INDEX

SECTION 1: PREPARING THE ATTACK

MODULE 1: SOCIAL ENGINEERING ATTACK VECTORS

1.1. Introduction

1.2. Email delivery & macro fundamentals

1.2.1 Email delivery fundamentals

• SPF, DKIM, DMARC, Accepted Domains & Spam Traps

• Circumventing Defenses

1.2.2 Macro fundamentals

• Macros: Documents Case

• Remote templates

1.3. Attack vector development

1.3.1 Custom macro development

• Macro leveraging file properties to hide its payload and StdIn to avoid logging

• Using ActiveX controls for macro execution

• The classic download and execute macro, with a twist

• Multi-platform macro malware

• RTF + Signed binary + DLL hijacking + Custom MSF loader =

• Embedding an executable in a macro (executable2vbs)

• Network-tracing macro

• Multi-stage macro malware using DNS for payload retrieval and exfiltration

• Macro malware performing direct shellcode injection

• Macros on PowerPoint (Custom Actions)

• Macro obfuscation

1.3.2 Abusing Office capabilities

- OLE objects for payload execution
- Exploiting MS16-032 via Excel DDE without macros
- Office-handled links

1.3.3 Uncommon extensions

- CHM Files + Custom JS Backdoor
- HTML Application (HTA) files
- Shortcut (LNK) files
- Web Query (IQY) files
- MSG files
- Rich Text Format (RTF) files

1.3.4 Custom ClickOnce applications

- Custom beaconing malware
- Minimizing on-disk footprint (PowerShell without PowerShell)

1.4 Phishing techniques

1.4.1 Leveraging CSRF and Open Redirects

1.4.2 Creating trustworthy-looking redirect forms (Custom JavaScript)

1.4.3 URL spoofing techniques

- Data URIs
- Phishing page (multilayer) obfuscation

1.4.4 BeEF and custom scripting to gain administrative access

1.4.5 Mimicking DYRE banking trojan’s spread method

1.5 Generic Anti-analysis

1.5.1 Apache mod_rewrite for anti-analysis

- User Agent Redirection

SECTION 2: RED TEAMING ACTIVE DIRECTORY

MODULE 1: ADVANCED AD RECONNAISSANCE & ENUMERATION

1.1 Introduction

1.2 The traditional approach

1.2.1 Using a sniffer or a network scanning tool

1.2.2 Recon & enumeration through a non-domain joined Linux machine

- Leveraging SNMP
- Recon through dig
- SMB (& NULL Sessions)
- Share enumeration

1.2.3 Defeating anonymous user restrictions (against legacy systems)

1.2.4 Recon & enumeration through a domain joined Windows machine

- net commands
- Enumeration through DNS
- Enumeration through NetBIOS
- dumpsec, shareenum, enum binaries

1.3 Red team-oriented reconnaissance & enumeration

1.3.1 Fundamentals & User Hunting

- DNS using LDAP
- SPN Scanning / Service Discovery
- Group Policies
- Fundamentals of user hunting (API calls, LDAP, PSReflect, linkable patterns etc.)

a. User Hunting

b. Stealthy User Hunting

- Local Administrator Enumeration
- Derivative Local Admin
- Identifying Administrator Accounts: Group Enumeration
- Identifying Administrator Accounts: RODC Groups
- Identifying Administrator Accounts: AdminCount =1
- GPO Enumeration & Abuse
- Identifying Administrator Accounts: GPPs
- Identifying Active Directory Groups with Local Admin Rights
- Identifying regular users having admin rights
- Identifying Virtual Admins
- Identifying Computers Having Admin Rights
- Interesting Group Enumeration
- Follow the Delegation
- Custom Domain/OU Delegation
- MS LAPS Delegation

1.3.2 Important AD Component Enumeration

- AD Forest Information
- AD Domain Information
- The PDC emulator
- Domain Trusts
- BloodHound
- Identifying Partner Organizations using Contacts

1.3.3 Interesting Corners of Active Directory

- Active Directory ACLs
- Sensitive Data in User Attributes

- AD User & Computer Properties
- Deleted AD Objects
- Domain Password Policies

1.3.4 Post-Exploitation Recon & Enumeration

- Defensive measure related information

1.3.5 Recon & Enumeration Tips & Tricks

- Recon & Enumeration without PowerShell
- Mapping the application server attack surface of an organization
    a. Stealthy web application mapping
    b. Gathering browser data to identify internal websites and applications

1.4 Situational Awareness

1.4.1 Evade Parent-Child Process Anomaly Detection

1.4.2 Abusing PowerShell

1.4.3 Information Gathering Through WMI

1.4.4 Seatbelt

MODULE 2: RED TEAMING ACTIVE DIRECTORY

2.1 Introduction

2.2 AD Fundamentals

- LDAP
- Authentication (incl. weaknesses & known attacks)
- Authorization
- AD & DNS
- AD Components (DCs, RODCs, Global Catalogs, Data Store, Replication,

Domains, Forests, Trusts etc.)

2.3 Traditional AD Attacks

2.3.1 LDAP Relay

2.3.2 Exploiting Group Policies

2.3.3 RDP MiTM

2.3.4 Sniffing Authentication Traffic

2.3.5 Downgrading NTLM

2.3.6 Non-MS Systems Leaking Credentials

2.3.7 LLMNR and NBT-NS poisoning (incl. enhancing Responder)

2.4 Red team-oriented AD attacks (Part 1)

2.4.1 PowerShell Defenses in AD

2.4.2 Bypassing PowerShell's Security Enhancements

2.4.3 Paths to AD Compromise

2.4.3.1 MS14-068

2.4.3.2 Unconstrained Delegation (incl. pass-the-ticket)

2.4.3.3 OverPass-the-Hash (Making the most of NTLM password hashes)

2.4.3.4 Pivoting with Local Admin & Passwords in SYSVOL

2.4.3.5 Dangerous Built-in Groups Usage

2.4.3.6 Dumping AD Domain Credentials

2.4.3.7 Golden Tickets

2.4.3.8 Kerberoast

2.4.3.9 Silver Tickets

2.4.3.10 Trust Tickets

2.5 Leveraging Kerberos Authentication

2.5.1 Kerberos tickets when NTLM is disabled

2.5.2 Password spraying using Kerberos

2.6 Red team-oriented AD attacks (Part 2)

- 2.6.1 Targeted Kerberoasting
- 2.6.2 ASREPRoast
- 2.6.3 Over-pass The Hash / Pass The Key (PTK)
- 2.6.4 Pass The Ticket (PTT)
- 2.6.5 The “Printer Bug” and Kerberos Unconstrained Delegation
- 2.6.6 Kerberos Constrained Delegation
- 2.6.7 Kerberos Resource-Based Constrained Delegation
  - 2.6.7.1 Kerberos Resource-Based Constrained Delegation Computer Object Take Over
  - 2.6.7.2 Kerberos Resource-Based Constrained Delegation Via Image Change
- 2.6.8 Kerberos Attacks Using Proxies
- 2.6.9 Abusing Forest Trusts
- 2.6.10 LAPS
  - 2.6.10.1 LAPS Exploitation
- 2.6.11 ACLs on AD Objects
- 2.6.12 Backup Operators

2.6 Red team-oriented AD attacks (Part 2)

- 2.6.13 ACLs in Active Directory
  - 2.6.13.1 Escalating Privileges using Exchange
  - 2.6.13.2 Invoke-ACLPwn
  - 2.6.13.3 NTLMRelayx
- 2.6.14 Abusing Privileged Access Management (PAM)
- 2.6.15 Just Enough Administration (JEA)
  - 2.6.15.1 Abusing Just Enough Administration (JEA)
- 2.6.16 DNSAdmins

SECTION 3: RED TEAMING CRITICAL DOMAIN INFRASTRUCTURE

MODULE 1: RED TEAMING MS SQL SERVER

1.1 Introduction

1.2 MS SQL Server Fundamentals

1.3 Locating & Accessing SQL Servers

- The unauthenticated perspective
- The local user perspective
- The domain user perspective

1.4 Escalating privileges within SQL Server

- Unauthenticated User / Local User / Domain User -> SQL login
- Gaining Initial Foothold on SQL Server
- SQL login -> sysadmin
- Weak Passwords & Blind SQL Server Login Enumeration
- Impersonation
    - i. Impersonation Privilege
    - ii. Stored Procedure and Trigger Creation / Injection Issues
    - iii. Automatic Execution of Stored Procedures
- sysadmin -> Service Account
- OS Command Execution through SQL Server
- Shared Service Accounts
- Crawling Database Links
- UNC Path Injection

1.5 Common Post-Exploitation Activities

- Persistence
- Setting up a debugger for utilman.exe
- Establishing persistence with xp_regwrite

- Exporting and backdooring custom CLR assemblies
- Identifying Sensitive Data
- Parsing and searching for sensitive data
- Targeting DBs featuring transparent encryption
- Extracting SQL Server Login password hashes

1.6 Poisoning the SQL Server Resolution Protocol

MODULE 2: RED TEAMING EXCHANGE

2.1 Introduction

2.2 Exchange fundamentals

2.2.1 Protocols

2.2.2 Functions / Components

- Autodiscover
- Global Address List
- Outlook Rules
- Outlook Forms

2.3 Attacking externally (Remote Compromise)

2.3.1 Recon & OWA Discovery

2.3.2 Domain Name Discovery (Timing attack)

2.3.3 Naming Schema Fuzzing

2.3.4 Username Enumeration (Timing attack)

2.3.5 Password Discovery (Password Spraying)

2.3.6 GAL Extraction

2.3.7 More password discovery

2.3.8 Bypassing 2 Factor Authentication

2.3.9 Remote Compromise

- Spreading the compromise

- Pillaging mailboxes for credentials/sensitive data
- Internal Phishing
- Malicious Outlook Rules (including bypassing network segmentation)
- Malicious Outlook Forms (including bypassing network segmentation)

2.4 Attacking from the inside

- Misusing Exchange ActiveSync (EAS) to access internal file shares

2.5 Privilege Escalation By Busing Exchange

MODULE 3: RED TEAMING WSUS

3.1 Introduction

3.2 Windows Update Fundamentals

- Windows Update from a security perspective
- Windows Update Overview (Windows Update Communications, Update types and storage)
- WSUS
- WSUS Security
- Identifying WSUS

3.3 Attacking WSUS

- Unencrypted Communications & Malicious Update injection
- Via straight ARP spoofing
- Via tampering with the target's proxy settings (WPAD Injection)
- Leveraging WSUS Interconnectivity

3.4 Leveraging Windows Update for Persistence

SECTION 4: EVASION

MODULE 1: DEFENSE EVASION

1.1 Evasion

1.2 AMSI

1.3 Bring Your Own Interpreter (BYOI)

1.4 Event Tracking for Windows (ETW)

1.5 SYSMON

1.6 Endpoint Detection and Response (EDR)

1.7 Discovery

1.8 Lateral Movement

1.9 Credential Access

1.10 Sensitive Groups

1.11 Custom Payload Development

1.12 Removing User-Mode Hooks

1.13 Stealth Macro Development

Lab 1: Custom Undetectable Macro Development

Your goal is to develop a custom macro-based attack (and the accompanying payloads), to compromise a target without being detected.

Lab 2: Establishing A Shell Through the Victim's Browser

During the lab you will develop a payload from scratch that will establish a shell through the victim’s browser.

Lab 3: Serving a Malicious Update Through WSUS

You are engaged in an internal network penetration test. Your goal is to compromise a Windows 7 machine (10.100.11.101) through a Windows 10 machine (10.100.11.100), leveraging weak network configurations and abusing WSUS.

Lab 4: SQL injection to Domain Administrator Hash

You are engaged in an external network penetration test. Your goal is to stealthily capture the Domain Administrator's password hash through the internet facing Web App 1, leveraging weak SQL Server and database configurations as well as legitimate SQL Server capabilities.

Lab 5: Red-teaming Active Directory Lab #1 (Covenant C2 VS ELS.LOCAL)

In this fully featured Active Directory lab you will heavily use Covenant C2 and modern C#/.NET tradecraft to achieve a great number of red-teaming objectives. You will have the opportunity to practice: attack path enumeration using Bloodhound, pivoting, lateral movement, (targeted) kerberoasting, golden/silver ticket creation, SIDHistory attacks, abusing constrained/unconstrained delegation, DCSync, SMB-based C2, bypassing Constrained Language Mode/AMSI/Applocker, attacking SQL Server, HTTP NetNTLM Relaying, privilege escalation, ACL-based attacks

Lab 6: Red-teaming Active Directory Lab #2 (ELS.BANK)

In this fully-featured and hardened Active Directory lab you will have to opportunity to practice: abusing a PAM trust, privilege escalation, ACL-based attacks, DCSync, abusing constrained delegation, decrypting a powershell secure string, malicious Kerberos ticket creation, abusing AD description attributes, abusing resource-based delegation, the “printer bug”, abusing the machine key of IIS

Lab 7: Red-teaming Active Directory Lab #3 (ELS.CORP)

In this fully featured Active Directory lab you will have to opportunity to practice: Phishing, stealthy enumeration, pivoting and lateral movement, SQL Server attacks, abusing forest trusts, Linux and Windows privilege escalation, malicious Kerberos ticket creation, the “printer bug”, exploiting web app vulnerabilities to gain initial foothold, exploiting domain-joined Linux machines and Jumphosts