

Tyrell Corporation

2026 Security Assessment & Testing Out Brief

CIS450 32264 – Winter 2026
Client Heather Johnson

A# Solutions LLC
Website Portfolio

CYBERSECURITY

ATTACKS
DATA
HARDWARE
Protect
Computer
SPYWARE
CYBERATTACKS
DATA
SYSTEM
Computer
Internet
SAFE
Systems
DANGER
PROTECT
SOFTWARE
OPERATING
Networks
SECURE
Bootkits
PHISHING
SPYWARE
Trojans
PROTECT
Payloads
Web shells
BACKDOORS
DIGITAL
PROTECTION
Information Technology
RANSOMWARE
VIRUS
Vulnerability

A# Solutions LLC
Website Portfolio

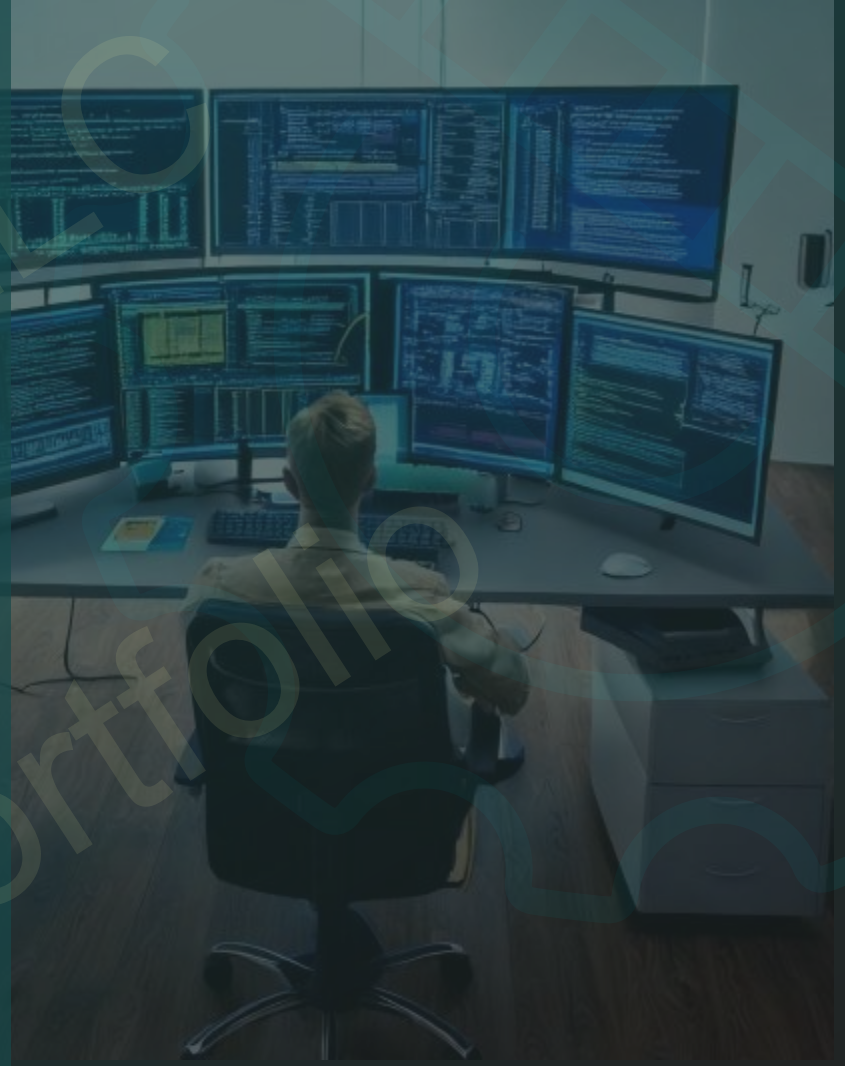
Consultant Team Leader:
David Holmes

Objectives of the Assessment

January 14th - March 4th

- Recon
- Vulnerability Analysis
- Exploitation

- Evaluate security posture of internal network devices and employee portal
- Simulate realistic attacker scenarios
- Identify vulnerabilities enabling privilege escalation or lateral movement
- Provide actionable remediation recommendations



Our objective was not only to identify vulnerabilities, but also to provide actionable remedies to all security risks.
Then provide the required material to assist your staff in securing these risks.

A# Solutions LLC Website Portfolio

Finding #1 – Legacy Operating Systems

Key Issues

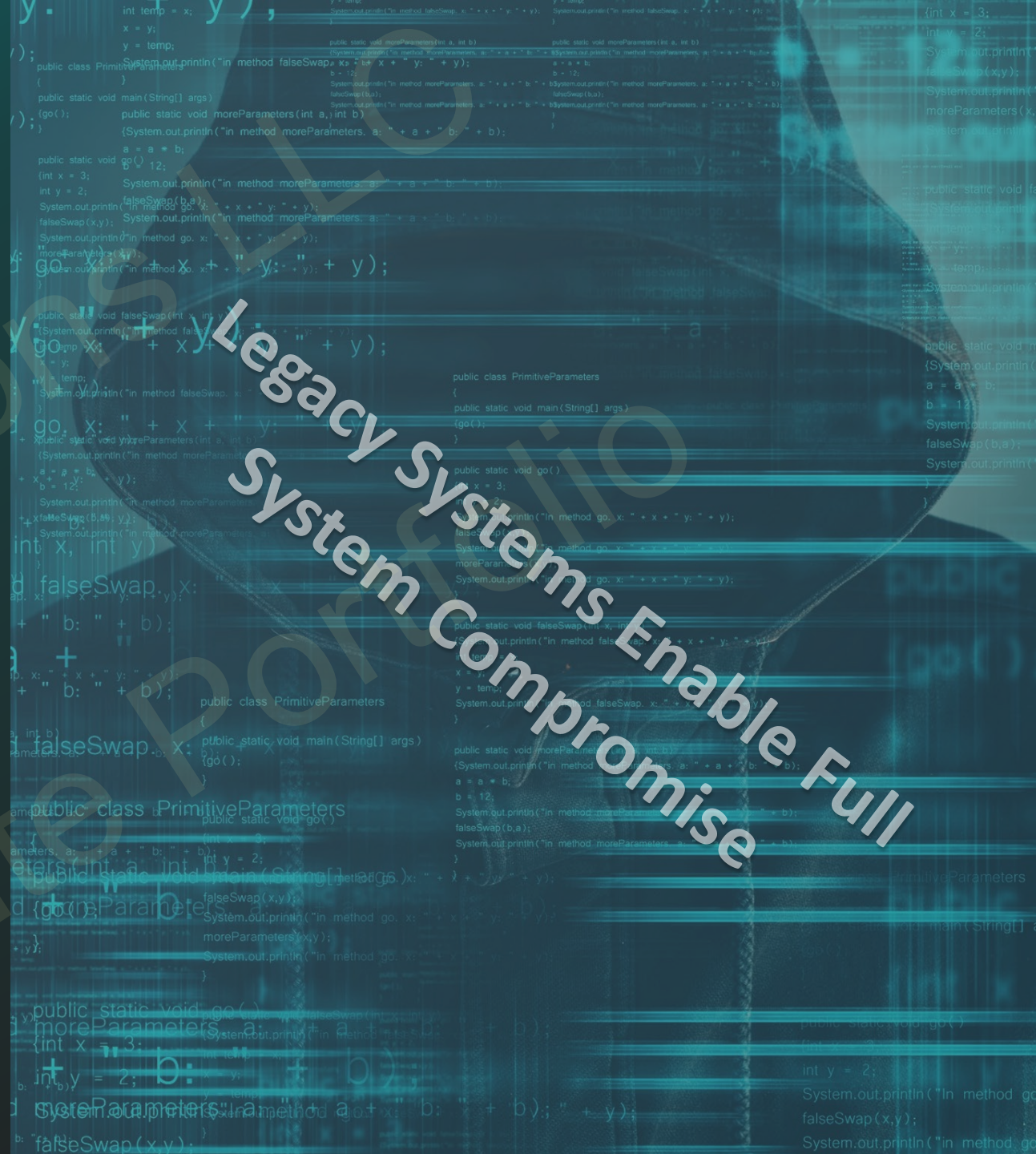
- Windows 7 systems still active
- SMBv1 remote code execution vulnerability
- Critical CVSS score (9.8)

Potential Impact

- Full system compromise
- Malware or ransomware deployment
- Lateral movement across the network

"Legacy systems act as an exponential risk multiplier. Because they often lack vendor support and modern security controls, they provide stable, well-documented entry points that attackers can exploit with minimal effort."





A# Solutions LLC Website Portfolio

Finding #2 – Identity and Credential Risks

Key Issues

- Weak credential protections
- NTLM authentication exposure
- Privilege escalation paths in Active Directory

Potential Impact

- Credential theft
- Password spraying attacks
- Potential domain administrator compromise



"The more best practices implemented, the fewer opportunities attackers have to breach a system."



A# Solutions LLC
Website Portfolio

Finding #3 – Employee Portal Vulnerabilities

Critical vulnerabilities discovered:

- OS command injection
- SQL injection
- Cross-site scripting
- Weak login protections

Potential Impact

- Database compromise
- Sensitive data exposure
- Server takeover

"Never rely on just one type of authorization measure to secure website applications."





A# Solutions LLC
Website Audits



High Priority Recommendations

Top Remediation Priorities

1. Remove legacy systems and disable SMBv1
2. Strengthen identity and access controls
3. Secure the employee web portal

Key Actions

- Upgrade unsupported operating systems
- Implement MFA for privileged accounts
- Apply secure coding practices and input validation

A# Solutions LLC Website Portfolio

Key Takeaways About Security Posture



Strengths

- Core infrastructure present
- Standard enterprise architecture

Areas for Improvement

- Legacy systems remain in production
- Identity security controls need improvement
- Web application security gaps

Overall Assessment

We found a high risk environment with several exploitable vulnerabilities that could enable enterprise-wide compromise if left unaddressed.

A# Solutions LLC Website Portfolio





How bad is our environment compared to other organizations you've tested?.

Are these attacks easy to perform, or are they pretty advanced? In other words, how worried should we be about the skill of our attackers?

If we fix all these things, can you come back and retest? How difficult would it be for us to test some of these on our own?

A# Solutions LLC Website Portfolio

Post-engagement support is included to ensure successful remediation. Our team is available for scheduled video consultations and phone support to assist your technical staff with patch implementation.

We appreciate your patience and interests throughout this engagement. We welcome any additional questions as you begin your remediation efforts.

Our mission is to ensure the Tyrell Corporation's security posture remains resilient while systematically reducing the attack surface and overall risk profile.

A# Solutions LLC Website Portfolio

"Thank You for your time"

Feel free to contact A# Solutions for any future needs or concerns

Contact Us:

David Holmes

david.a.holmes@asharpsolutions.com