**Raport de Testare a Penetrării**

**Client: Spital**

**Data: 12 Februarie 2025**

**1. Descrierea domeniului și metodei de testare a penetrării**

**1.1 Servicii de Testare**

* Testare tehnică de penetrare la nivel de rețea pentru gazde din rețelele interne
* Testare tehnică de penetrare la nivel de rețea pentru gazde cu acces la internet
* Inginerie socială prin phishing telefonic
* Inginerie socială prin phishing email

**1.2 Metodologie**

Pentru fiecare serviciu au fost utilizate următoarele metode:

* Recunoaștere și scanare inițială
* Identificare vulnerabilități
* Exploatare vulnerabilități
* Post-exploatare și colectare dovezi
* Documentare rezultate

**2. Descrierea succintă a domeniului testării**

**2.1 Zone Testate**

1. Rețea Internă:
   * Sisteme Windows conectate la rețeaua internă
   * Servere critice (inclusiv McAfee Security Server)
   * Sisteme de stocare date pacienți
   * Infrastructură de rețea
2. Sisteme cu Acces la Internet:
   * Servere web expuse
   * Gateway-uri și sisteme perimetrale
   * VPN și servicii de acces la distanță
3. Factor Uman:
   * Personal medical
   * Personal administrativ
   * Personal IT

**2.2 Rezultate Principale**

În urma testării rețelei interne, au fost identificate:

* Vulnerabilități critice în protocoalele SMB
* Acces neautorizat la sisteme critice
* Expunerea datelor confidențiale ale pacienților
* Susceptibilitate la atacuri de inginerie socială

**3. Măsuri întreprinse**

**3.1 Acțiuni Realizate pe Zone**

**3.1.1 Rețea Internă**

* Scanare completă porturi și servicii
* Identificare și exploatare vulnerabilități SMB
* Compromitere sisteme critice
* Extragere date sensibile

**3.1.2 Sisteme cu Acces la Internet**

* Scanare externă de vulnerabilități
* Testare configurații VPN și acces la distanță
* Verificare expunere servicii critice

**3.1.3 Testare Factor Uman**

* Campanie phishing prin email
* Apeluri telefonice de inginerie socială
* Evaluare awareness securitate

**3.2 Detalii Tehnice Vulnerabilități**

Vulnerabilitatea principală identificată: SMB ETERNALBLUE

* CVE-uri asociate: CVE-2017-0143, -0144, -0145, -0146, -0148
* Vector de atac: Port 445 TCP
* Impact: Acces complet la sistem fără autentificare
* Sisteme afectate: Multiple sisteme Windows din rețeaua internă

**4. Concluzie**

**4.1 Impact asupra Securității**

1. Vulnerabilități Tehnice Critice:
   * Sisteme vulnerabile la exploituri cunoscute (EternalBlue)
   * Configurații nesecurizate ale serviciilor critice
   * Lipsă segmentare efectivă a rețelei
2. Riscuri pentru Datele Pacienților:
   * Acces neautorizat la informații medicale confidențiale
   * Potențială încălcare a HIPAA și GDPR
   * Expunere date personale sensibile
3. Probleme de Securitate Operațională:
   * Susceptibilitate ridicată la atacuri de inginerie socială
   * Lipsă monitorizare efectivă
   * Proceduri inadecvate de management al accesului

**4.2 Consecințe Posibile**

1. Impact Imediat:
   * Scurgeri de date medicale confidențiale
   * Întreruperea serviciilor medicale critice
   * Compromiterea sistemelor de securitate
2. Impact pe Termen Lung:
   * Penalități pentru neconformitate cu reglementările
   * Pierderea încrederii pacienților
   * Costuri semnificative de remediere

**4.3 Recomandări de Remediere**

**4.3.1 Pași Detaliați de Remediere PowerShell**

1. Remediere Vulnerabilități SMB

*# Dezactivare SMBv1*

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 -Force

*# Activare SMB Signing*

Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\LanmanServer\Parameters" RequireSecuritySignature -Type DWORD -Value 1

*# Blocare port 445 pentru acces extern*

New-NetFirewallRule -DisplayName "Block SMB External" -Direction Inbound -LocalPort 445 -Protocol TCP -Action Block -RemoteAddress Internet

1. Configurare Windows Defender

*# Activare protecție în timp real*

Set-MpPreference -DisableRealtimeMonitoring $false

*# Activare protecție rețea*

Set-MpPreference -EnableNetworkProtection Enabled

*# Configurare scanare*

Set-MpPreference -ScanScheduleDay Everyday

Set-MpPreference -RemediationScheduleDay Everyday

1. Hardening Active Directory

*# Politici parolă*

Set-ADDefaultDomainPasswordPolicy -ComplexityEnabled $true -MinPasswordLength 14 -MinPasswordAge "2.00:00:00" -MaxPasswordAge "60.00:00:00"

*# Blocare cont după încercări eșuate*

Set-ADDefaultDomainPasswordPolicy -LockoutDuration "01:00:00" -LockoutThreshold 5 -LockoutObservationWindow "00:30:00"

*# Audit policies*

Auditpol /set /category:"Account Logon" /success:enable /failure:enable

Auditpol /set /category:"Account Management" /success:enable /failure:enable

Auditpol /set /category:"DS Access" /success:enable /failure:enable

1. Logging și Monitorizare

*# Configurare retenție logs*

wevtutil sl Security /rt:365d

wevtutil sl Application /rt:365d

wevtutil sl System /rt:365d

*# Activare logging PowerShell*

Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" -Name "EnableScriptBlockLogging" -Value 1

*# Configurare Event Forwarding*

winrm quickconfig -quiet

wecutil qc -quiet

1. Restricționare Acces

*# Dezactivare guest account*

Disable-LocalUser -Name "Guest"

*# Restricționare acces RDP*

Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name "fDenyTSConnections" -Value 1

*# Configurare Windows Firewall*

Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

**5. Anexe**

**5.1 Documentație Tehnică**

* Mapare completă MITRE ATT&CK
* Ghiduri CIS Benchmarks pentru sistemele afectate
* Documentație completă CVE-uri identificate
* Rapoarte scanare vulnerabilități

**5.2 Scripts și Tooling**

* Scripts verificare configurație
* Scripts remediere automată
* Templates configurație securizată
* Tooling pentru monitorizare continuă

**5.3 Documentație Compliance**

* Checklist HIPAA
* Matrice conformitate GDPR
* Politici de securitate recomandate
* Proceduri operaționale standard

**5.4 Materiale Training**

* Ghid awareness securitate
* Proceduri răspuns incidente
* Materiale anti-phishing
* Ghiduri best practices

**5.5 Rapoarte Detaliate**

* Raport analitic vulnerabilități
* Statistici și metrici impact
* Timeline remediere recomandată
* Analiză cost-beneficiu măsuri securitate