



Leading the Convergence of National Security and TechnologySM

North Dakota 2013 IT Security Audit Vulnerability Assessment & Penetration Test Project Briefing

ManTech Project Manager

Mark Shaw, Senior Executive Director
Cyber Security Solutions Division
ManTech Mission, Cyber, and Intelligence Solutions Group
mark.shaw@mantech.com
(703)388-2126



- Assessment conducted November 2013-January 2014
- 5 Major Project Tasks
 - External Vulnerability Assessment
 - Internal Vulnerability Assessment
 - Application Vulnerability Assessment
 - Security Assessment of Non-consolidated IT Services
 - Penetration Testing



- A Network Vulnerability Assessment targets an organization's IT infrastructure (network, servers, workstations, etc) with the goal of identifying security weaknesses that could be exploited
- External assessments are conducted from the Internet and mirror the threat of a malicious outsider (ie- hacker)
- Internal assessments are conducted on an internal corporate network and mirror the threat of a malicious insider



- Assessment methodology
 - Commercial vulnerability scanning software used initially to identify all systems connected to the network and the services they are providing (ie- web server, email server, file server, workstation, etc)
 - Scanning software then runs a series of automated checks to identify vulnerabilities in the installed software and system configurations/settings
 - Test team then validates the results of the automated scans and conducts manual reviews of the identified systems



- Assessment methodology (continued)
 - Once the Test team has completed review, the consolidated findings are be presented in a written technical report which identifies the vulnerabilities found during the assessment along with specific remediation recommendations for how to correct the findings and properly secure the system.



- External Assessment
 - Test Team focused efforts on approximately 40 publically accessible network segments hosting both ITD and State Agency systems
- Internal Assessment
 - Test Team scanned 30 internal network segments hosting both ITD and State Agency systems



- All vulnerability findings were rated as high, medium or low risk
 - **High Risk:** A malicious user that exploits this level of vulnerability could achieve full control of the system and all data contained on the system
 - **Medium Risk:** A malicious user that exploits this level of vulnerability could achieve limited user level control of the system and/or compromise data contained on the system
 - **Low Risk:** A malicious user that exploits this level of vulnerability could achieve limited access to data contained on the system



- 38 total Vulnerability findings
- All findings could be classified into two major areas:
Systems missing critical software patches, and
Systems with configuration vulnerabilities
- Missing Software Patches (OS or Application)
 - 23 High risk, 6 Medium Risk
- Configuration Vulnerabilities
 - 4 High risk, 4 Medium risk, 1 Low risk



Application Vulnerability Assessment Overview

- Two-tiered approach to application security testing
 - Automated scanning
 - Manual assessment
- Focus on common application vulnerability issues
 - Un-validated input
 - Non-functioning access controls
 - Authentication and session management issues
 - Cross-site scripting flaws
 - Buffer overflows
 - Injection flaws
 - Improper error handling
 - Insecure data storage
 - Denial of service (DoS)

Application Vulnerability Assessment Scope

- ManTech assessed two applications
 - State NDGOV Portal
 - CJIS Application
- Allow ITD to benchmark the state's Application Assessment process against Test Team findings



Application Vulnerability Assessment Results

- 3 total vulnerability findings
- NDGOV Portal
 - 2 Medium risk
- CJIS
 - 1 Medium risk

Security Assessment of Non-consolidated IT Services Overview and Scope

- Test Team evaluated the physical and logical security of electronic mail, database administration, and application server services that were not consolidated within ITD
- Limited vulnerability scanning and application scanning were conducted if requested by the agency
- Items evaluated included:
 - Physical Security
 - Network Configuration and Architecture
 - Network Access Controls
 - Auditing
 - Malware Protection/Antivirus
 - Recovery and Back-Up Procedures
 - Vulnerability Scanning
 - Security Patch Updates



Security Assessment of Non-consolidated IT Services Scope

- Agencies assessed during this phase include
 - Office of the Attorney General
 - Department of Mineral Resources Oil and Gas Division
 - Public Service Commission
 - Water Commission
 - Housing and Finance Agency
 - Department of Emergency Services.



Security Assessment of Non-consolidated IT Services Results

- Results of the physical and network security assessments varied greatly by agency depending on the mission of the agency assessed
- Agencies lacked formal processes and in some cases tools to conduct periodic network vulnerability assessments of their infrastructure.

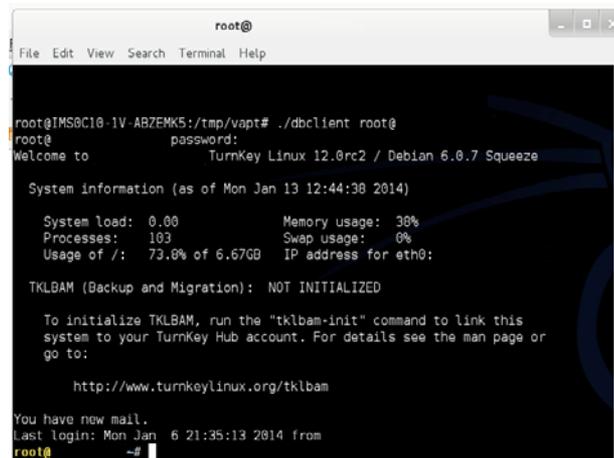
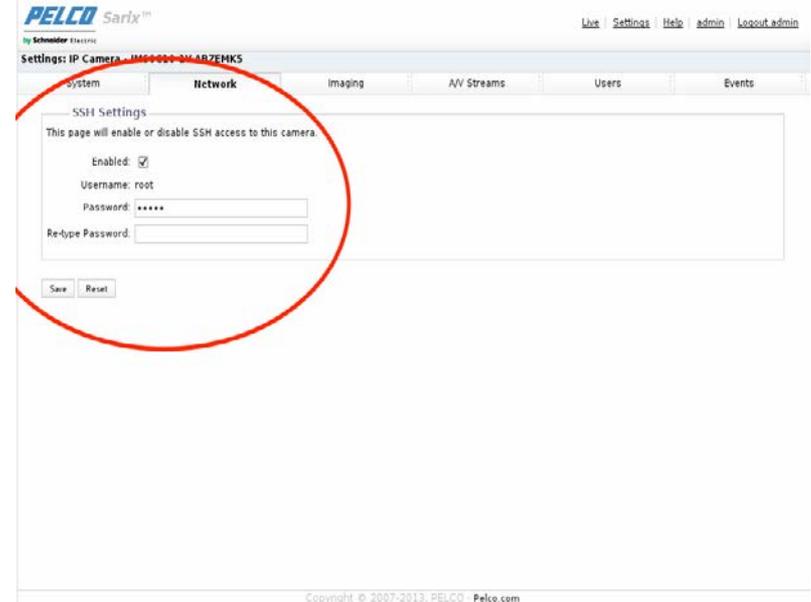
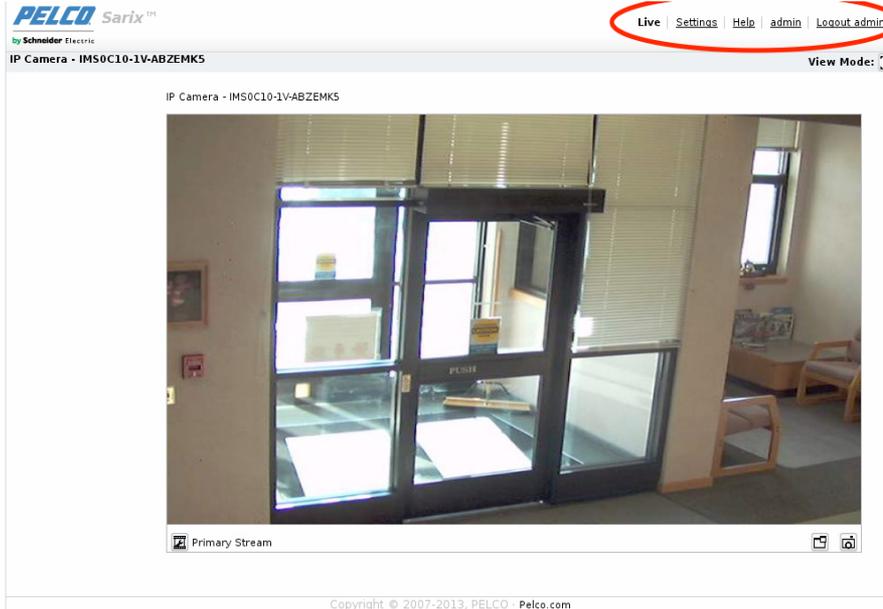


- Purpose is to emulate realistic & current threats in an attempt to gain access to systems and/or information via both technical and non-technical means
- Testing attempts to exploit discovered vulnerabilities and test an organization's response procedures
- Two Primary Test methods
 - Direct System Exploitation
 - Social Engineering (not executed during this assessment)

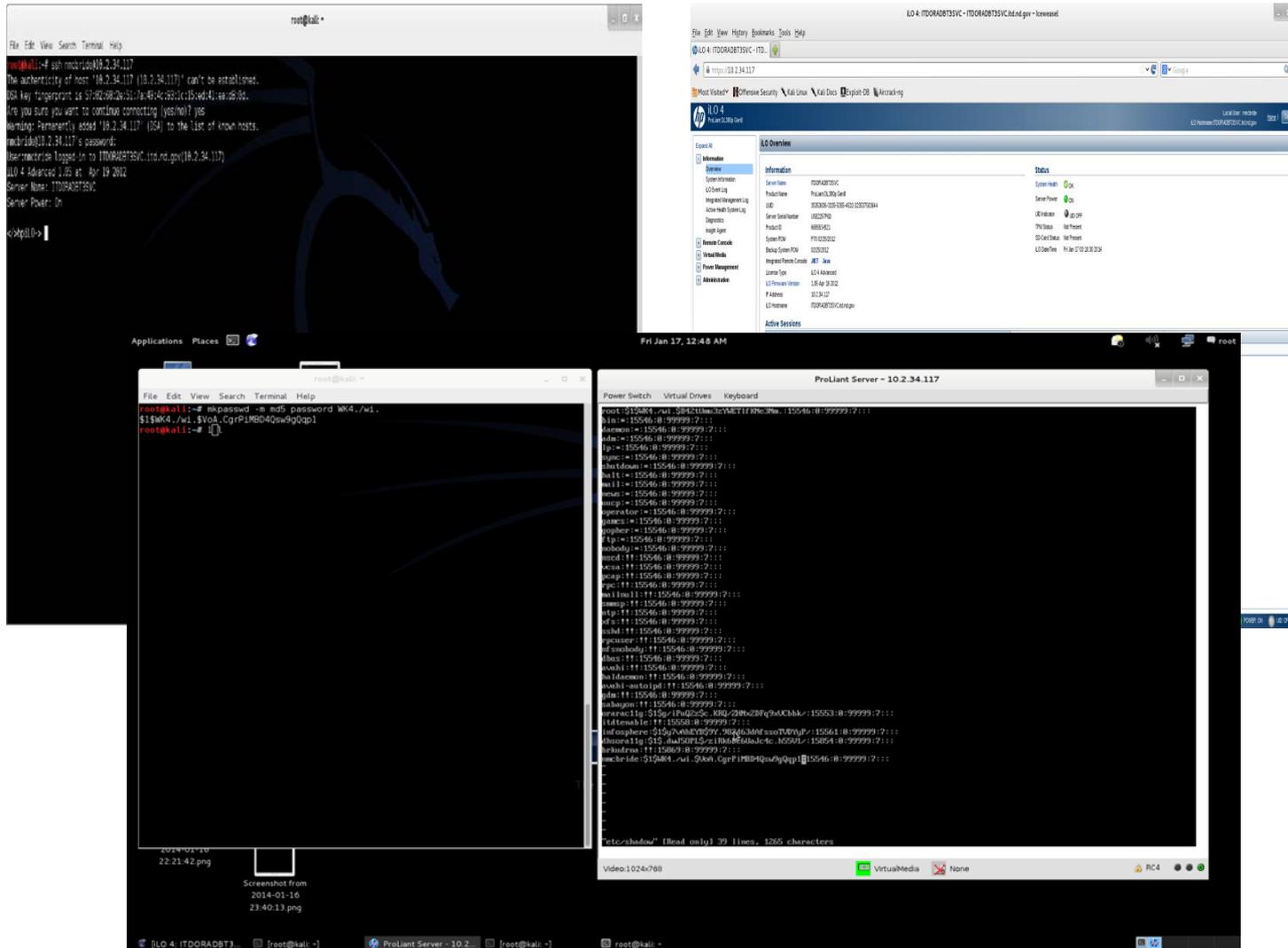


- Direct Exploitation
 - Test Team explored 10 potential scenarios based on assessment results
 - All scenarios assumed access to the internal state network
 - Of the scenarios, 4 led to direct system access

Penetration Testing Example- IP Camera



Penetration Testing Example- DRAC Authentication Bypass



- Continue Maturation of Patch Management Program
 - Baselines need to be established for all operating system and application software used on the network and regular patching processes set up to ensure all systems receive critical patches in a timely fashion
 - Focus on 3rd party applications; consider application whitelisting
 - Adherence to patch management timelines with compliance monitoring
 - Continuous Monitoring approach for real-time visibility
- Internal Network Segmentation
 - Critical servers and development systems should be segregated from the internal network to minimize exposure of critical data
- Require use of Encrypted protocols for Remote Management
 - Only encrypted protocols should be used to remotely manage systems

- Restrict Access to Protocols for Remote Management from the Internet
 - IP-based access controls should be implemented to restrict access to trusted systems.
- Develop Formal Vulnerability Scanning Program- Non-consolidated IT Services
 - Institute periodic review and assessment process for non-consolidated IT services to proactively measure compliance with vulnerability patching requirements.



- Results of this assessment are typical for organizations of a similar size and maturity
- Number one recommendation that can be implemented to improve security of the network is to continue to mature patch management program and ensure non-consolidated IT services are included.

