AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AttackBed

A Damn Vulnerable Network for Profit and Fun

Wolfgang Hotwagner

June 26, 2026

Introduction

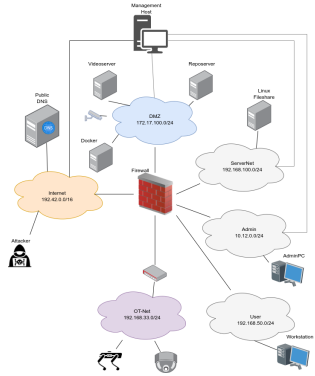
$ whoami?

Motivation for simulating networks

- Generate realistic data
- Demonstration
- Reproducible research
- Test and evaluate log analysis tools

Src: https://imgflip.com/i/av36ch

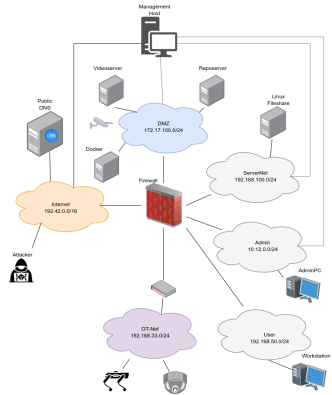
What is it?



AttackMate

Attackbed

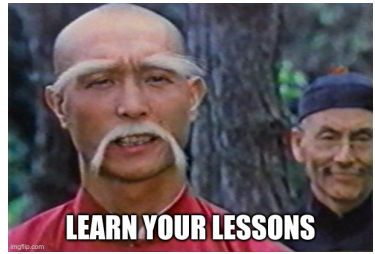
- packer -> ansible -> terraform
- Simulate Vulnerable Company Network
- Different Attack-Chains
- OT-Support
- Management-Host
- Fake Internet
- Reproducible



Kyoushi 2.0

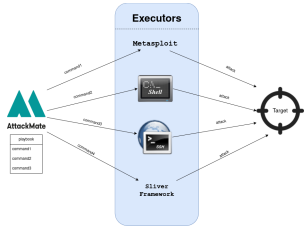
Lessons Learned

- Use most simple ansible/terraform code
- Create images
- Redundant config/code is okay
- Static networks are okay
- No production code
- New structure: Scenario based



Src: https://imgflip.com/i/av2tzc

AttackMate



Src: https://github.com/ait-testbed/attackmate

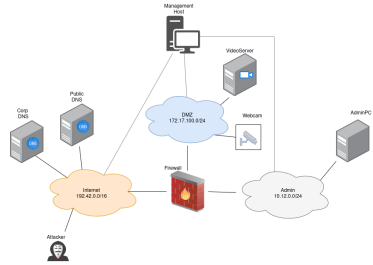
- Reproducible Attack-Chains
- Portable Playbooks
- For every phase of the killchain
- Realistic attacks
- Real Tools and exploits

Scenarios

Videoserver Scenario

Privilege Escalation

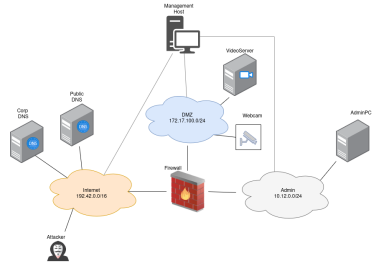
- DNS-Scan
- Nmap-Scan
- Web-Scan
- ZoneMinder Exploit
- 6 different PrivEsc
- 3 different Persistency methods



Linux Malware Scenario

Malware and Rootkit

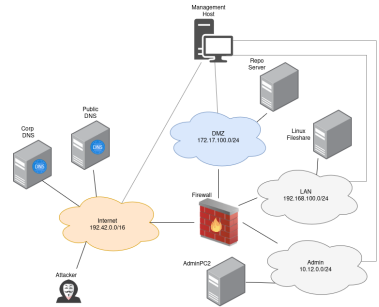
- Zoneminder Exploit
- 2 different Persistency methods
- Sliver installation
- Malicious activity
- Rootkit installation
- Malicious activity hidden



Lateral Movement Scenario

From DMZ to Servernet

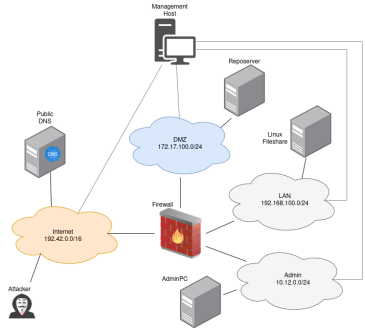
- Bruteforce: ssh or vnc
- Sniffed credentials from a FTP-Connection
- Lateral movement
  - writeable share
  - buffer overflow exploit
  - apt repository
  - puppet configuration management
- 5 different impacts on host (including ransomware)



Network Scenario

Portknocking

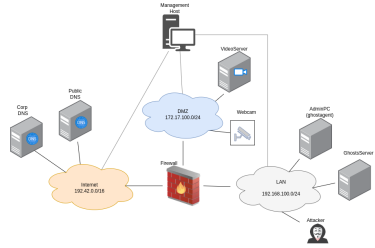
- Hacker gains access on Firewall
- Installs portknocking mechanism
- Portknocking sequence triggers install and exec of malware
- Add IPtables rules to gain access on internal machine



LAN-Turtle Scenario

Adversary in the Middle

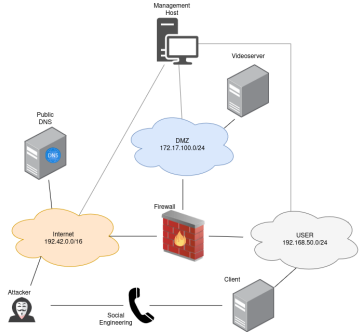
- Hacker is in Network
- Arpspoofing to AitM
- Sniff session-id
- Use session-id to gain access



Client Scenario

Phishing

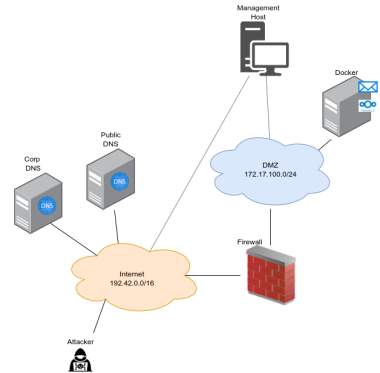
- Office Macro / Screensharing-App
- Icmp-Exfiltration
- Alternative: Malicious Browser Extension



Docker Scenario

Nextcloud and Mail

- SMTP-Enum
- Bruteforce IMAP
- Nextcloud Exploit
- Access to docker-daemon
- Deploy malware-container

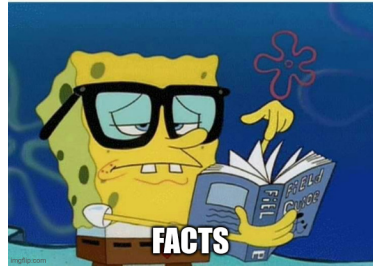


MITRE Enterprise

Techniques

Facts and Numbers

- 8(?) Scenarios
- 35 Unique Attack-Chains
- 699 Techniques
- 90 Unique Techniques



Src: https://imgflip.com/i/av3j14

Exploits

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Public

- Zoneminder Metasploit
- Nextcloud Metasploit
- healthcheck

Src: https://imgflip.com/i/av3bx1

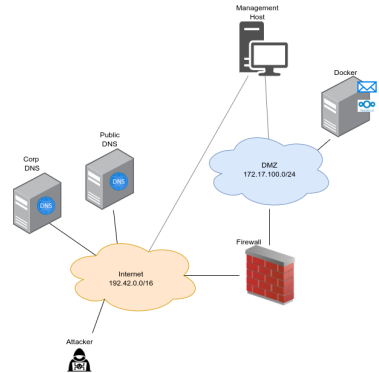
Papers

- CAM-LDS: Cyber Attack Manifestations for Automatic Interpretation of System Logs and Security Alerts
- AttackMate: Realistic Emulation and Automation of Cyber Attack Scenarios Across the Kill Chain
- Resource-Aware Deployment Optimization for Collaborative Intrusion Detection in Layered Networks
- The AInception Dataset https://zenodo.org/records/17659656
- Dynamic Shields: A Game-Theoretic Reinforcement Learning Framework for APT Mitigation

Demo

Nextcloud and Mail

- SMTP-Enum
- Bruteforce IMAP
- Nextcloud Exploit
- Access to docker-daemon
- Deploy malware-container



Use cases?

Applications

Conclusio

- OpenSource Framework for Testbeds and Attacks
- Sophisticated Attacks-chains
- Many techniques covered
- Realistic attacks

Resources

- https://github.com/ait-testbed/attackbed
- https://github.com/ait-testbed/attackmate
- AttackMate Talk: https://www.youtube.com/watch?v=jaJAvCBL040

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Thank You!

Wolfgang Hotwagner