FORTRA

RED TEAM USE CASE

Hospital Network

Background

A regional hospital network conducts a Red Team engagement to evaluate its cybersecurity defenses. The exercise aims to simulate a sophisticated cyberattack targeting patient data, medical devices, and critical infrastructure, testing the hospital's ability to detect, respond to, and recover from an intrusion.

Phase 1: Initial Access Operations

The Red Team begins by gathering intelligence on the hospital network's employees, vendors, and third-party service providers.

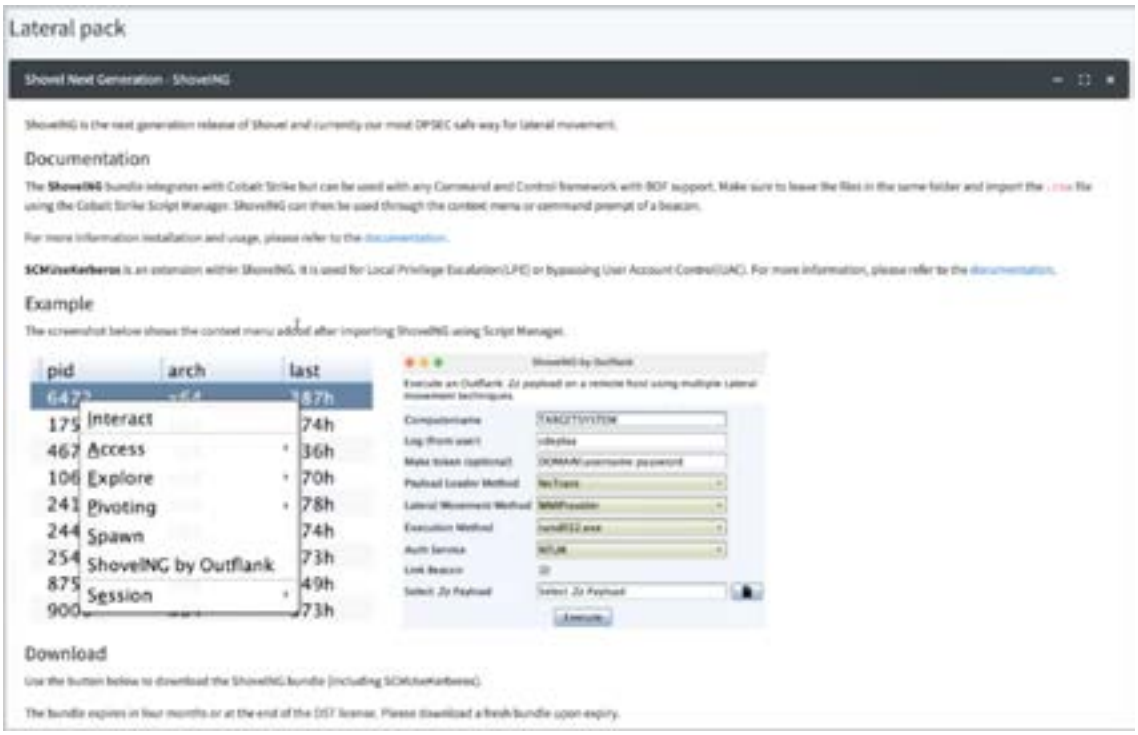
- Reconnaissance: They identify a vulnerable third-party billing vendor with weak cybersecurity controls.
- Spear Phishing Attack: Using social engineering, the Red Team sends a phishing email to a vendor employee, impersonating the hospital network's IT department. The email contains a malicious link that deploys a payload generated using Outflank Security Tooling's (OST's) PE Payload Generator when clicked.

- Web Drive-By Attack: The Red Team also compromises a medical industry website frequently visited by hospital staff, injecting a browser exploit to gain initial access.

Phase 2: Lateral Movement & Privilege Escalation

Once inside the hospital network network, the Red Team moves laterally and escalates privileges:

- Credential Harvesting: Using Credential Pack, they extract cached credentials from compromised workstations.
- Lateral Movement: They pivot across the network, accessing electronic health record (EHR) systems and connected medical devices using Lateral Pack.



- Privilege Escalation: Exploiting a misconfigured domain controller, they elevate privileges to a domain admin level using Impacket, allowing unrestricted access.

Phase 3: Maintaining Persistence & Evasion

To remain undetected, the Red Team establishes multiple persistence mechanisms:

- Quiet Transmission: They use DNS over https tunneling and encrypted HTTPS communication through Cobalt Strike to exfiltrate data without triggering alerts.
- Asynchronous Communication: A covert Beaconing technique allows them to maintain control over compromised systems while avoiding detection.

Phase 4: Targeted Attack Scenarios

The Red Team simulates real-world cyber threats targeting healthcare infrastructure:

- Medical Device Exploitation: They compromise an IoT-connected MRI scanner, demonstrating how attackers could manipulate scan results or disrupt patient care.

- Ransomware Deployment: Using Ransomware Simulator, they encrypt non-essential patient records to test the hospital's incident response plan.
- Data Exfiltration: They exfiltrate sensitive patient data, including medical histories and insurance records, highlighting potential HIPAA violations.

Phase 5: Red Team Engagement & Blue Team Training

This exercise involves collaboration between offensive and defensive teams:

- Shared Sessions: The Red Team provides real-time insights into attack methodologies.
- Extensive Logging: Every action is documented for forensic analysis and post-engagement review .
- Purple Team Exercises: The Blue Team improves detection capabilities based on Red Team findings.
- Incident Response Drill: The hospital's cybersecurity team practices containment, eradication, and recovery strategies.

Outcome & Lessons Learned

- Identified Weaknesses: Gaps in third-party security, endpoint detection, and network segmentation were exposed.
- Security Improvements The hospital network implements multi-factor authentication (MFA), network segmentation, and enhanced monitoring for medical devices.
- Enhanced Preparedness: The hospital now conducts regular Red Team engagements to maintain a proactive security strategy.

This Red Team exercise demonstrates how healthcare organizations can identify and mitigate cyber risks before real attackers exploit them, ensuring patient safety and data security.

FORTRA

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.