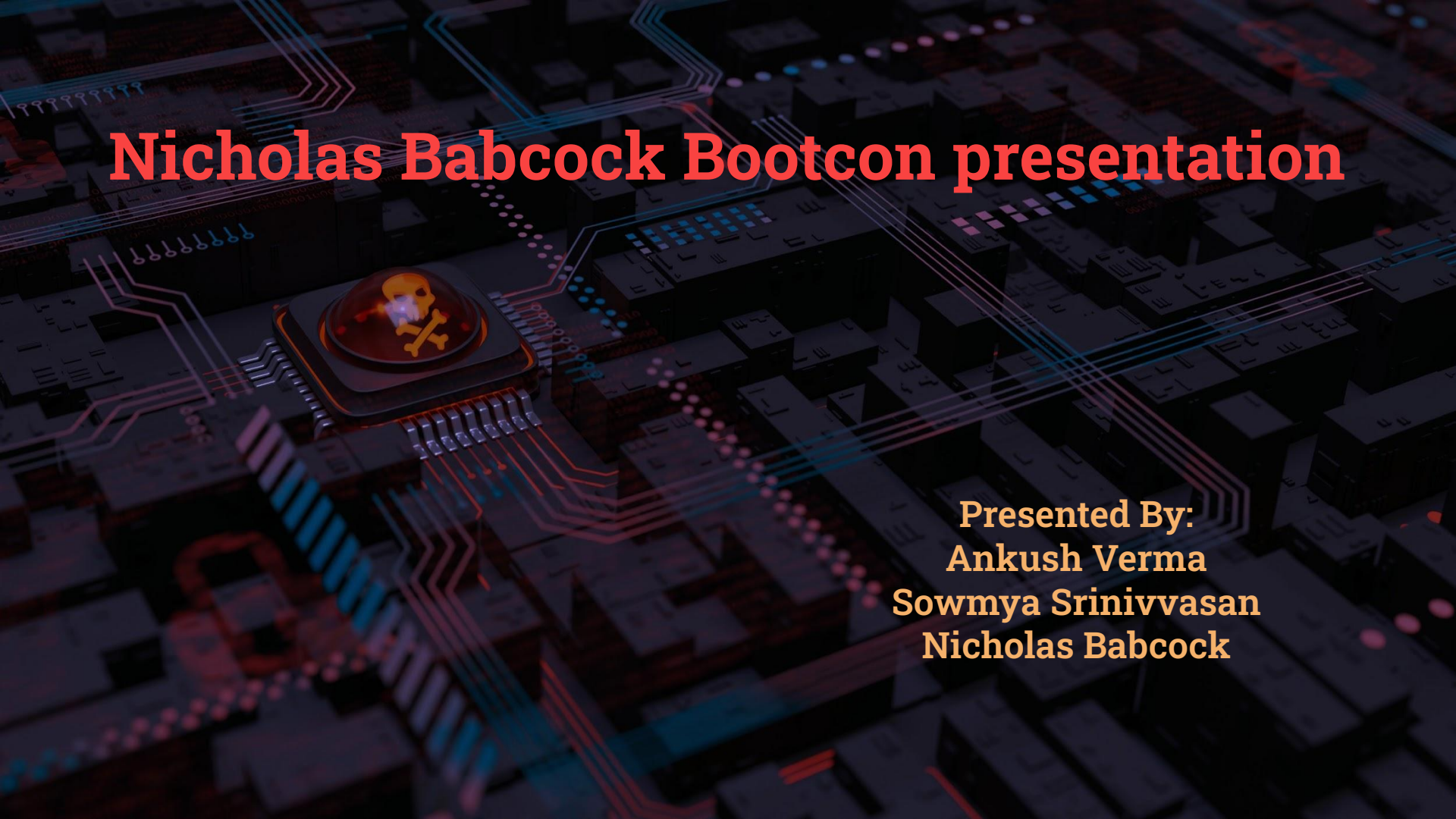
Nicholas Babcock Bootcon presentation



Presented By:
Ankush Verma
Sowmya Srinivvasan
Nicholas Babcock

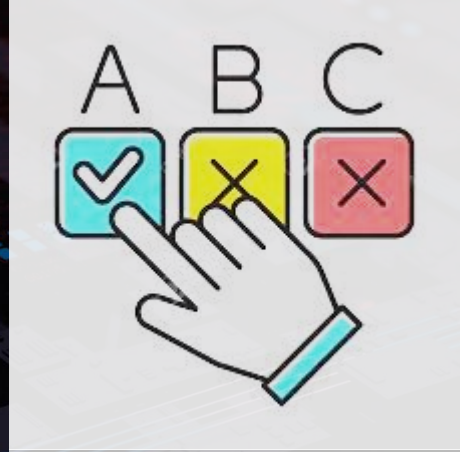
Introduction To Malware Analysis

- Malware analysis helps us understand how malicious code infects systems, spreads, and operates.
- It alters system files, manipulates the registry for persistence, and exploits network connections to steal data or contact C2 servers.
- Understanding these behaviors allows us to develop defenses, monitor threats, and prevent attacks.
- The more we analyze malware, the better we can protect our systems from future threats.

Project Goal

- Build a controlled, isolated environment to safely analyze malware without risking main systems.
- Observe malware behavior on both system and network levels to understand its lifecycle.
- Identify Indicators of Compromise (IOCs) to enhance detection and response strategies.
- Test and evaluate security tools to improve detection and prevention methods.

Why we chose Malware Analysis



- **Hands-On Learning Experience**
  - Provides practical exposure to malware analysis techniques
- **Threat Detection & Response**
  - Helps in identifying Indicators of Compromise (IoCs)
- **Safe Malware Analysis Environment**
  - Prevents real-world damage by containing malware in a sandbox
- **Relevance to Cybersecurity Roles**
  - Essential for red teamers, SOC analysts, and threat hunters

Concepts applied

Networking Concepts

- Command & Control (C2) Communication
- DNS Tunneling

Security Concepts

- Sandboxing
- Persistence Mechanisms
- Process Injection

Forensic Analysis Concepts

- Memory Forensics
- Log Analysis

Cryptographic Concepts

- Encryption & Obfuscation
- Decryption of Payloads

Tools Overview

- **Hardware & Virtualization**: VMware Workstation
- **Windows VM**: FLARE-VM for malware execution
- **Linux VM**: INetSim for network simulation
- **Monitoring & Analysis Tools**:
  - Sysmon(System Monitor) & Procmon(Process Monitor)
  - Wireshark (Network Analysis)
  - Volatility (Memory Forensics)

Flare-VM

- Pre-configured Windows based VM that was designed to be used in malware analysis and reverse engineering
- Allows the analysis of malware within a safe and isolated environment
- Allows analysis for both static and dynamic executions

INetSim

- Simulates network services during code execution, helping in the analysis
- Emulates protocols such as HTTP, DNS, FTP, SMTP and others for the malware to interact with
- Helps with identifying malware's network communication patterns
- Captures and logs suspicious network activity for analysis

Sysmon

- A Windows tool for detailed system event logging.
- Helps detect malware, attacks, and suspicious activity.
- Works with SIEM tools like Splunk.

Procmon

- Real-time process monitoring tool
- Monitors process creation & termination.
- Tracks file & registry changes
- Shows network activity & thread details.
- Filters & highlights suspicious behavior.

Wireshark

- A packet capture and analysis tool.
- Captures real-time network traffic.

Volatility

- Is an advanced memory framework that allows to you examine the memory dumps to identify malware, rootkits and others
- Used to detect hidden processes, code injections and other malicious executions within computer memory
- Volatility is powerful as it provides a CLI to aid in analysis and gives customization over our investigation

DEMONSTRATION


THANK YOU