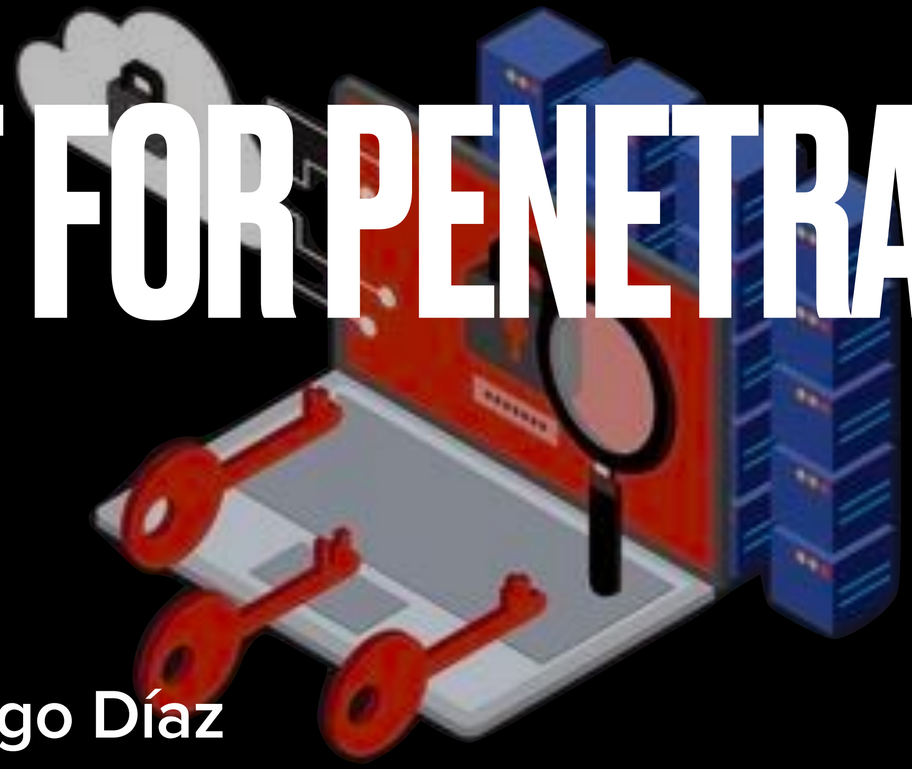
VAPT REPORT FOR PENETRATION TESTING



Prepared by Esperanza Buitrago Díaz

FEBRUARY 2026

EXECUTIVE SUMMARY

- Secure postures across multiple layers of the environment.
- Identify vulnerabilities.
- Demonstrate exploitability.
- Provide actionable recommendations

PROFESSIONAL SUMMARY

Esperanza Buitrago Díaz

Major:
- BSc. in Mathematics
- MSc. In pure and applied logic

Experience:
- Data Science
- Data Engineering
- Software Engineering

Linkedin:
https://www.linkedin.com/in/ebuitragod

Github:
https://www.github.com/ebuitragod

MULTI-PHASE ENGAGEMENT

- Phase 1: Internal Network penetration test
  - Simulated attack:
    - 6 vulnerabilities found
- Phase 2: Web application security assessment
  - Authentication penetration test of DVWA
    - 4 vulnerabilities found
- Phase 3: Credential security and password cracking assessment
  - Simulated initial access via EternalBlue with 2 compromised user accounts
- Phase 4: Digital forensic investigation
  - Forensic analysis of a compromised disk imaged

VULNERABILITY SUMMARY BY SEVERITY

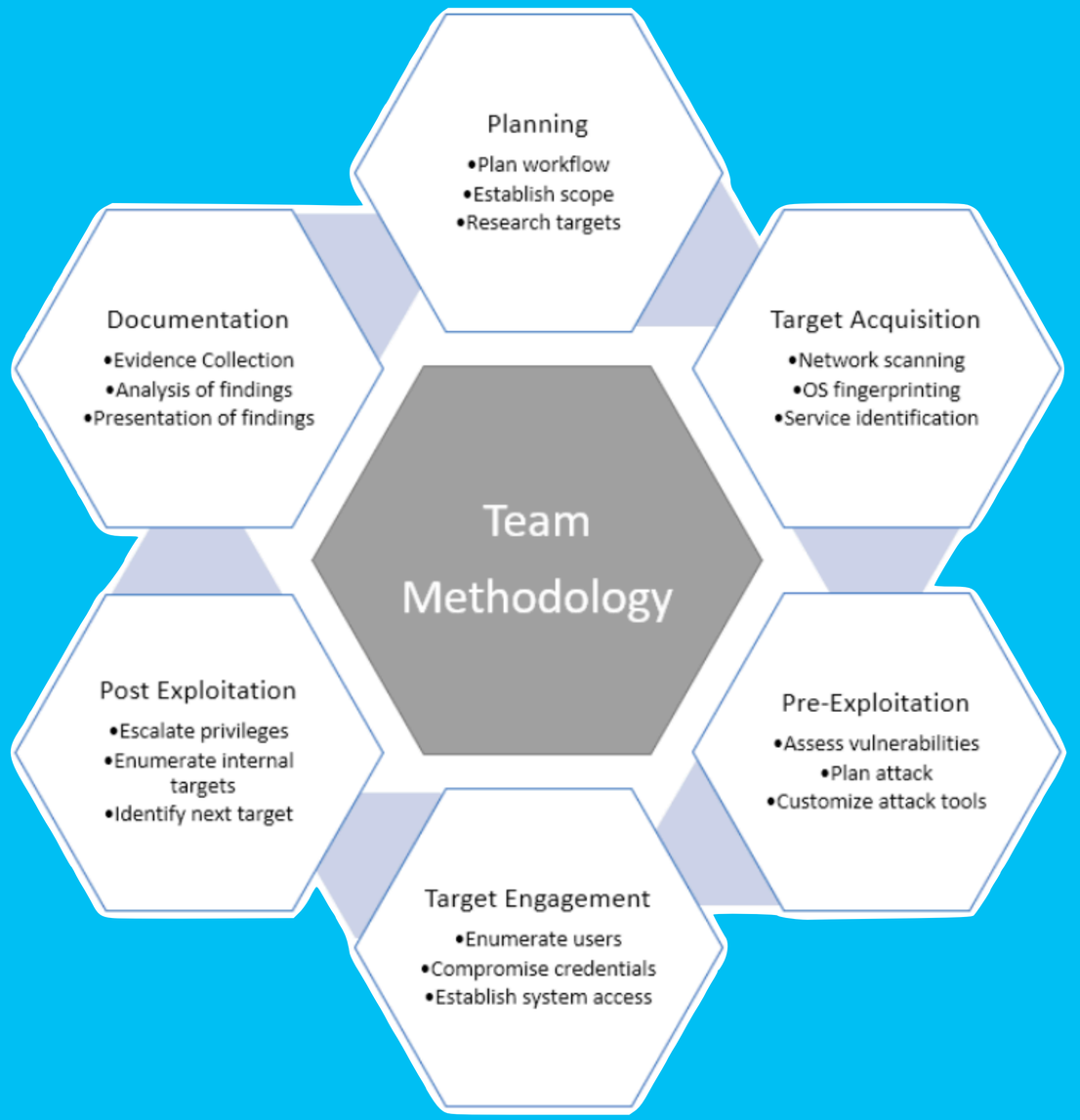
PHASE	CRITICAL	HIGH	MEDIUM	LOW
1 - Internal Network assessment	1	2	3	-
2 - Web Application assessment	1	3	-	-
3 - Credential security assessment	-	1	3	
4 - Forensic investigation	-	1	1	2

TESTING METHODOLOGY

- Penetration testing execution standards (PTES)
- NIST SP 800-115

ETHICAL AND OPERATIONAL CONSIDERATIONS

- All testing was conducted in a controlled, and isolated lab environment.
- Evidence was preserved.
- CoC was maintained,
- Findings were fully documented in real-time.
- All exploited system were restored.



ASSESSMENT FINDINGS

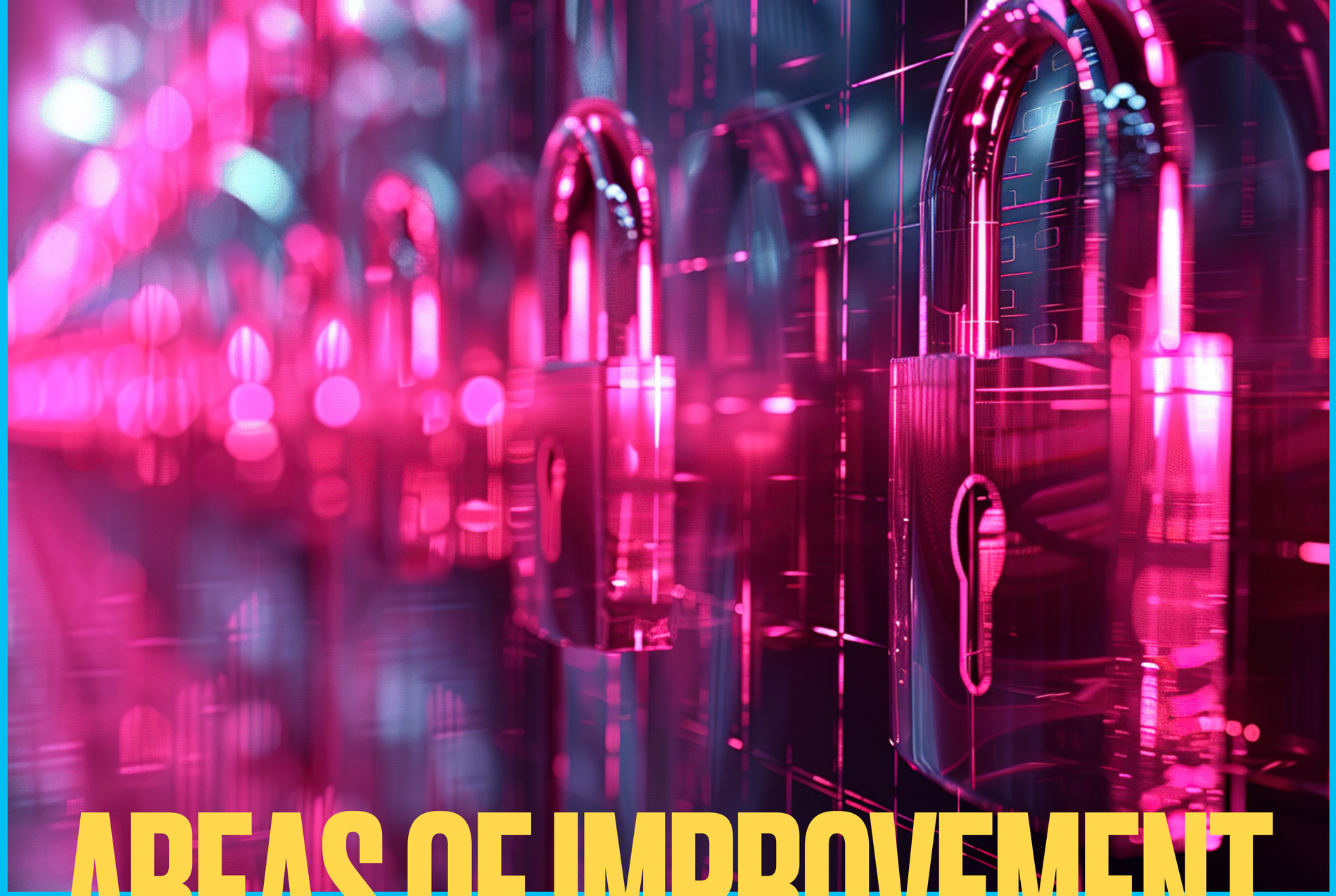
Finding	Risk score	Exploitation likelihood	Business impact	Remediation difficulty
1- MS17-010 EternalBlue SMB remote code execution	10	Likely	Major	Easy
2- SQL injection in Web Application	10	Likely	Major	Easy
3- Unpatched Windows 7 Operating System (EOL)	9	Likely	Major	Moderate
4- Systematic data concealment *via* obfuscation and compression	8	Likely	Major	Moderate
5- Stored Cross-Site Scripting (XSS)	9	Likely	Moderate	Easy
6- Unrestricted file upload to Web Server	8	Likely	Moderate	Easy

ASSESSMENT FINDINGS

Finding	Risk score	Exploitation likelihood	Business impact	Remediation difficulty
7- Weak pasword policy and SMB brute-force vulnerability	7	Likely	Major	Moderate
8- Hidden JPG files recovered from deleted and compressed space	7	Possible	Major	Hard
9- SAM database hash extraction	7	Possible	Major	Hard
10- Unauthenticated SMB service exposure	7	Possible	Moderate	Easy
11- Remote Code Execution *via* Meterpreter (Post-exploitation)	7	Possible	Moderate	Moderate
12- File signature mismatch and extension obfuscation	5	Possible	Moderate	Easy

ASSESSMENT FINDINGS

Finding	Risk score	Exploitation likelihood	Business impact	Remediation difficulty
13- Microsoft RPC service exposure	6	Possible	Minor	Easy
14- Legacy RTSP service exposure	5	Possible	Moderate	Easy
15- HTTPAPI services with default configurations	4	Possible	Minor	Easy
16- Insecure default and common passwords	6	Likely	Moderate	Easy
17- Image integrity verification	0	N/A	N/A	Easy
18- Proper Chain of Custody established	0	N/A	N/A	Easy



AREAS OF IMPROVEMENT

- Short term recommendation
  - Critical vulnerability remediation
  - Security control implementation
- Long term recommendation
  - Strategic security initiatives
  - Organizational security maturity
  - Technology investment

SHORT-TERM RECOMENDATIONS

CRITICAL VULNERABILITY REMEDIATION

- Patch critical vulnerabilities
  - Apply EternalBlue patches
  - Update EOL Win
  - Implement emergency patch management procedures
- Credential security enhancement
- Web application security
- Network service hardening

SHORT-TERM RECOMENDATIONS

CRITICAL VULNERABILITY REMEDIATION

- Patch critical vulnerabilities
- Credential security enhancement
  - Reset all compromised passwords
  - Enforce password policy
  - Enable LSA protection on all Windows systems
- Web application security
- Network service hardening

SHORT-TERM RECOMENDATIONS

CRITICAL VULNERABILITY REMEDIATION

- Patch critical vulnerabilities
- Credential security enhancement
- Web application security
  - Fix SQL injection and XSS vulnerabilities in DVWA
  - Implement input validation and output encoding
  - Deploy WAF
- Network service hardening

SHORT-TERM RECOMENDATIONS

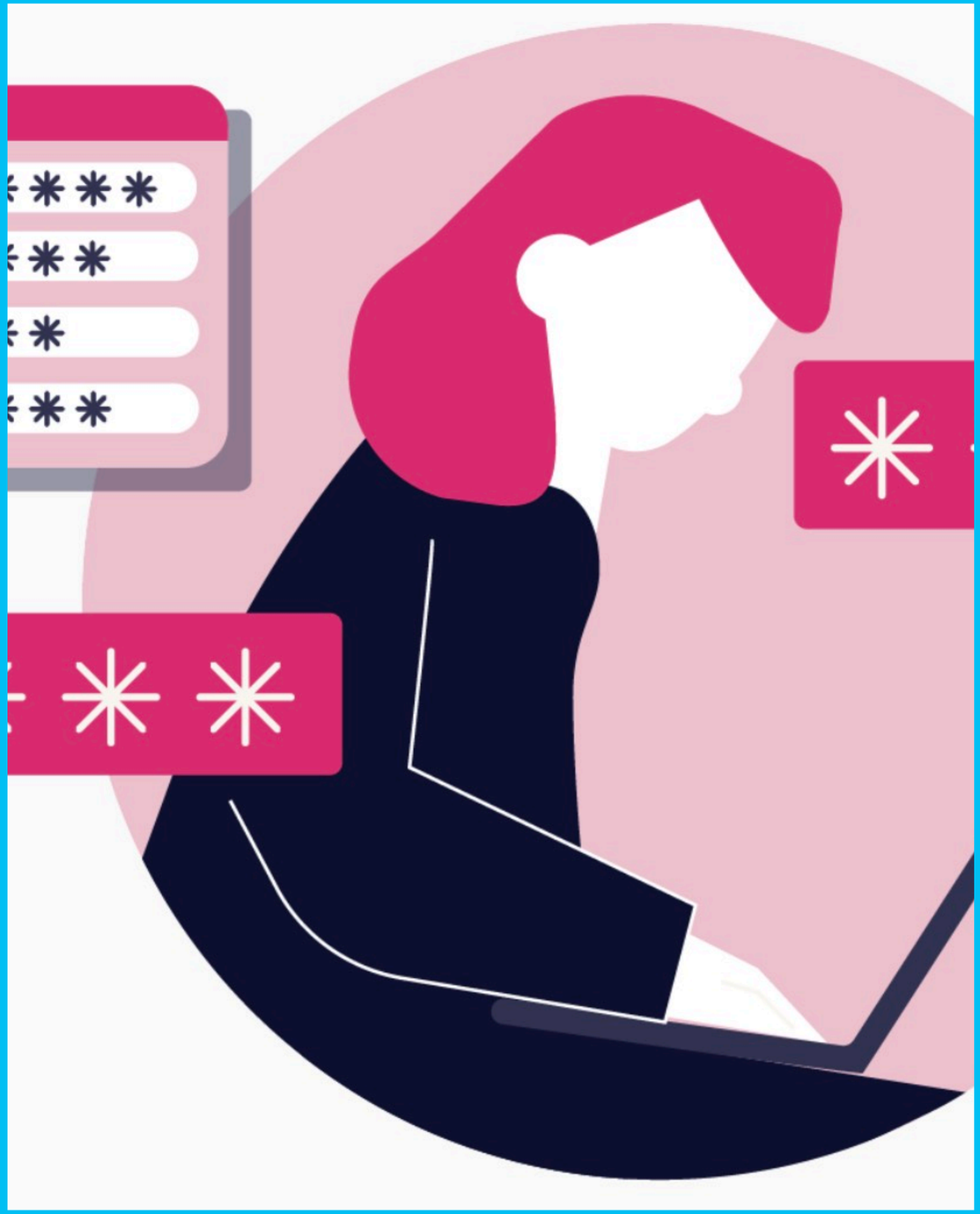
CRITICAL VULNERABILITY REMEDIATION

- Patch critical vulnerabilities
- Credential security enhancement
- Web application security
- Network service hardening
  - Disable SMBv1 protocol access
  - Restrict RPC, RTSP, and HTTPAPI services.
  - Implement network segmentation
  - Configure firewall rules

SHORT-TERM RECOMENDATIONS

SECURITY CONTROL IMPLEMENTATION

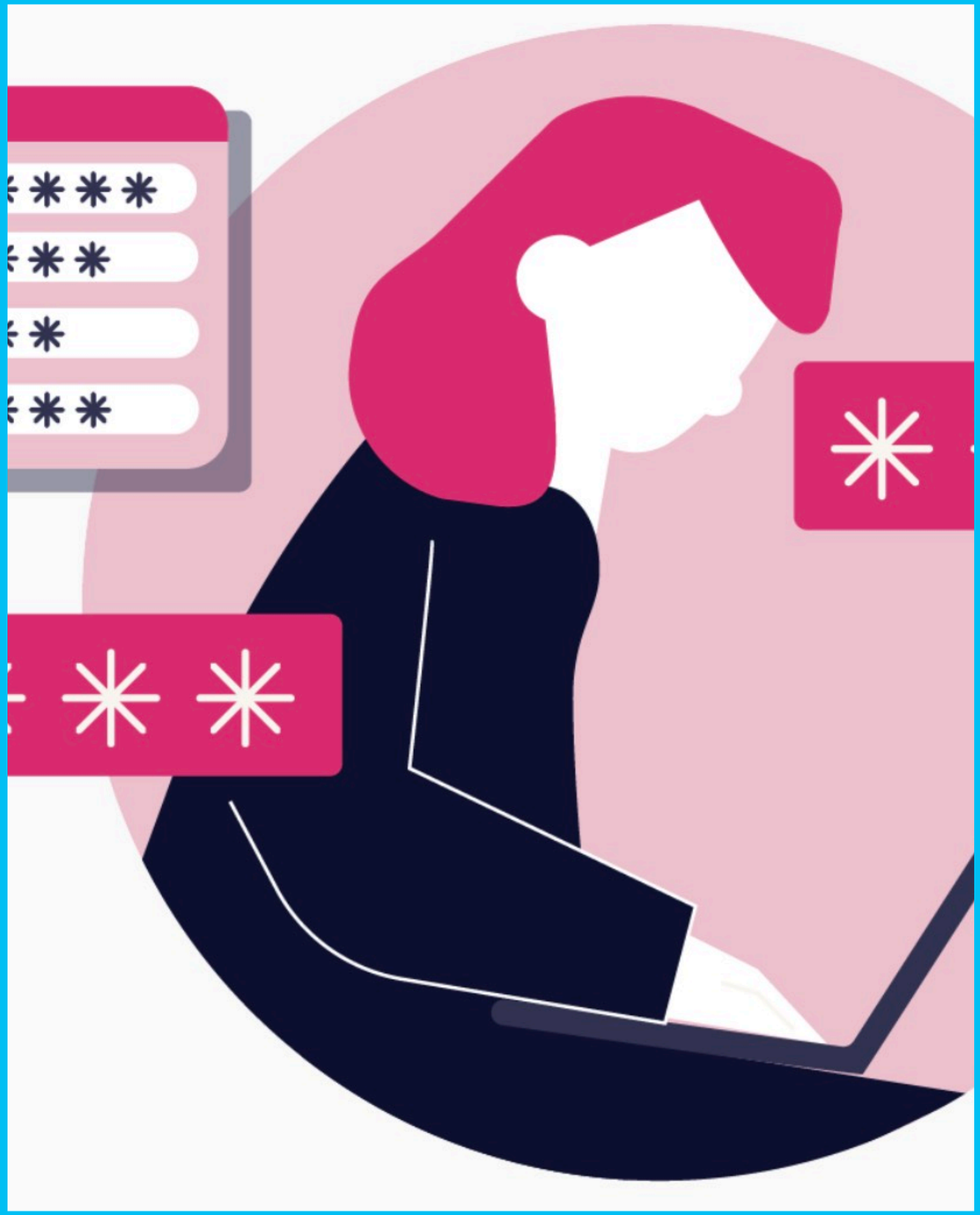
- Endpoint protection
  - Deploy EDR
  - Implement application whitelist
  - Enable Windows Defender Credential guard
- Monitoring and detection



SHORT-TERM RECOMENDATIONS

SECURITY CONTROL IMPLEMENTATION

- Endpoint protection
- Monitoring and detection
  - Implement real-time alerting for brute-force attempts
  - Monitor for hash extraction and pass-the-hash attacks



LONG-TERM RECOMMENDATIONS

STRATEGIC SECURITY INITIATIVES

- Architecture modernization
- Identity and access management
- Advanced threat protection
- Secure development lifecycle
- Forensic and incident response capability
- Compliance and governance

LONG-TERM RECOMMENDATIONS

ORGANIZATIONAL SECURITY MATURITY

- Security awareness and training
  - Conduct regular phishing simulations exercises
  - Provide role-based security training
- Vendor and third-party risk management

LONG-TERM RECOMMENDATIONS

TECHNOLOGY INVESTMENTS

- Security tool consolidation
- Continuous security validation

PRIORITY MATRIX

Priority	Timeframe	Focus area	Key actions
Critical	0 - 1 days	Vulnerability remediation	• Patch EternalBlue • Reset credentials • Disable SMBv1
High	7 - 30 days	Security controls	• Implement MFA • Deploy EDR • Configure monitoring
Medium	1 - 3 months	Architecture	• Migrate EOL systems • Implement segmentation
Long-term	3 - 6 months	Maturity	• Establish program • Implement frameworks • Continuous testing

THANK YOU

Prepared by
Esperanza Buitrago Díaz

Cybersecurity bootcamp
February 2026

Linkedin:
https://www.linkedin.com/in/ebuitragod

Github:
https://www.github.com/ebuitragod