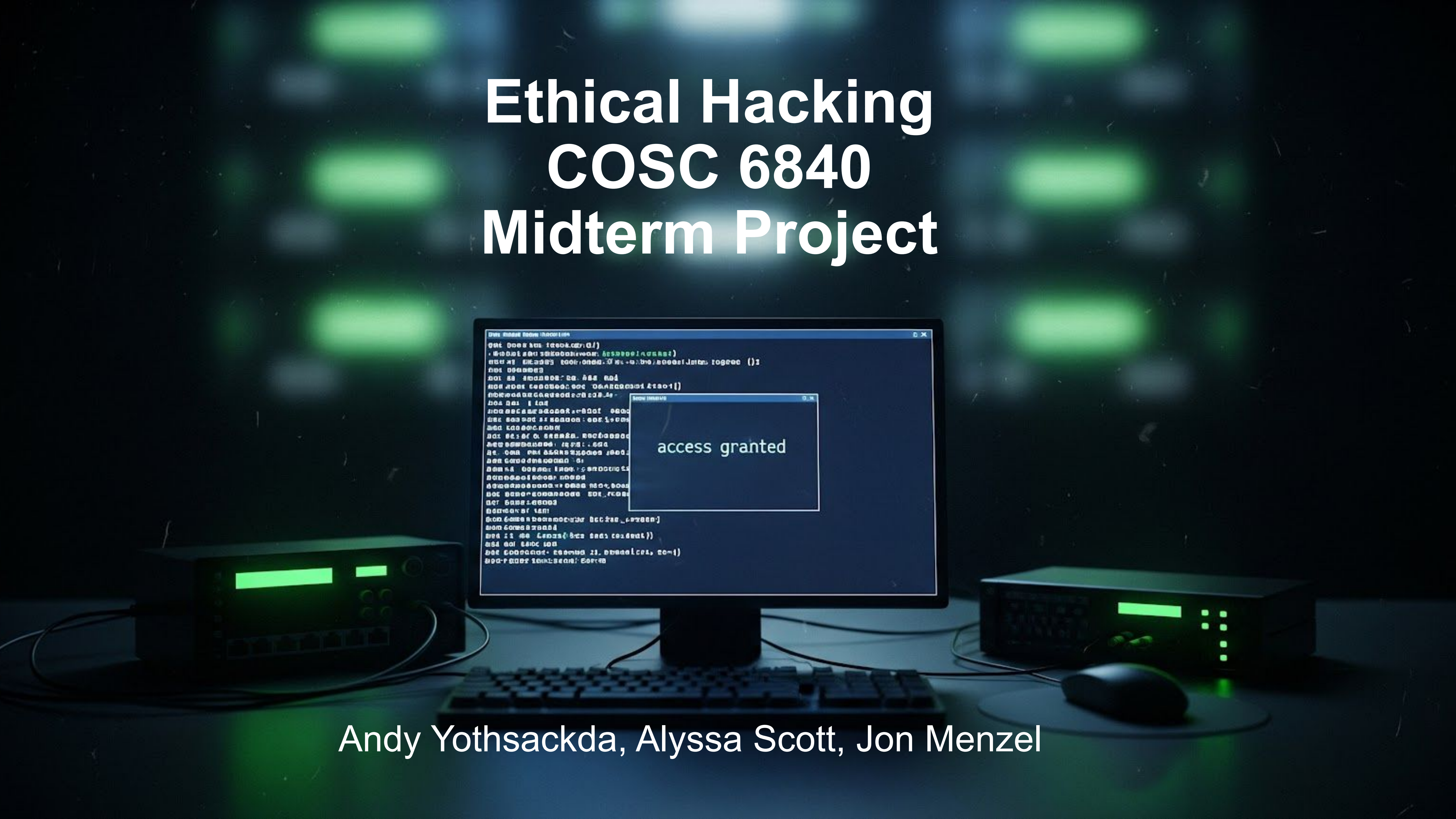
Ethical Hacking
COSC 6840
Midterm Project



Andy Yothsackda, Alyssa Scott, Jon Menzel

Introduction

Client: ThanosTech LLC

Scope: A Comprehensive Firmware Security Assessment

Objectives: Identify Vulnerabilities & Develop Automated Exploitation Script

Deliverables: Provide a Vulnerability Report, Proof-of-Concept Script, & Presentation

Methodology & Tools

- Ubuntu
- Visual Studio Code
- Python 3.10
- Binwalk
- Noseyparker

Vulnerability Findings Pt.1

Product: **TP-Link TL-WR841N**

- Vulnerability: Dropbearpwd Improper Authentication Information Disclosure
- Announced Date: May 2, 2024
- Dropbearpwd vulnerability (CVE-2023-50224) affects TP-Link TL-WR841N routers, allowing network-adjacent attackers to disclose sensitive information without authentication. (https://nvd.nist.gov/vuln/detail/cve-2023-50224)
- The flaw in the httpd service (TCP port 80) stems from improper authentication, enabling attackers to retrieve stored credentials from /tmp/dropbear/dropbearpwd and bypass HTTP Basic authentication. (https://www.tp-link.com/us/support/faq/4365/)

Vulnerability Findings Pt. 2

Product: **D-Link DCS-8000LH**

Initial Analysis Date by NIST: February 13th, 2019

Vulnerabilities

- D-Link DCS series Wi-Fi cameras expose sensitive device configuration information.
- This affects many DCS series models with firmware versions 1.00 and above.
- The configuration file is remotely accessible without authentication at <Camera-IP>/common/info.cgi.
- The file includes details like model, MAC address, IP address, and various device settings.
- https://nvd.nist.gov/vuln/detail/cve-2018-18441#:~:text=Description,cgi%2C%20with%20no%20authentication

Automation Script & Recommendations

- GitHub: https://github.com/jmenz-93/team-ftw-fw

Immediate Remediation (Critical Security Updates)

- Notify Customers on Vulnerability Findings
- Remove Hardcoded Secrets/Add Encryption to Plain Text Secrets
- Disable Insecure Management Interfaces
- Verify Firmware Integrity
- Update Core Components

Long Term Hardening (Configuration & Access Control)

- Integrate SonarQube into CI/CD for Code Quality Scanning
- Hire Ethical Hackers for PEN testing
- Require MFA/Security Keys for Device Access
- Ensure All Ports are Secured
- Have Cybersecurity work with Software Engineers to Develop Secure Code

Priority Focus:

Remove embedded credentials, disable Telnet/plaintext services, rotate exposed keys; Component updates.

thank you for listening