FORTRA®

CASE STUDY (PENETRATION TESTING SOFTWARE FOR A HOSPITAL)

Enhancing Hospital Cybersecurity with Automated Penetration Testing Software

Preconditions:

- The hospital network, systems, and applications are connected and operational.
- The penetration testing software is licensed, installed, and configured.
- Scope is clearly defined to avoid disruptions to patient care.

Workflow:

1. **Define Scope and Targets**
   Hospital systems including the patient portal, EHR, IoT devices and internal network are selected for testing.
2. **Run Reconnaissance and Scanning**
   The software maps the network, identifies open ports, services, and operating systems.
3. **Exploitation and Attack**
   The tool safely runs exploits associated to known vulnerabilities (CVE based) and also looks automatically for injection vulnerabilities on Web Applications, runs privilege escalation exploits on compromised targets, does credential harvesting, and simulates ransomware propagation.
4. **Analyze Results and Risk Levels**
   Vulnerabilities are prioritized based on exploitability and business impact (e.g., a flaw in the EHR system is rated as critical).
5. **Generate Reports**
   Reports are created for IT teams (technical detail) and for executives (risk overview, compliance gaps).
6. **Remediation and Retesting**
   After fixes are applied, the software is used to verify that vulnerabilities have been properly mitigated.

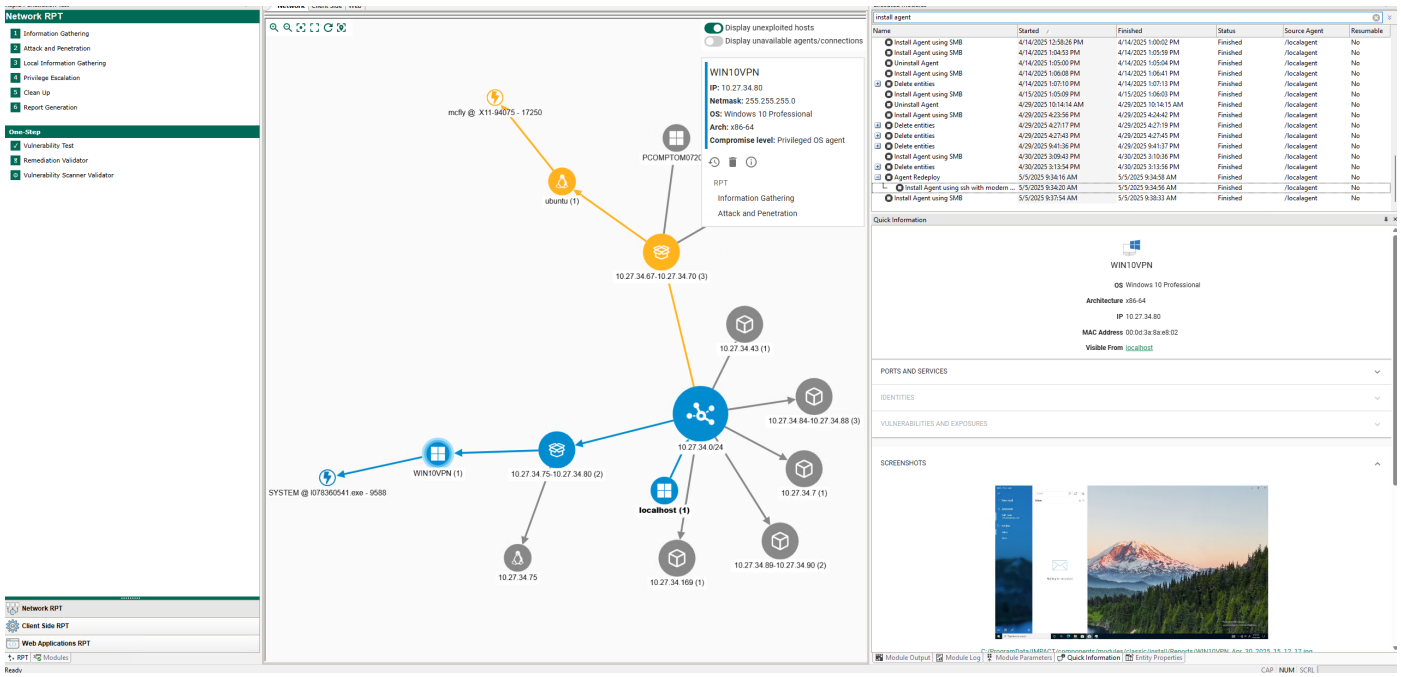
AT-A-GLANCE

OBJECTIVE:

To continuously assess and strengthen the hospital's cybersecurity posture using automated penetration testing software that simulates attacks on digital assets and networks.

ACTORS:

- **IT Security Team:** Uses the software to identify vulnerabilities.
- **Compliance Officer:** Monitors compliance with HIPAA and cybersecurity standards.
- **Hospital Management:** Reviews reports and allocates resources based on risk findings.
- **Penetration Testing Software** (e.g., Core Impact): Performs automated discovery, remote exploitation , lateral movement and privilege escalation, and reporting.



Example Outcome:

- Discovered outdated firmware on Wi-Fi access points vulnerable to remote code execution
- Detected hardcoded credentials on networked medical imaging systems
- Found misconfigured file permissions exposing PHI to all employees

Benefits:

- Ongoing, scalable, and repeatable security assessments
- Reduced reliance on costly manual testing
- Early detection of vulnerabilities before attackers exploit them
- Supports regulatory compliance (HIPAA, NIST, ISO 27001)
- Protects patient data and hospital operations

Postconditions:

- Security posture is improved
- Compliance reports are ready for audit
- A schedule is created for periodic testing (e.g., quarterly)

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.