NetSPI™

# Mainframe Penetration Testing

NetSPI's mainframe solution reduces risk and improves overall security. Due to their complicated nature and organic growth over decades vulnerabilities may exist in your mainframe environment. NetSPI's penetration testing can offer valuable insight into your LPAR security, providing actionable guidance on how to improve your mainframe security, and help meet compliance requirements.

## Improve Your Mainframe Security

NetSPI's mainframe testing reduces risk and improves overall security.

Your mainframe may be susceptible to attacks from internal threats or APTs. NetSPI's penetration testing simulates adversarial attacks to emulate threats that exist today against your mainframe environment producing real world results on actual vulnerabilities.

During our assessments NetSPI evaluates your mainframe for security vulnerabilities in RACF, ACF2 or TopSecret. We look at dataset and USS file permission security, network security, JES2 & TSO configuration, DB2 & CICS regions. Testing can be conducted on a per LPAR basis or against entire sysplexes providing actionable recommendations for remediation and improving your organization's mainframe security.

Our testers have deep experience evaluating and testing mainframe security controls with over 20 years of industry expertise.

## Our Mainframe Testing Solution

NetSPI tests your in scope mainframes and systems. We follow manual and automated pentesting processes that use commercial, open source, and proprietary software to evaluate your infrastructure from the perspective of an anonymous (non-credentialed) user. However, testing can also be conducted starting from an authenticated perspective. Our standard testing approach is based on NIST 800-53 special publication, PCI DSS, IBM recommendations, the MITRE ATT&CK framework, and other industry best practices. We offer three types of testing depending on scope and client needs.

### Blackbox (Unauthenticated) Testing*

- Network service discovery
- Vulnerability discovery and verification
- VTAM/SNA discovery
- Logical unit enumeration
- Application ID discovery
- TN3270 application testing
- Web application testing
- Password auditing
- Network job entry

** If access can be gained to TSO or USS this testing may continue to presumed breach depending on scope.*

### Presumed Breach Authenticated Testing

- Automated vulnerability discovery
- RACF/TopSecret/ACF2 testing
- Vulnerability verification and exploitation
- Offline password auditing
- APF authorization privilege escalation
- TSO, JES2, and UNIX System Services testing
- SVC privilege escalation

### CICS Application Testing

- Tests common application vulnerabilities
- CICS transaction review/testing
- AID testing
- BMS testing
- CICS web application testing
- CICS API testing

### CICS Region Testing

- Check for common CICS region misconfiguration
- Enumerate/Brute force transaction IDs
- Test access to critical transactions
- Password auditing

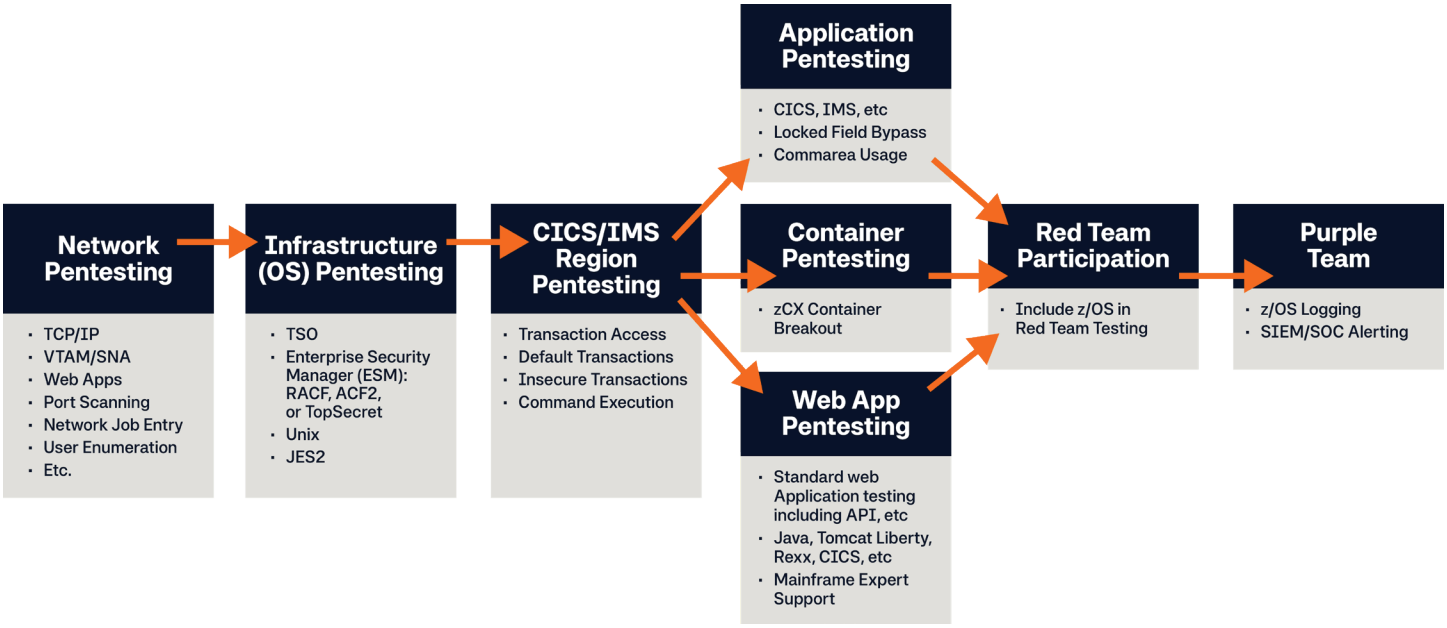
NetSPI™

## Top 10 z/OS Vulnerabilities

1. Weak dataset permissions
2. System OPERATIONS/SPECIAL
3. ESM misconfiguration
4. ESM database access
5. Excessive access to APF authorized libraries
6. Excessive ESM permission in UNIX
7. Misconfigured CICS regions
8. Legacy trusted NJE nodes
9. Unmonitored SURROGAT access
10. Inadequate password controls

---

# z/OS Mainframe Testing Maturity




**To learn more about NetSPI's Mainframe Penetration Testing solutions, visit www.netspi.com or contact us.**

## You Deserve The NetSPI Advantage

**300+ In-House Security Experts**

**Intelligent Processes**

**Advanced Technology**

## Your Proactive Security Partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), External Attack Surface Management (EASM), Cyber Asset Attack Surface Management (CAASM), and Breach and Attack Simulation (BAS) as a Service.