CoAction

Penetration Testing

Continuously Improve your Organization's Cybersecurity Resilience

The assessment objective is to inspect assets to provide an inventory of assets and vulnerabilities to support the data required to help meet the IDENTIFY, PROTECT, DETECT phases of the NIST Cybersecurity Framework (CSF).

IDENTIFICATION OF ASSET WEAKNESSES & INSPECTIONS OF TECHNICAL FLAWS

- Adversary emulation
- Vulnerability scanning
- Manual & Automated Asset and application security posture evaluations adhering to both PTES & OWASP standards
- Risk of compromise ratings
- Remediation recipes
- Report documentation

CoActionTech.com

sales@coactiontech.com

CoAction

Penetration Testing

Sample Penetration Testing Objectives

Standard Testing

1. Production systems within designated segments:
   a. Windows based OS
   b. Linux based OS
   c. Networking infrastructure (switches, routers, firewalls, wireless devices)
   d. Databases
2. RFC1918 addresses associated within designated zone(s)
3. Publicly / Internet Accessible
4. Retest of all critical/high findings

Optional Testing

1. Development systems
2. Wireless networks and systems
3. Publicly addressable / internet accessible assets not explicitly stated
4. Third party software as a service (SaaS) assets and applications
5. Physical assessments
6. Assessment of Security Operation Center (SOC) readiness and detection capability
7. Review of Information security Policies and frameworks.
8. Architecture reviews
9. Social Engineering Scenarios

Cloud Testing (AWS/GCP/Azure/Private)

1.Accounts, IAM/PAM users, Groups, Roles, And access levels.
a.Accounting, Authentication and Authorization (AAA)
2. Data at Rest & in Transit
a. Access & Authorization (Permissions) b. Versioning
c. Replication / Backup
d. Encryption
3. OS & Application Security
a. API Keys (Distribution, Access, & Revocation)
b. Network Restrictions (ACL, White-Listings, Bastion) c. Least Privilege Checks
4. Network Security & Segmentation a. VPCs & Security Groups
b. Network Access Control Lists (Network & Hosts)
c. Threat Protection Layers
5. Audit Trail (Logging), Monitoring, Alerting & Response

CoAction

Penetration Testing

Technical Details

FINDING SEVERITY RATINGS

SEVERITY	RANGE	Definition
Critical	9.0 - 10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0 - 8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0 - 6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1 - 3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	INFO	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

- **POSITIVE FINDINGS**
- **RISKY FINDINGS**
- **OPPORTUNITIES FOR IMPROVEMENT**
- **RECOMENDED CLEAN UP ACTION ITEMS**

TECHNICAL SUMMARY OF TEST PERFORMED

Information Gathering / Reconnaissance

Testing for Server Version Disclosures
Review file shares, Public Repositories, Dark/Grey websites and forums for Information Leakage
Active Directory
Testing for weak GPO policies

Outdated Software

Testing for Out of Date Operating Systems
Testing for Out of Date Firmware
Testing for Out of Date Software

Authentication

Testing for Lockout Policy
Testing for Default Credentials
Testing for Anonymous Login
Testing for MFA
Testing for Weak Authentication
Testing for Null Session

Network Design

Testing for Network Layout
Testing for Segmentation
Testing for IoT Devices
Testing for Firewall Rules

Authorization

Testing for Over Permissive File Access
Testing for Bypassing Authorization Schema
Testing for Insecure Direct Object References

Configuration Management

Review Local Firewall Rules
Review Local Configurations

Active Directory

Testing for ASREP Roasting Vulnerabilities
Testing for Kerberoasting Vulnerabilities
Testing for Weak Password Policy
Testing for GPP Passwords
Testing for GPP Autologon
Testing for AdminCount Attributes
Testing for PasswordNot Required Attributes
Testing for Delegation Issues

Cryptography

Testing for Weak Transport Layer Security
Testing for Weak Encryption
Testing for Sensitive Information Sent Via Unencrypted Channels
Testing for Unsigned SMB