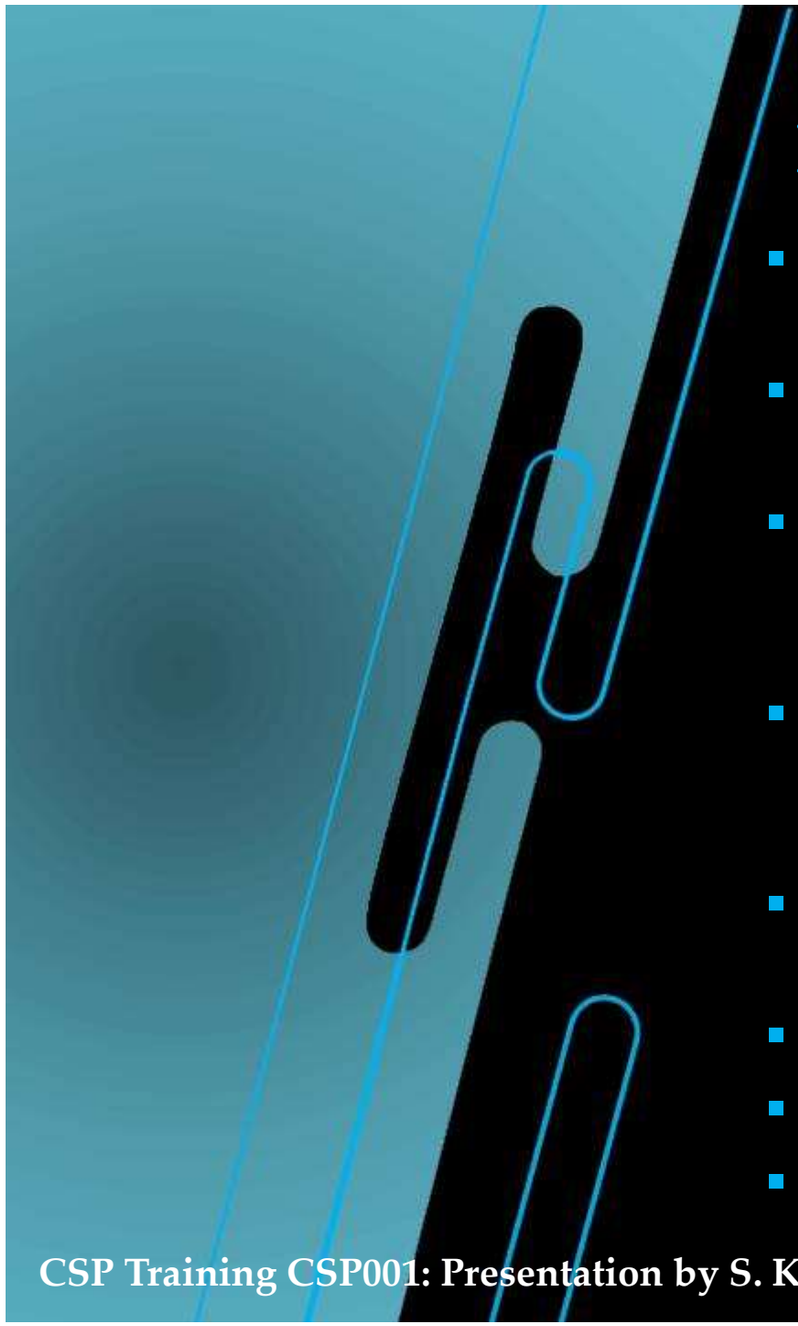
AI and Cybersecurity: Research in Maritime

CSP007

PRESENTATION BY: STYLIANOS KARAGIANNIS, (PDMFC, PORTUGAL)



Maritime Transport Systems Vulnerabilities

- VSAT is a device used to establish satellite communications, connecting ships to satellites for various purposes.
- SAILOR 900 VSAT High Power. This specific model of VSAT is equipped with a web server accessible via ports 80 and 443.
- Identified Vulnerabilities: Three vulnerabilities have been identified in the SAILOR 900 VSAT: CVE-2022-22707, CVE-2019-11072, and CVE-2018-19052.
- A proof of concept for exploiting CVE-2018-19052 has been made available on GitHub, allowing potential attackers to exploit this vulnerability.
- The web interface of the SAILOR 900 VSAT provides access to various functionalities including:
- Ship's location information
- Device details
- Satellite connection settings

Preventive Measures for Ship Hacking

Check and Block Exposure

- Evaluate devices connected to public networks.
- Block exposure of vulnerable devices to minimize risk.

Review Permissions and Security Settings

- Assess system requirements for public network connections.
- Ensure robust permissions and security settings to mitigate potential vulnerabilities.

Change Default Passwords

- Administer password changes for administrator accounts.
- Use strong, unique passwords to prevent unauthorized access.

Keep Devices and Systems Updated

- Regularly update all devices and systems.
- Install the latest security patches to address known vulnerabilities and enhance overall cybersecurity.

MITRE ATLAS

Knowledge base of adversary behaviors against ML systems.

Example: Poison Training Data

- Adversaries modify datasets to embed vulnerabilities.
- Vulnerabilities activated by data samples with Insert Backdoor Trigger.
- Data poisoning via ML Supply Chain Compromise or post-Initial Access.
- ID: AML.T0020
- Case Studies: VirusTotal Poisoning, Tay Poisoning

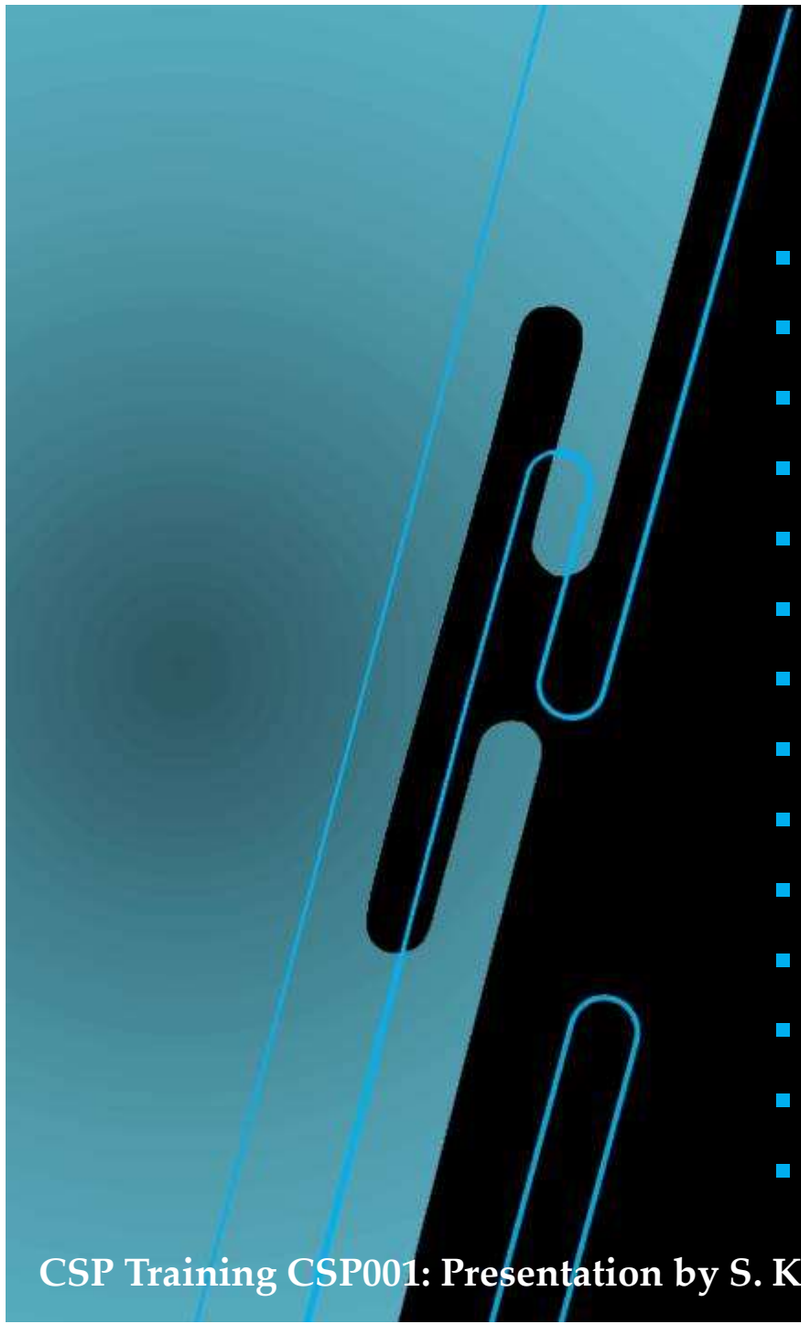
Mitigations:

- Limit Model Artifact Release
- Control Access to ML Models and Data at Rest
- Sanitize Training Data

Tactics:

Resource Development

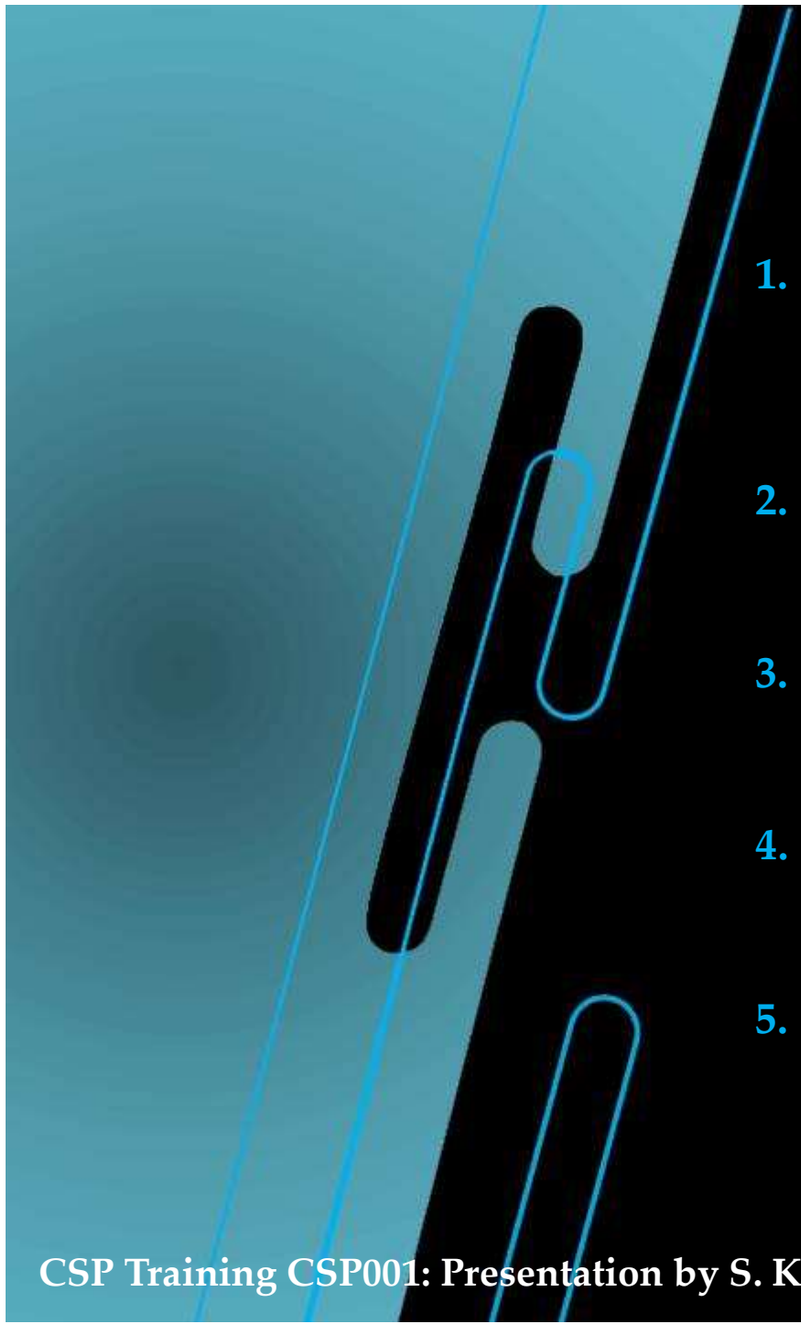
Persistence



MITRE ATT&CK FRAMEWORK

Adversarial Tactics, Techniques, and Common Knowledge

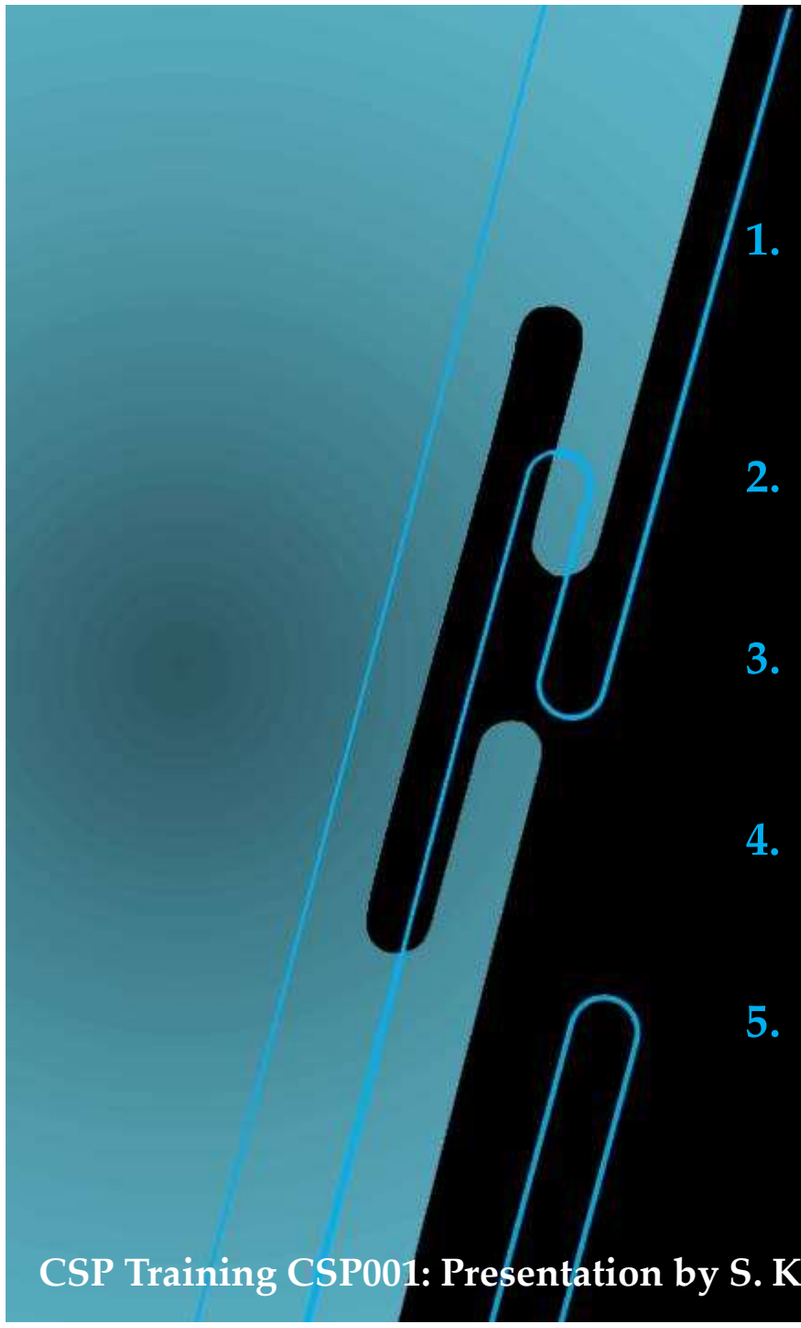
- **Reconnaissance:** Gather information for future operations.
- **Resource Development:** Establish resources to support operations.
- **Initial Access:** Gain access to the target network.
- **Execution:** Run malicious code.
- **Persistence:** Maintain progress.
- **Privilege Escalation:** Obtain higher-level permissions.
- **Defense Evasion:** Avoid detection.
- **Credential Access:** Steal account names and passwords.
- **Discovery:** Determine the target environment.
- **Lateral Movement:** Move through the target environment.
- **Collection:** Gather data of interest.
- **Command and Control:** Communicate with compromised systems.
- **Exfiltration:** Steal data.
- **Impact:** Manipulate, interrupt, or destroy systems and data.



MITRE ATT&CK in Maritime Pt.1

Adversarial Tactics, Techniques, and Common Knowledge

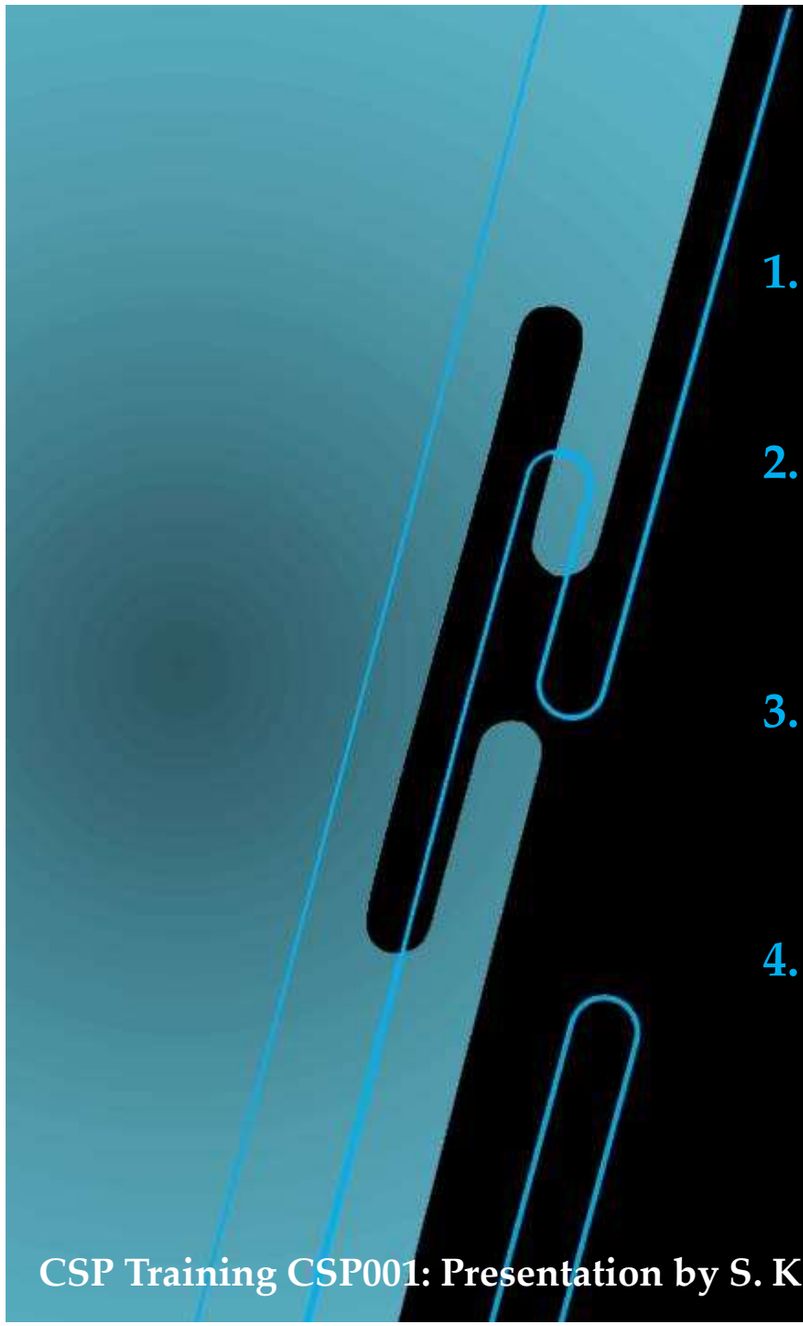
1. **Reconnaissance:** Gathering intelligence on vessel communication systems, port infrastructure, and maritime cybersecurity measures. Hackers researching vessel communication protocols and port cybersecurity defenses.
2. **Resource Development:** Acquiring tools and developing malware tailored to maritime systems. Cybercriminals developing malware designed to exploit vulnerabilities in ship navigation systems.
3. **Initial Access:** Exploiting vulnerabilities in vessel IT systems or port networks. Hackers gaining unauthorized access to a ship's onboard systems through a phishing attack targeting crew members.
4. **Execution:** Launching malicious code to disrupt vessel operations or compromise sensitive data. Malware deployed to manipulate navigation systems, causing a ship to deviate from its intended course.
5. **Persistence:** Establishing backdoors or maintaining access to compromised maritime systems. Hackers installing persistent malware on a vessel's systems to maintain control even after initial access is detected and mitigated.



MITRE ATT&CK in Maritime Pt.2

Adversarial Tactics, Techniques, and Common Knowledge

1. **Privilege Escalation:** Elevating access to critical maritime systems or data repositories. Hackers exploiting vulnerabilities to escalate privileges and gain access to sensitive cargo manifests or navigation controls.
2. **Defense Evasion:** Evading detection by maritime cybersecurity defenses. Malware designed to evade detection by antivirus software or intrusion detection systems onboard vessels.
3. **Credential Access:** Stealing maritime personnel credentials to gain unauthorized access. Cybercriminals compromising crew member accounts to access sensitive maritime systems and data.
4. **Discovery:** Mapping out vessel networks, identifying vulnerabilities, and potential targets. Hackers conducting network scans to identify vulnerable vessels with outdated cybersecurity protections.
5. **Lateral Movement:** Moving laterally within vessel networks to expand access and control. Hackers pivoting from compromised crew devices to shipboard control systems, such as engine controls or cargo management systems.



MITRE ATT&CK in Maritime Pt.3

Adversarial Tactics, Techniques, and Common Knowledge

1. **Collection:** Gathering sensitive maritime data or intellectual property. Cyber spies stealing proprietary shipping route information or cargo manifests for economic espionage purposes.
2. **Command and Control:** Establishing communication channels with compromised maritime systems. Cybercriminals using command and control servers to remotely manipulate vessel navigation systems or cargo handling equipment.
3. **Exfiltration:** Extracting stolen maritime data or valuable cargo information. Hackers exfiltrating sensitive cargo manifests or port security protocols for use in future attacks or for sale on the dark web.
4. **Impact:** Severe disruptions to vessel operations, maritime commerce, or critical infrastructure. Cyberattacks causing vessels to be stranded at sea or port operations to be paralyzed, resulting in significant financial losses and reputational damage.

MITRE ATT&CK in Maritime Ex.1

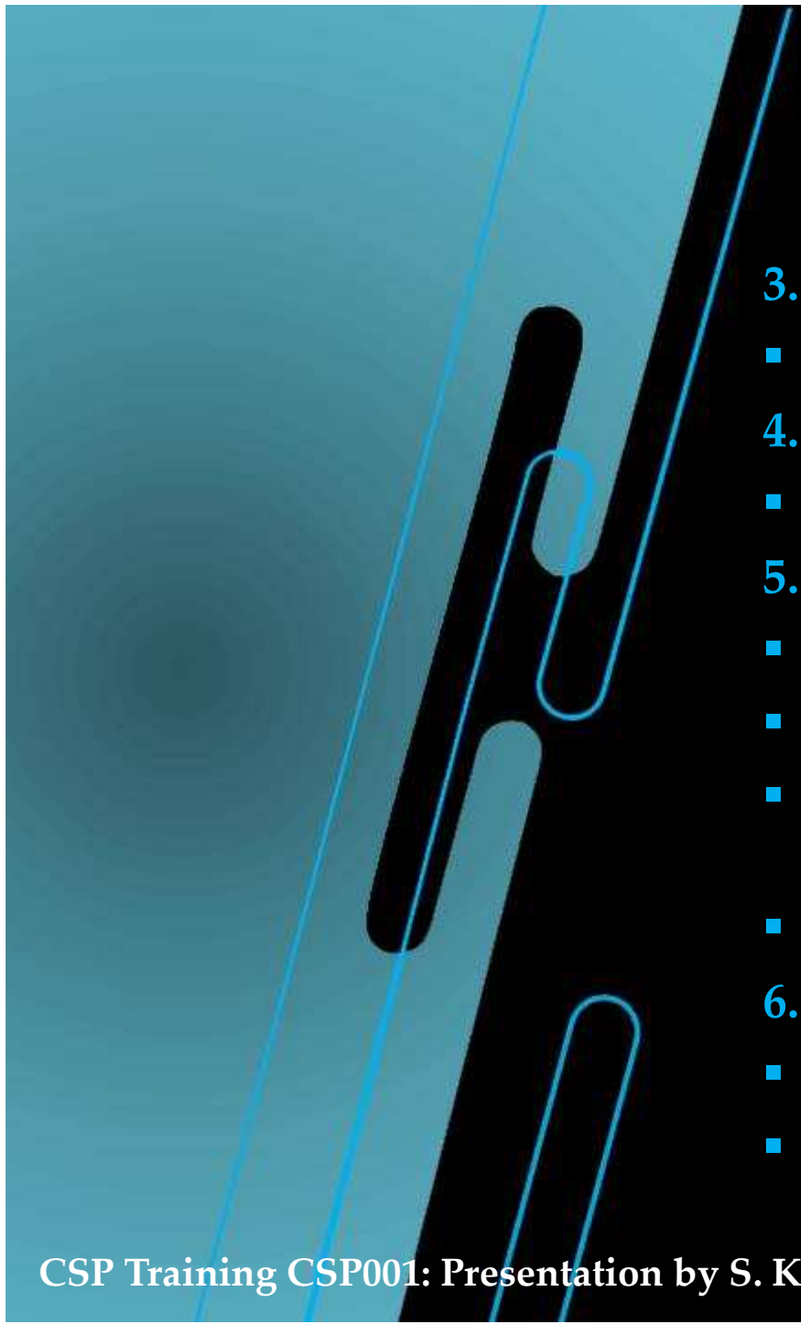
Adversarial Tactics, Techniques, and Common Knowledge

1. Reconnaissance

- The adversary obtains information on the equipment of the target ship.
- The adversary searches for marine satellite communication equipment.
- Attackers can utilize IoT search engines.
- Examples of search keyword in Censys: services.banner = “sailor 600”.
- The adversary obtains the BWMS password through the Social Network Service of the crew member.

2. Resource Development

- The adversary identifies the known vulnerabilities of maritime satellite communication terminals (CVE-2013-6034, CVE-2013-6035).
- Some satellite communication devices can be accessed using TCP port 1827 without authentication.
- The adversary identifies a valid account at the maritime satellite communication terminal.
- Some devices use the default account (“admin”)



MITRE ATT&CK in Maritime Ex.1

Adversarial Tactics, Techniques, and Common Knowledge

3. Initial Access

- The adversary accesses the onboard network with a valid account.

4. Lateral Movement

- The adversary accesses the BWMS via the onboard network.

5. Command and Control:

- The adversary attacks the BWMS attack surfaces.
- The adversary executes the BWMS attack vectors.
- The adversary modulates the pump data (running the port side pump or the starboard side pump).
- **The adversary turns off the pump alarm.**

6. Impact

- The ship sinks.
- The ship capsizes.

MITRE ATT&CK in Maritime Ex.2

Adversarial Tactics, Techniques, and Common Knowledge

1. Reconnaissance

- Acquiring ship boarding rights.
- Physically accessing the ECDIS software.

2. Initial Access

- Using the ECDIS factory default password (pw: 0000) to gain access.

3. Defense Evasion

- Loading a fake Windock DLL.
- Procedure for DLL injection attack
  - Attach the process.
  - Allocate memory within the process.
  - Copy the DLL or DLL path to the process memory and determine the appropriate memory address.
  - Instruct the process to run the fake DLL.
- Injecting the payload stored in the USB into the ECDIS.
- Activating the keyboard with the “Windows + R” keyboard shortcut.

MITRE ATT&CK in Maritime Ex.2

Adversarial Tactics, Techniques, and Common Knowledge

4. Persistence

- Executing the payload.

5. Collection

- Modifying the Winsock DLL file for a Man-in-the-Middle (MiTM) attack by the ECDIS software.

6. Command and Control

- Altering the NMEA command, causing the ship to go off course.

7. Impact

- Paralyzing the ECDIS (blue screen).
- Stranding the ship.
- Causing the ship to go off course.

Thank you

Organization: PDMFC

Please send all questions to:
stylianos.karagiannis@pdmfc.com