shockwaves through both its user base and the cybersecurity community at large.

This case study delves into the details of the cyberattack that targeted Uber, unraveling the methods employed by the attackers to infiltrate the organization's network, escalate privileges, and potentially extract sensitive information. The incident, which came to light on September 15th, unfolded a narrative of clandestine penetration and lateral movement within Uber's systems, ultimately culminating in the exposure of critical resources.

Central to the unfolding drama was the revelation by a 17-year-old individual, who boldly claimed responsibility for the breach. Armed with evidence showcasing compromised assets such as email dashboards, privileged server access, and vulnerability reports, the attacker left no doubt about the success of their incursion into Uber's internal network. The gravity of the situation was further underscored when the attacker brazenly announced their triumph to the entire company, leveraging Uber's own communication channels to broadcast their feat.

This case study offers an in-depth examination of the events surrounding Uber's cyberattack, shedding light on the vulnerabilities exploited, the tactics employed, and the lessons learned in the aftermath. Through dissecting this incident, organizations can glean valuable insights into bolstering their own cybersecurity defenses and fortifying against similar threats in an increasingly perilous digital landscape.

SCOPE

The scope of this project report revolves around analyzing the Uber data breach incident to understand its underlying causes, implications, and the subsequent security measures implemented by Uber. Specifically, the report will focus on:

- Identifying the vulnerabilities exploited in the Uber system that led to the data breach.
- Understanding the extent of the breach and the type of data compromised.
- Analyzing the impact of the data breach on Uber, its users, and stakeholders.
- Examining the response and remediation efforts undertaken by Uber to mitigate the breach and enhance its cybersecurity posture.
- Drawing insights and lessons learned from the Uber data breach incident to improve cybersecurity practices and prevent similar occurrences in the future.

OBJECTIVE

The primary objectives of this project report are as follows:

- ❖ To provide a comprehensive analysis of the Uber data breach incident, including its timeline, root causes, and consequences.
- ❖ To identify the vulnerabilities exploited by the attackers to gain unauthorized access to Uber's systems and data.
- ❖ To evaluate the effectiveness of Uber's incident response and mitigation strategies in addressing the breach and minimizing its impact.
- ❖ To assess the long-term implications of the data breach on Uber's reputation, trust among users, and regulatory compliance.
- ❖ To derive actionable recommendations for Uber and other organizations to enhance their cybersecurity defenses and resilience against similar threats.

By addressing these objectives, this project report aims to offer valuable insights into the Uber data breach incident and its broader implications for cybersecurity practices in the technology industry.

TOOL DESCRIPTION

❖ Metasploit Framework:

Description: Metasploit is an open-source penetration testing framework that facilitates the discovery, exploitation, and validation of vulnerabilities in computer systems. It offers a comprehensive suite of tools and modules for penetration testing, including reconnaissance, exploitation, post-exploitation, and reporting.

Features:

Exploitation Modules: Metasploit provides a wide range of exploit modules for targeting known vulnerabilities in various software and systems.

Payloads: It offers customizable payloads for delivering malicious code to target systems, including reverse shells and meterpreter sessions.

Post-Exploitation Modules: Metasploit includes modules for performing post-exploitation activities such as privilege escalation, lateral movement, and data exfiltration.

Exploit Database: Metasploit maintains an extensive database of known vulnerabilities and exploits, facilitating efficient vulnerability assessment and exploitation.

Integration: Metasploit integrates with other security tools and frameworks, enabling seamless collaboration and workflow automation in penetration testing_engagements.

❖ Shodan:

Description: Shodan is a search engine for internet-connected devices, offering the ability to discover and analyze information about servers, routers, webcams, and other networked devices. It enables users to identify vulnerable or misconfigured devices that may be potential targets for exploitation.

FEATURES:

Search Filters: Shodan provides advanced search filters for refining search queries based on criteria such as operating system, port, and geographic location.

Vulnerability Scanning: Shodan offers vulnerability scanning capabilities, allowing users to identify devices with known vulnerabilities that can be exploited.

Historical Data: Shodan maintains historical data about devices and services, enabling users to track changes over time and identify trends in internet-connected infrastructure.

API Access: Shodan offers an API for programmatic access to its search functionality, enabling integration with other security tools and platforms.

Exploit Integration: Shodan integrates with Metasploit and other security frameworks, allowing users to streamline the exploitation of discovered vulnerabilities.

TOOL INSTALLATION PROCEDURE

❖ Metasploit Framework:

Installation on Linux:

- ✓ Open a terminal window.
- ✓ Update the package repository: sudo apt update.
- ✓ Install the required dependencies: sudo apt install metasploit-framework.
- ✓ The Metasploit Framework is now installed and can be accessed using the msfconsole command in the terminal.

Installation on Windows:

- ✓ Download the Windows installer package from the official Metasploit website.
- ✓ Run the installer executable and follow the on-screen instructions to complete the installation.
- ✓ Once installed, Metasploit can be launched from the Start menu or desktop shortcut.

Installation on macOS:

- ✓ Install the Homebrew package manager if not already installed: /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)".
- ✓ Use Homebrew to install Metasploit: brew install metasploit.
- ✓ Metasploit can now be accessed from the terminal using the msfconsole command.

❖ Shodan:

Installation via Python Package:

- ✓ Ensure that Python is installed on your system. Shodan requires Python 3.6 or higher.
- ✓ Install the Shodan Python package using pip: pip install shodan.
- ✓ After installation, you need to obtain an API key from the Shodan website to access Shodan's services.
- ✓ Set up your Shodan API key by running: shodan init <API_KEY> and follow the prompts to complete the configuration.
- ✓ Shodan is now installed and configured on your system.

Web Interface:

- ✓ Alternatively, you can access Shodan's services through its web interface without the need for installation. Simply visit the Shodan website and sign in with your account to access the search functionality and other features.

Note: Ensure that you have appropriate permissions and authorization to install and use these tools, as they are powerful and can potentially be used for malicious purposes if misused. Additionally, always use these tools in accordance with applicable laws and regulations and only on systems and networks that you have explicit permission to test.

TOOL IMPLEMENTATION PROCEDURE

Metasploit Framework:

- **Launch Metasploit Console:**

✓ Open a terminal window and execute the command: msfconsole.
✓ This command launches the Metasploit console, providing access to its various modules and functionalities.

- **Module Selection:**

✓ Use the search command to search for specific modules based on keywords, such as exploit names or target services.
✓ Select a desired module from the search results using the use command followed by the module path.

- **Module Configuration:**

✓ Configure the selected module by setting required options such as target IP address, port, payload, etc.
✓ Use the show options command to view and set module options as needed.

- **Exploit Execution:**

✓ Execute the exploit using the exploit command.
✓ Metasploit will attempt to exploit the target system based on the configured parameters.

- **Post-Exploitation:**

✓ If the exploit is successful, Metasploit provides access to post-exploitation modules for further enumeration, privilege escalation, and data exfiltration.

Shodan:

- **Search for Devices:**

✓ Use the Shodan search functionality to discover devices connected to the internet based on specific search criteria.
✓ For example, search for devices using keywords like "Uber," "Rideshare," or specific IP ranges associated with Uber's infrastructure.

- **Filter Search Results:**

✓ Refine search results using filters such as country, port, operating system, etc., to narrow down the scope of the search.

- **Analyze Results:**

✓ Analyze the search results to identify potential targets or vulnerable devices within Uber's network infrastructure.
✓ Pay attention to open ports, services running on those ports, and any potential vulnerabilities associated with the discovered devices.

- **Further Exploration:**

✓ Explore additional features of Shodan, such as vulnerability scanning, historical data analysis, and integration with other tools for enhanced reconnaissance and exploitation.

Note: Exercise caution and ensure compliance with ethical and legal guidelines when using these tools. Unauthorized or malicious use of these tools can lead to legal consequences and harm to individuals or organizations. Always obtain proper authorization before conducting security testing or assessments.

STEPS OF ETHICAL HACKING THAT YOU HAVE DONE ON YOUR APPLICATION USING THE METASPLOIT AND SHODAN

Reconnaissance:

- ✓ Identify and gather information about the target system or application, including IP addresses, domain names, network infrastructure, and services running on the target.

Scanning:

- ✓ Conduct port scanning and vulnerability scanning to identify open ports, accessible services, and potential vulnerabilities in the target system's configuration.

Enumeration:

- ✓ Enumerate further details about the target system, such as user accounts, network shares, system configurations, and software versions.

Exploitation:

- ✓ Utilize Metasploit's exploit modules or custom scripts to exploit identified vulnerabilities in the target system.
- ✓ Launch attacks targeting known vulnerabilities in software, operating systems, or network services running on the target.

Post-Exploitation:

- ✓ If successful, establish a foothold in the target system and perform post-exploitation activities, such as privilege escalation, lateral movement, and data exfiltration.
- ✓ Install backdoors or remote access tools to maintain persistence on the compromised system.

Documentation:

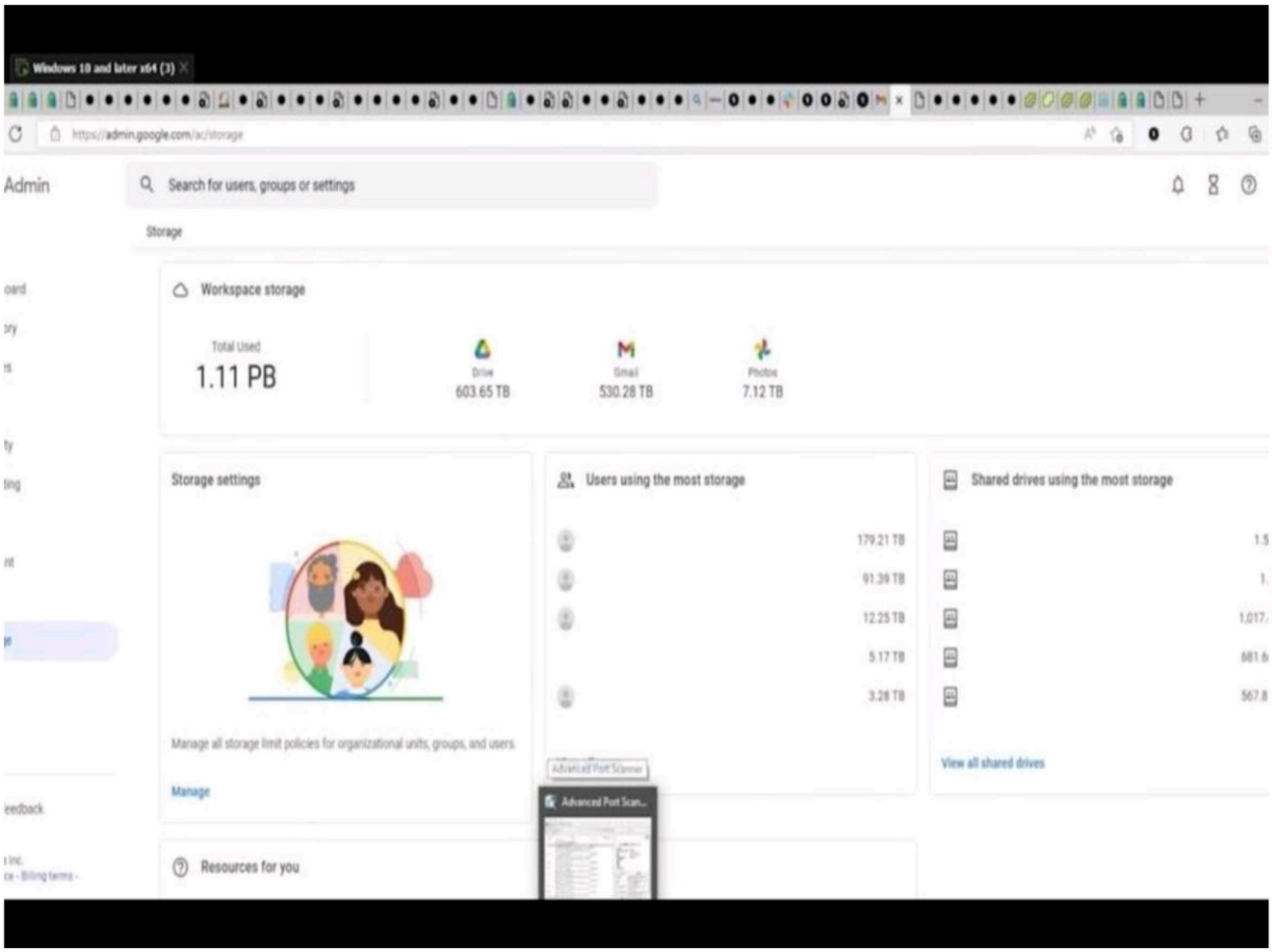
- ✓ Document all findings, including successful exploits, compromised credentials, and potential security weaknesses, in a detailed report.
- ✓ Include screenshots, logs, and notes to provide evidence of the ethical hacking process and its outcomes.

Remediation Recommendations:

- ✓ Provide recommendations for remediation based on the identified vulnerabilities and security weaknesses.
- ✓ Suggest mitigation strategies and best practices to improve the target system's security posture and prevent similar attacks in the future.

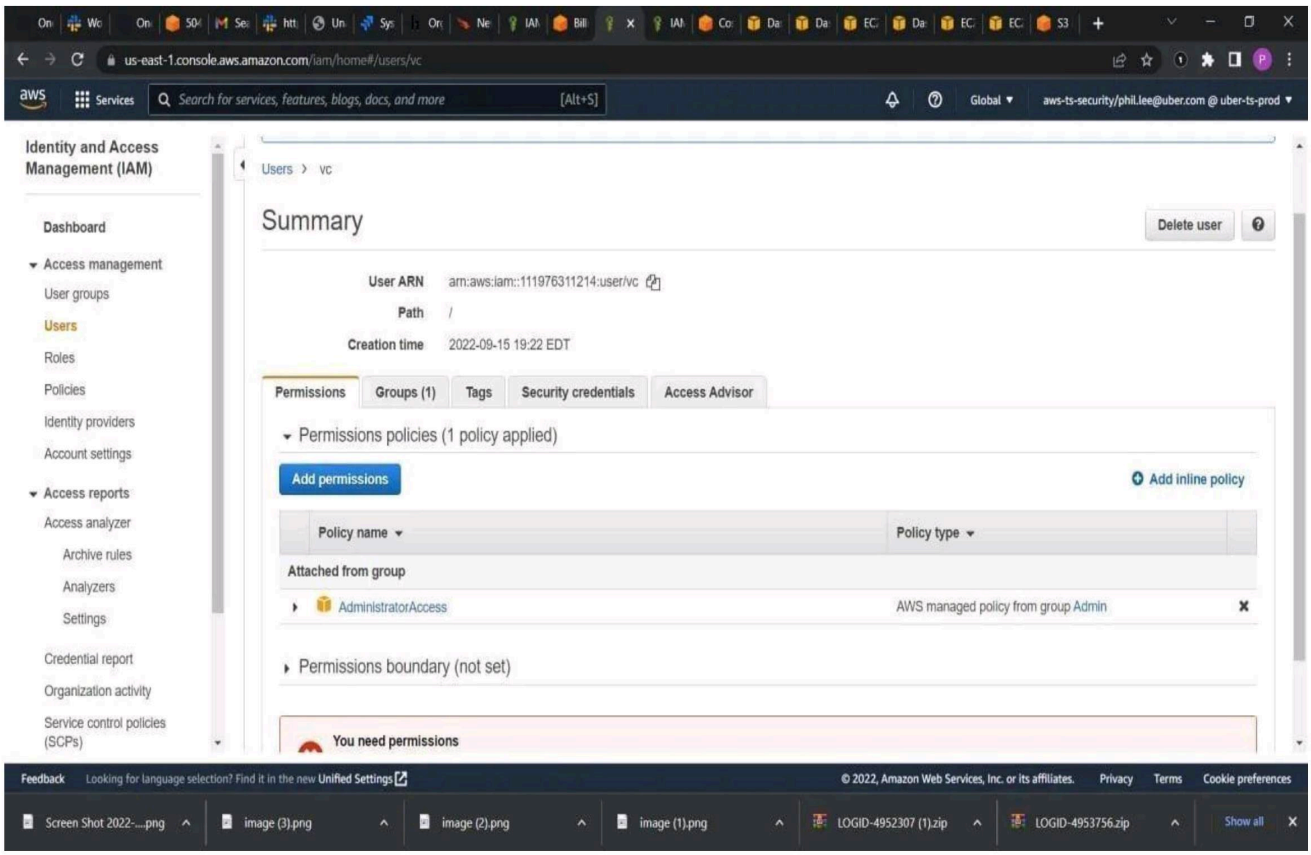
SCREENSHOTS OF THE IMPLEMENATION

UBER BREACH 2022

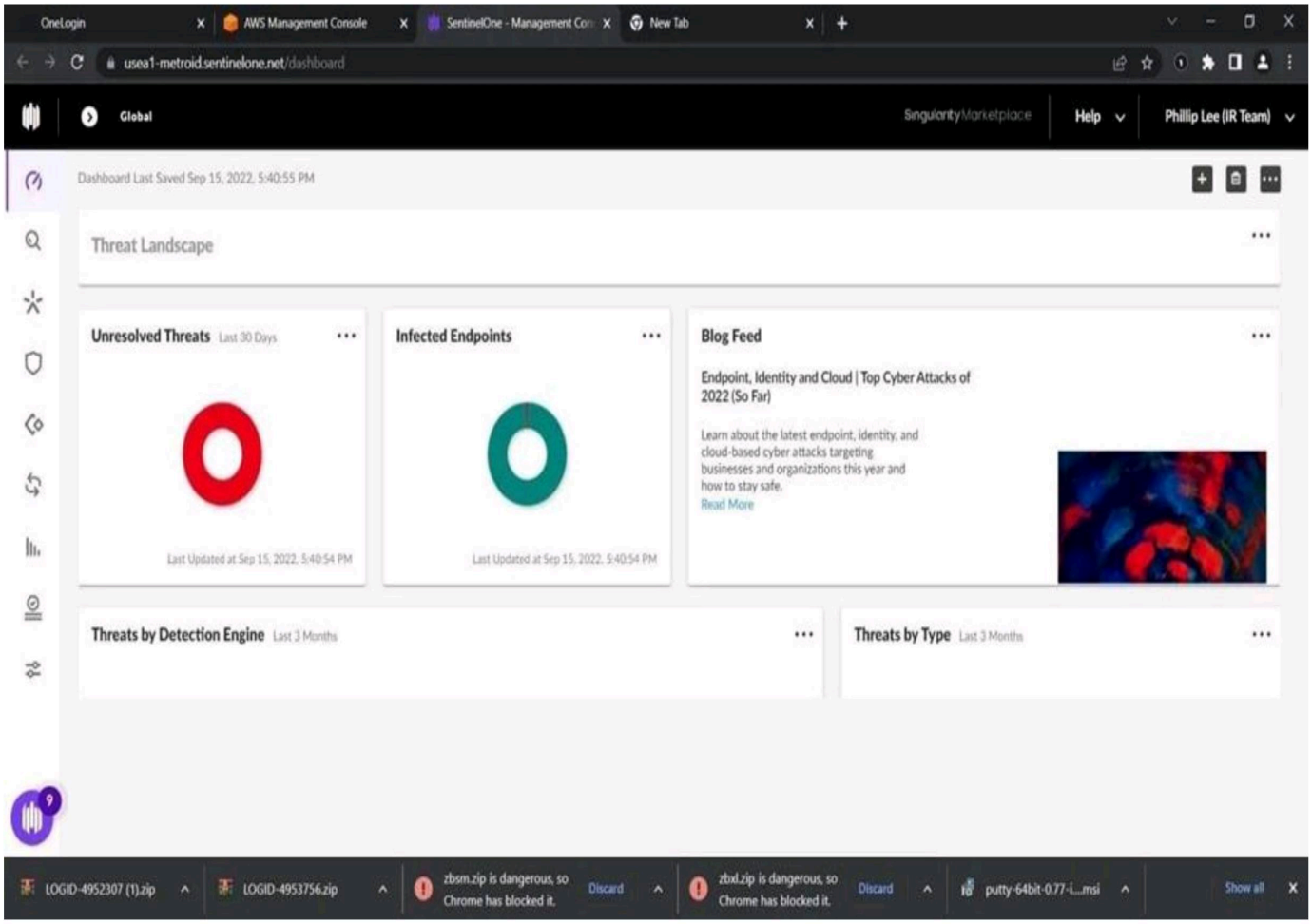


GOOGLE WORKSPACE

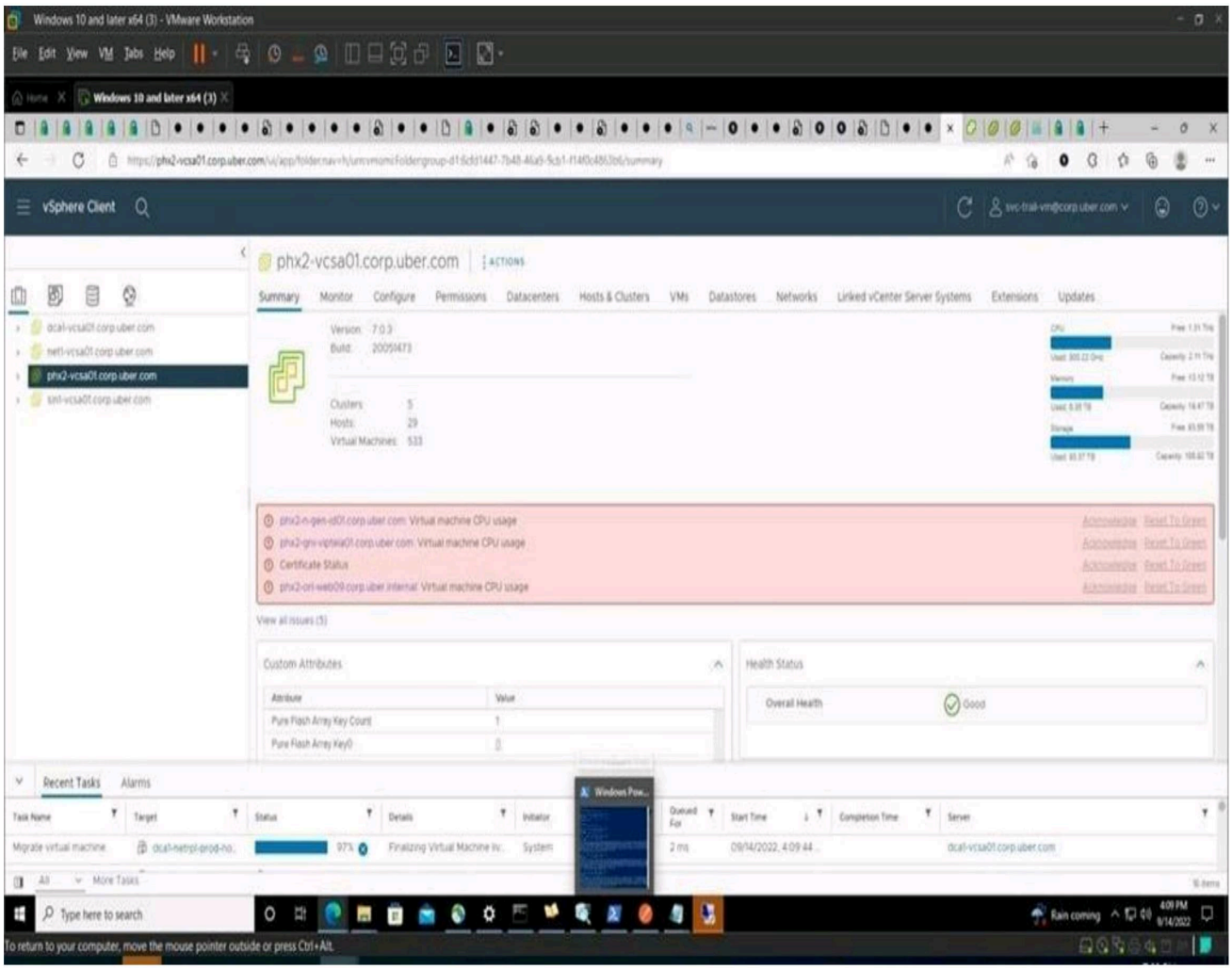
UBER BREACH 2022 AWS



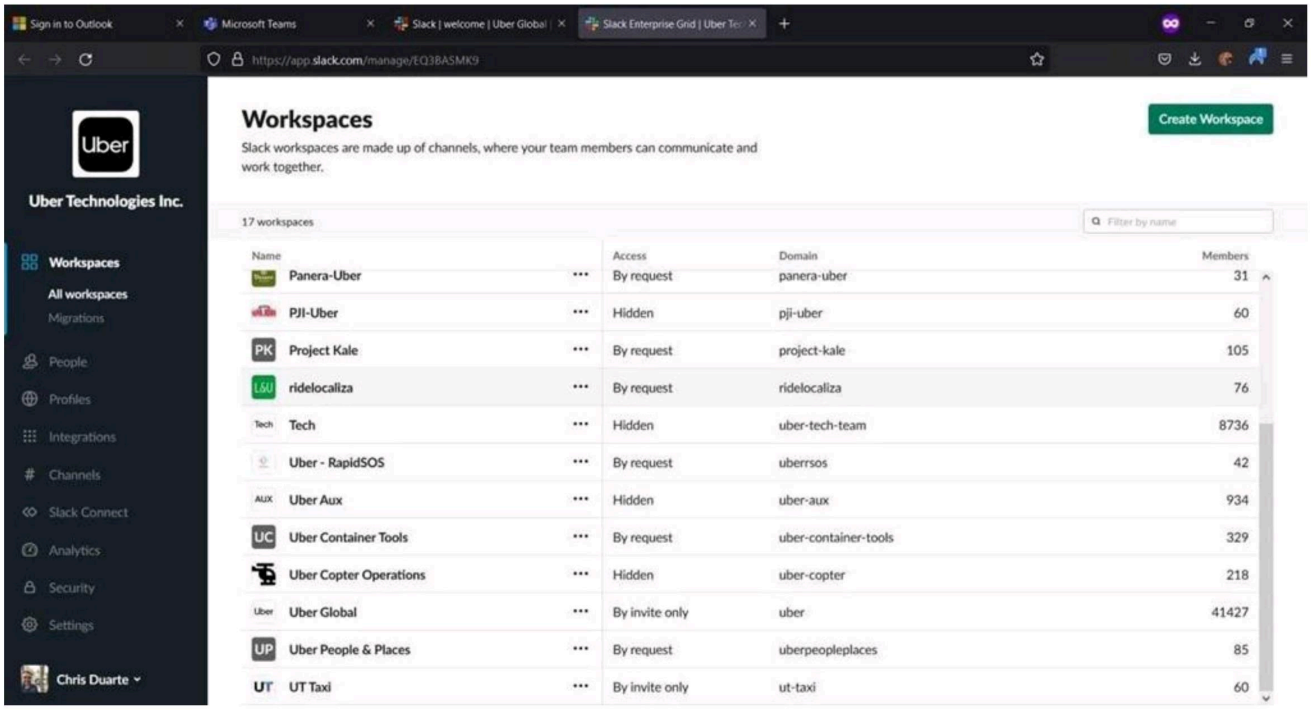
UBER BREACH 2022 SENTINALONE



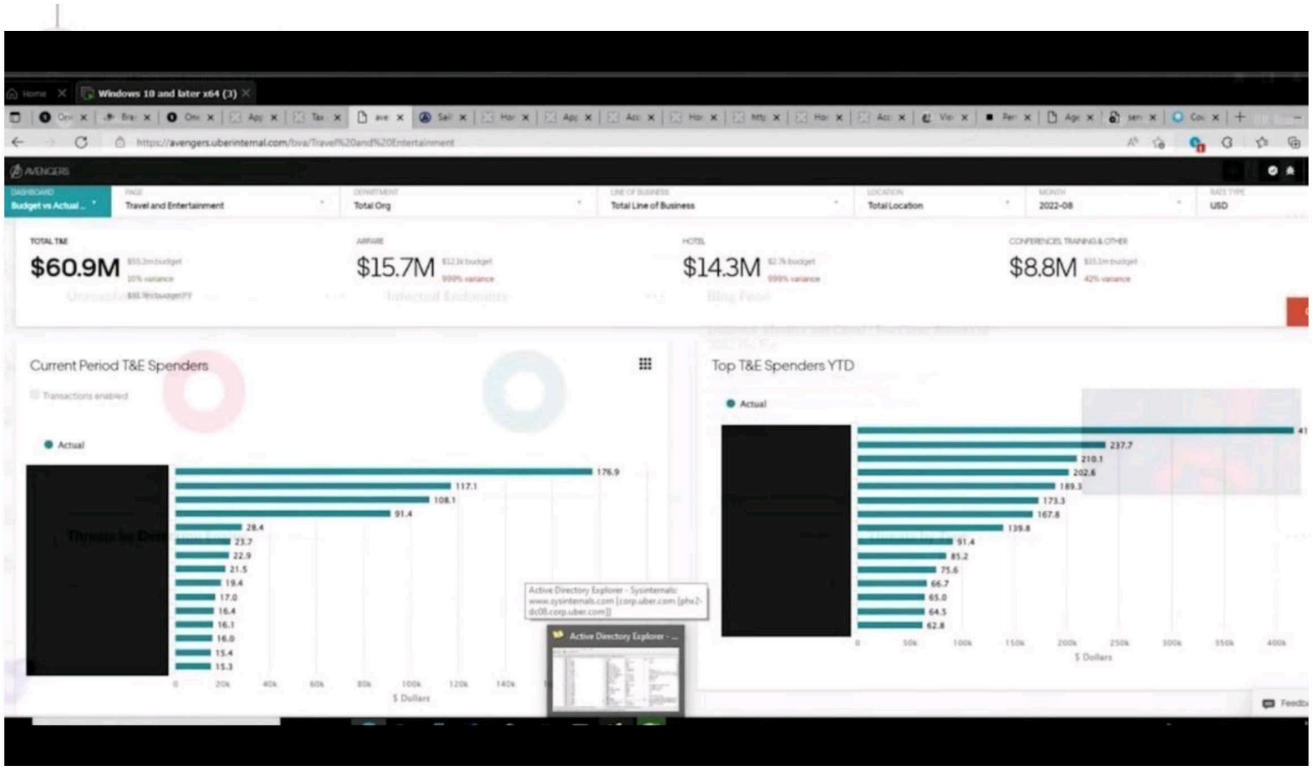
UBER BREACH 2022 vMware



UBER BREACH 2022 SLACK



UBER BREACH 2022 HACKERONE



Timeline of Key Events

Conclusion:

The crucial lesson from this Uber breach is that in today's evolving cybersecurity landscape, continuous training and putting people at the centre of security are paramount.Human error, often unintentional, can lead to dire consequences, making it crucial for organizations to invest in robust security awareness training. It's not just about technology; it's about bringing the culture of security and ensuring that employees are well-prepared and enabled to recognize & respond to threats efficiently. This human- centric approach is key to preventing cyberattacks and safeguarding sensitive data.

Moreover, the Uber breach highlights the significance of rapid incident response and transparent communication. Timely detection and swift action can mitigate the impact ofa breach, while open dialogue with stakeholders fosters trust and demonstrates a commitment to accountability and remediation.

Ultimately, the aftermath of the Uber cyberattack serves as a clarion call for organizationsacross industries to prioritize cybersecurity as a fundamental pillar of their operations. Bylearning from the missteps and oversights that led to this breach, companies can fortify their defenses, bolster resilience, and navigate the digital landscape with confidence and resilience in the face of evolving threats.

References

https://humanfirewall.io/the-uber-breach-case-study-cybersecurity-lessons-learned/

https://www.upguard.com/blog/what-caused-the-uber-data-breach

https://teampassword.com/blog/2022-uber-breach

https://www.linkedin.com/pulse/uber-breach-2022-10qbit-1c/