Tuần 4 - Triển khai biện pháp phòng chống

Biện pháp phòng ngừa và chuẩn bị

Hardening AD và hệ thống

- Vô hiệu hóa Truy cập SAM qua NULL Session
  - Đảm bảo GPO (Default Domain Controllers Policy) được cấu hình để không cho phép liệt kê tài khoản SAM ẩn danh
- Yêu cầu Kerberos Pre-authentication
  - Đảm bảo flag `Do not require Kerberos preauthentication` bị tắt cho tất cả các tài khoản
- Quản lý mật khẩu mạnh
  - Áp dụng chính sách mật khẩu mạnh. Sử dụng LAPS (Local Administrator Password Solution). Đảm bảo mật khẩu tài khoản dịch vụ (Service Accounts) mạnh và được xoay vòng (áp dụng gMSA - Group Managed Service Accounts)
- Hạn chế truy cập WinRM
  - Không cho phép nhóm Domain Users kết nối WinRM. Chỉ cấp quyền cho nhóm quản trị cụ thể từ các trạm quản trị đặc quyền (Privileged Access Workstations - PAW). Sử dụng JEA (Just Enough Administration)
- Áp dụng nguyên tắc đặc quyền tối thiểu (Principle of Least Privilege - PoLP)
  - Rà soát và thu hồi quyền không cần thiết trên ACLs. Ví dụ: `dev01` không nên có `GenericWrite` trên admin_service
- Delegation Control
  - Hạn chế tối đa các loại Delegation. Đối với RBCD (Resource-Based Constrained Delegation), giám sát việc thay đổi thuộc tính `msDS-AllowedToActOnBehalfOfOtherIdentity`. Đánh dấu tài khoản nhạy cảm là "Account is sensitive and cannot be delegated"
- LSASS Protection
  - Bật Credential Guard và LSA Protection (as a Protected Process Light - PPL) để ngăn chặn việc dump LSASS
- NTLM Restriction/Hardening
  - Ưu tiên Kerberos. Vô hiệu hóa NTLMv1, hạn chế NTLMv2
- Quản lý bản vá & cấu hình an toàn
  - Cập nhật bản vá, áp dụng các cấu hình chuẩn từ Microsoft (SCT), CIS Benchmarks

Xây dựng kiến trúc an toàn

- Mô hình Tiered Administration
  - Cách ly tài khoản quản trị và tài sản theo tầng
- Privilege Access Workstations
  - Sử dụng máy trạm chuyên dụng, được bảo vệ cho tác vụ quản trị
- Phân đoạn mạng
  - Cách ly các vùng mạng

Chuẩn bị ứng phó và nâng cao nhận thức

- Xây dựng và kiểm thử kế hoạch ứng phó (Incident Response)
- Đào tạo nhận thức an ninh cho người dùng và quản trị viên
- Đánh giá an ninh định kỳ

Biện pháp phát hiện & ứng phó ban đầu

Giám sát, cảnh báo và phân tích (SIEM, EDR, AD monitoring)

- Sử dụng SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), và Công cụ Giám sát AD (AD Monitoring Tools)
- Thiết lập cảnh báo cho các hoạt động đáng ngờ liên quan đến các kỹ thuật đã mô phỏng: RID Cycling, AS-REP Roasting, lạm dụng WinRM, các truy vấn LDAP/SMB hàng loạt (dấu hiệu BloodHound), thay đổi ACL/thuộc tính AD quan trọng (phát hiện ACL/RBCD Abuse), hành vi dump LSASS (`Mimikatz`), và xác thực NTLM bất thường (dấu hiệu Pass-the-Hash)
- Theo dõi các Event ID quan trọng (ví dụ: `4768` cho Kerberos TGT, `5136` cho thay đổi đối tượng AD, `4624`/`4776` cho logon/NTLM, `4688` cho tạo tiến trình, log Sysmon)

Hành động ứng phó ban đầu

- Cô lập hệ thống
- Vô hiệu hoá tài khoản
- Thu thập volatile data (RAM, process, kết nối mạng)
- Thông báo cho đội IR

Biện pháp khắc phục & rút kinh nghiệm

Loại bỏ và khôi phục

- Loại bỏ persistence của hacker
- Khôi phục hệ thống (rebuild/recovery from known good state)
- Reset password: đặc biệt là `krbtgt` (đổi 2 lần - double reset)
- Xác minh tính toàn vẹn

Phân tích điều tra (Forensics)

Phân tích log, RAM dump, disk image để hiểu rõ chuỗi tấn công, root cause, và TTPs

Rút kinh nghiệm và cải thiện

- Cập nhật kế hoạch IR
- Tăng cường biện pháp kiểm soát
- Nâng cao nhận thức