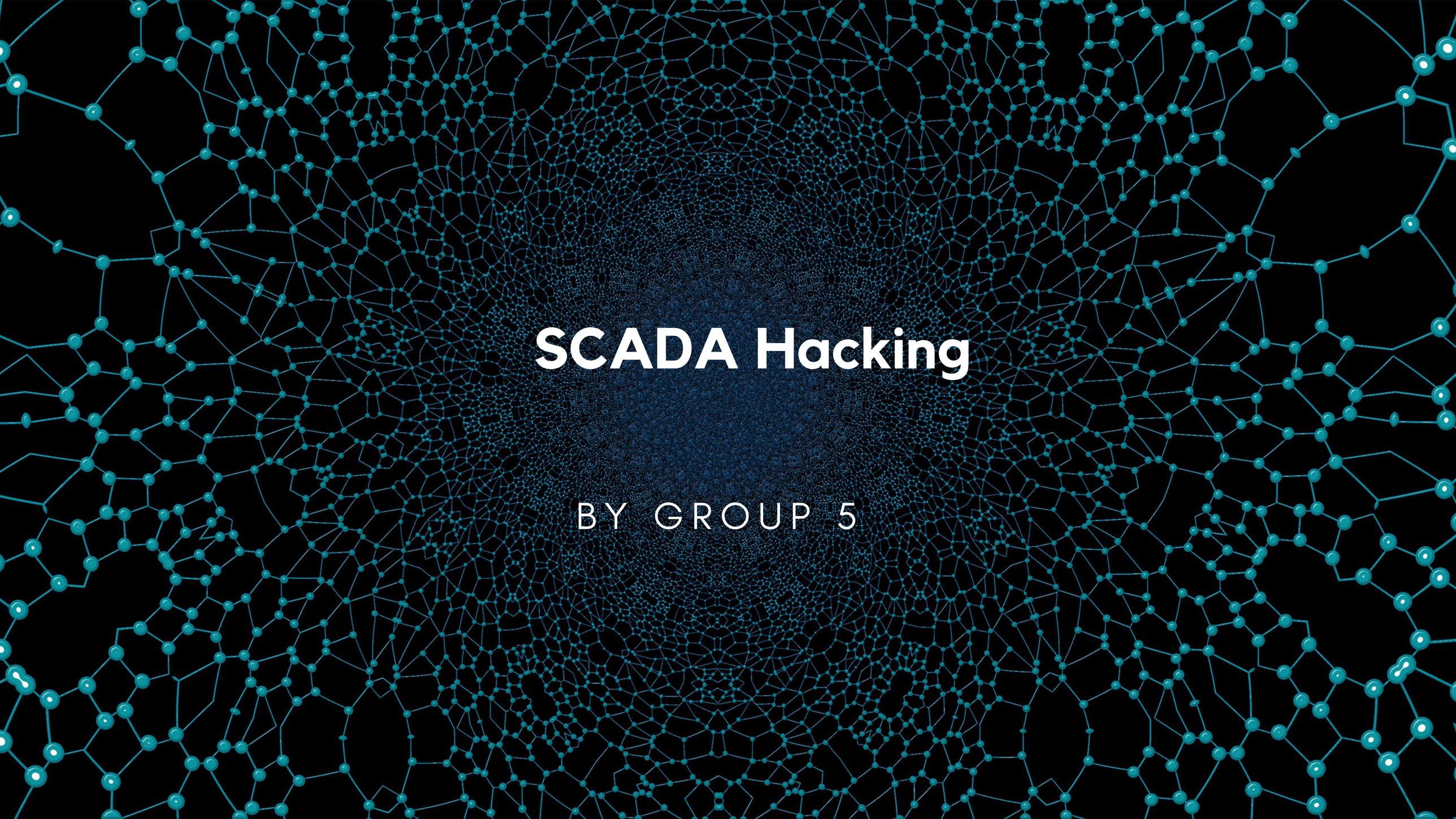


SCADA Hacking

BY GROUP 5

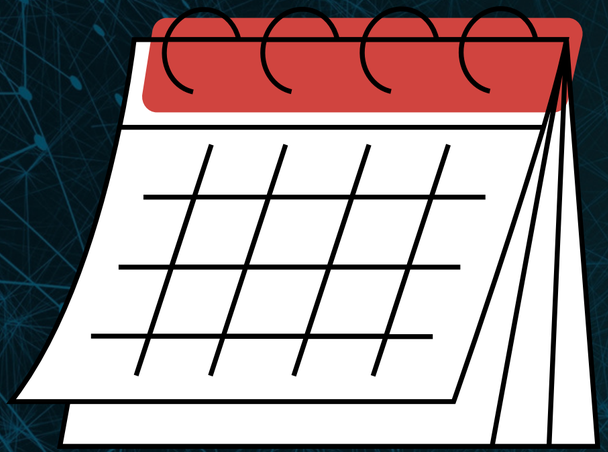
GROUP MEMBERS

1. Jayshree Karmakar 20BCY10042
2. Rupesh Kumar 20BCY10057
3. Priyam Dabli 20BCY10095
4. Shivam Kumar 20BCY10206
5. Samarth Rajput 20BCY10208

Our Guide

Dr. Muneeswaran V is working as Assistant Professor Sr. grade in the school of CSE, VIT Bhopal. He completed his B.E. (CSE) in the year 1999 from Madurai Kamaraj University, Madurai, and his M.E. (CSE) from Annamalai University, Chidambaram in the year 2005. He completed his Ph.D during 2021 in the area of Information Security from Anna University, Chennai. He has served in different academic and administrative roles at various academic institutes for more than 18 years. His research interests include Information Security, Quantum Cryptography, Data Science and Machine Learning. He has published 37 research publications in reputed International Journals/Conferences.

Project TimeLine:



Start of Project : 27 October 2023

Review 1: Planning Objective And Modules

Review 2: Done with Module 2 and 40% Demo(Practical)

Final Review: Completed Our all Module and
Full Demonstration with help of our mentor.

Introduction

Supervisory Control and Data Acquisition, or SCADA, is a system used in many industries, including in the nation's critical infrastructure, to help with maintaining efficiency, data processing and communicating issues for faster resolution. Part of this functionality is undoubtedly due to the injection of proverbial IT DNA into traditional processing systems.

Despite this, SCADA security is markedly different from IT security. This article will provide a high-level introduction to SCADA security and will explore the different types of ICS, ICS components, BPCS and SIS, and industrial control systems (or ICS) strengths and weaknesses from a security perspective.

Introduction

SCADA hacking refers to the unauthorized access, manipulation, or disruption of SCADA systems through various cyberattacks. These attacks can target both the hardware and software components of SCADA systems and can have serious implications, including:

1. Data Theft
2. System Manipulation
3. Service Disruption
4. Sabotage

Common Methods of SCADA Hacking:

SCADA hacking can occur through various methods, including:

1. Exploiting Vulnerabilities
2. Malware
3. Phishing
4. Insider Threats
5. Distributed Denial of Service (DDoS)

Objective

SCADA hacking can occur through various methods, including:

1. Gathering info online about scada devies
2. Developing attack methodology to target plc devices
3. Mapping the attack surface by threat actor
4. We would be making a project based on techniques used by Threat Actors to target the SCADA Devices like PLC (Programmable Logic Controllers).
5. Distributed Denial of Service (DDoS)

Proposed Work

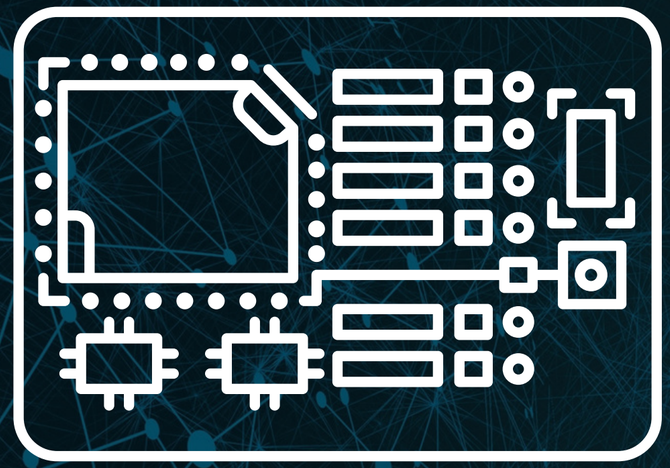
With ever changing cybersecurity the targets of the malicious threat actors have changed too. With rapid industrialization and our dependence on computers and automated programs to share our workload has grown rapidly. To impact and make a country suffer , this over depndence is harmful and often used as potential cyberweapon to mount attack on critical infrastrucutre like the Electric Power Plants, Water Dams, Food Industries, Automobile manuffacturing , etc. We will be demonstrating the techniques used by threat actors to attack critical infrastrucutre

Failures While Making Project:

SCADA hacking can occur through various methods, including:

1. Connectivity issues : We have faced restricted connection with HTTP server.
2. Geo Fencing: Security controls and inbuilt monitoring system may add delays , in execution and identity verification.

Module Description:



Module 1: Initial Reconnaissance

Module 2: OSINT

Module 3: OSINT-In-Depth & Attack Posture Development

Module 4: Demonstration

○ Module-1 Initial Reconnaissance

- Initial Reconnaissance: In this stage, the attacker researches the targeted company's systems and employees and outlines a methodology for the intrusion.
- The attacker may also search for infrastructure that provides remote access to an environment or look for employees to target for social engineering attacks.

Module-2 OSINT

- Open Source Intelligence (OSINT) is the collection, analysis, and dissemination of information that is publicly available and legally accessible. Right now, OSINT is used by a organizations, including governments, businesses, and non-governmental organizations. It is useful in information gathering for a wide range of topics such as security threats, market research, and competitive intelligence.
- OSINT collection methodologies
- edit
- Collecting open-source intelligence is achieved in a variety of different ways,[4] such as:
- Social Media Intelligence, which is acquired from viewing or observing a subjects online social profile activity.
- Search engine data mining or scraping.
- Public records checking.
- Information matching and verification from data broker services.

○ Module-3 OSINT in depth & attack posture

- Gathering information from public sources.
- Tools include search engines, social media, and specialized tools.
- Analyzing and correlating data for insights.
- Contributes to threat intelligence.
- Adheres to legal and ethical standards.

and attack posture Development :-

- Identify targets and assess vulnerabilities.
- Exploit weaknesses using malware, exploits, or social engineering.
- Escalate privileges and move laterally within the network.
- Establish persistence for long-term access.
- Exfiltrate data covertly.
- Cover tracks and evade incident response.
- Emphasizes ethical and legal considerations.

Literature Review

SCADA (Supervisory Control and Data Acquisition) hacking encompasses various approaches, often divided into two broad categories. The first involves exploiting software vulnerabilities and weaknesses in the SCADA systems themselves, such as insecure network configurations or outdated software. The second category pertains to social engineering and spear-phishing attacks, which target the human element within an organization to gain unauthorized access. These methods are part of a broader landscape of tactics that malicious actors employ to compromise critical infrastructure and pose significant cybersecurity challenges.

Attack Infrastructure

Attack Infrastructure Link: https://www.taskade.com/d/QfQa8hp7qT9gUTXX?share=view&view=6yDCafJUf7Yc4rYn&as=mindmap


Simulation Execution
1. Validate environment setup #EnvironmentValidation
1. Check hardware connections
2. Check software configurations
3. Test network connectivity
2. Perform attack simulation #SimulationExecution
1. Run attack scripts
2. Document system responses
3. Collect and analyze data #DataAnalysis
1. Record system behaviors
2. Analyze system logs
3. Identify successful and unsuccessful attacks
Post-Simulation Review
Evaluate attack outcomes #OutcomeEvaluation
eview attack methods
Assess system vulnerabilities
Compare expected and actual outcomes
Develop mitigation strategies #MitigationPlan
Propose system modifications
Recommend policy changes
Suggest training enhancements
Document and share findings #KnowledgeSharing
Write simulation report
Present findings to stakeholders
Distribute recommendat
improvement
Continuous Improvement
Incorporate feedback and lessons learned #ContinuousImprovement
Update attack scenarios
Enhance system configurations
Refine mitigation strategies
Schedule next simulation #FuturePlanning
Determine simulation frequency
Plan for next simulation
Set goals for future improvements

Demonstration

○ Future Prediction

Predicting specific future events, especially in the realm of cybersecurity, is challenging. However, it's likely that SCADA (Supervisory Control and Data Acquisition) systems will continue to be a target for hackers due to their critical role in controlling and monitoring industrial processes.

To address these potential threats, ongoing efforts in research, development, and implementation of robust cybersecurity measures will be essential. Collaboration between governments, industries, and cybersecurity experts will play a crucial role in building resilient SCADA systems for the future.

References

- M. Paquet-Clouston, B. Haslhofer, and B. Dupont, “Ransomware Payments in the Bitcoin Ecosystem,” 2018.
- D. Nieuwenhuizen, “A behavioural-based approach to ransomware detection,” 2017.
- D. Distler, “Malware Analysis : An Introduction.” SANS Institute, USA.
- S. Kok, A. Abdullah, M. Supramaniam, T. R. Pillai, and I. A. T. Hashem, “A Comparison of Various Machine Learning Algorithms in a Distributed Denial of Service Intrusion,” Int. J. Eng. Res. Technol., vol. 12, no. 1, pp. 1–7, 2019.
- J. A. Gómez-Hernández, L. Álvarez-González, and P. García-Teodoro, “R-Locker: Thwarting ransomware action through a honey file-based approach,” Comput. Secur., vol.73, pp. 389–398, 2018.
- https://www.youtube.com/watch v=O36wWU4TfrI&pp=ygURcmFuc29td2FyZSBhdHRhY2s%3D


THANK YOU