OTLab 11

AiTM MFA Bypass

Prof. Dr. Luiz Fernando Freitas-Gutierres (a.k.a. substationworm)

`linkedin.com/in/lffreitas-gutierres`

`github.com/substationworm/OTLab`

`luiz.gutierres@ufsm.br`

Problem Overview

Containerized Hosts

- `user-browser` (*victim workstation*): The legitimate client system used by the operator to access the industrial web interface. This workstation is the target for credential harvesting and session compromise.
- `phishing-proxy` (*AiTM phishing proxy*): A malicious service that transparently relays communications between the victim workstation and the legitimate HMI server while capturing authentication credentials and session cookies.
- `legit-hmi` (*authorized HMI server*): The legitimate HMI system that provides operational control and monitoring services within the industrial environment.
- `attacker` (*adversary*): The threat actor who deploys and manages the phishing infrastructure in order to conduct credential theft, session hijacking, and access persistence.

Tasks

1. Access the victim container (`user-browser`) and open the text-based web browser using the following command: `elinks http://phishing.test`. *The user assumes they are accessing the legitimate HMI system; however, in reality, they are connecting to a spoofed malicious domain engineered to closely resemble the authentic HMI address.*

2. Authenticate using the following credentials: `operator` (username), `otlab123` (password), `000111` (MFA code). After successful authentication, explore the HMI web interface. Do not log out at this stage.

3. In a separate terminal session, access the `attacker` container and execute this command: `tail -f /loot/cookies.log`. *The phishing proxy will intercept and log the victim's session cookie, enabling MFA bypass and session takeover.*

4. Assign the captured session cookie to a variable named `COOKIE` on the `attacker` system. Then reuse the cookie to access the application through the phishing proxy: `curl -H "Cookie: ihm_session=$COOKIE" -H "Host: phishing.test" http://172.30.0.20/home -L`. Successful access without MFA confirmation is expected.

5. On the `attacker` system, test direct access to the authorized HMI server using the stolen cookie: `curl -H "Cookie: ihm_session=$COOKIE" http://legit-hmi:8000/home` or `curl -H "Cookie: ihm_session=$COOKIE" -H "Host: legit.test" http://172.30.10.40:8000/home`. *This step simulates an attack scenario in which an adversary reuses a valid session token directly against the legitimate infrastructure. This technique mirrors attacks commonly observed against SaaS platforms (e.g., Office 365), VPN gateways, and, in this exercise, an OT-ICS system.*

6. Perform a global logout by clicking `Log out` in the `user-browser` session. Afterward, attempt to reuse the cookie again from the `attacker` system: `curl -i -H "Cookie: ihm_session=$COOKIE" -H "Host: phishing.test" http://172.30.0.20/home`. *The request should be redirected to the login page, indicating the session is invalid. This demonstrates the effectiveness of global logout mechanisms as a defensive control. The* `attacker` *would now be required to capture a new session cookie to regain access.*

Tools

The following tools are available for completing OTLab 11: `curl`, `elinks`, and `tail`.

Nomenclature

- AiTM: Adversary-in-the-middle.
- HMI: Human-machine interface.
- ICS: Industrial control system.
- MFA: Multi-factor authentication.
- OT: Operational technology.
- SaaS: Software as a service.
- VPN: Virtual private network.