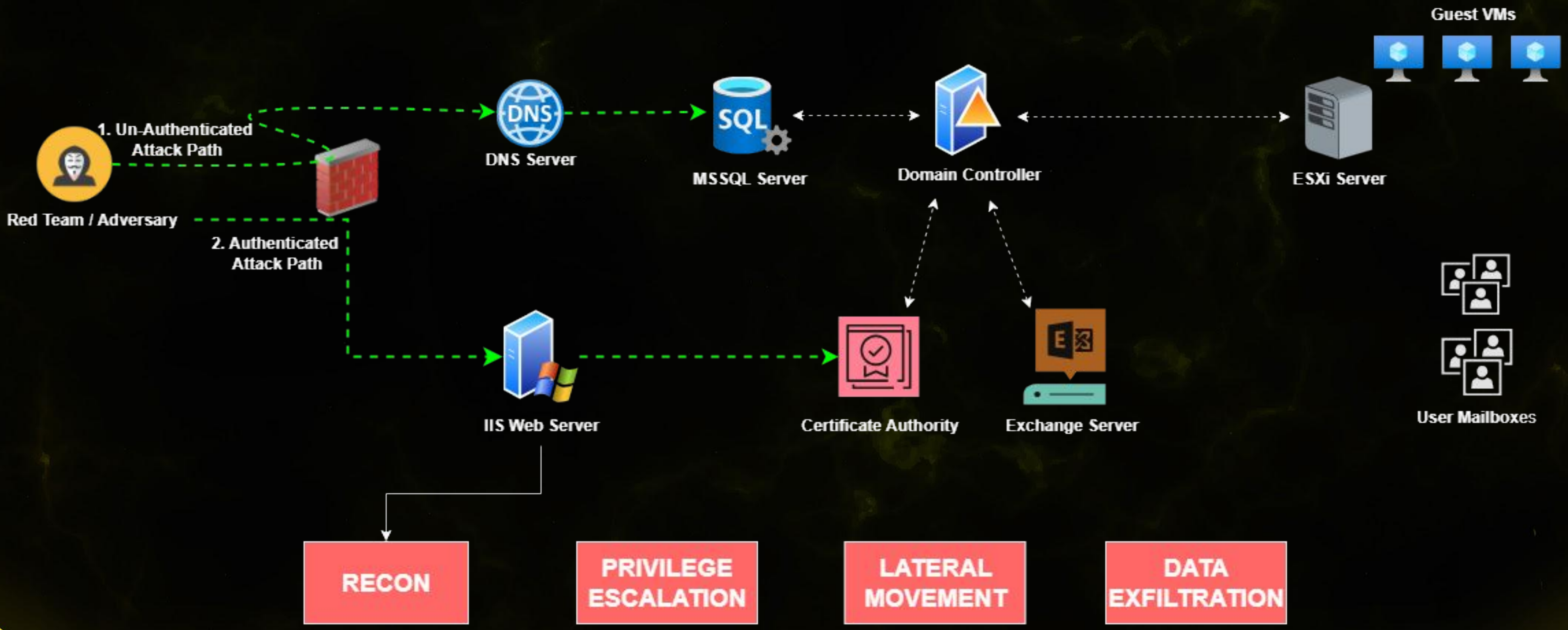
CWL
CyberWarFare Labs

Certified AD Red Team Specialist (AD-RTS)

Certified AD Red Team Specialist (AD-RTS) Architecture



CWL
CyberWarFare Labs

I. Active Directory Security

1.1 Introduction

1.2 Entra ID & On-Premise AD

1.3 Core Components of AD

- 1.3.1 Schema
- 1.3.2 Global Catalog
- 1.3.3 Database (NTDS.dit)
- 1.3.4 Group Policy
- 1.3.5 AD Objects

1.4 Authentication & Authorization in AD

1.5 Highly abused roles

II. Certificate Services Security

2.1 Introduction

2.2 Core Components

- 2.2.1 Authority
- 2.2.2 Templates
- 2.2.3 Web Enrollment
- 2.2.4 Certificate Revocation List
- 2.2.5 Certificate Distribution Point

2.3 Common Attacks & Mis-configuration

III. Abusing Exchange Server Roles

3.1 Introduction

3.2 Core Components

- 3.2.1 Outlook Web Access
- 3.2.2 Exchange Web Services
- 3.2.3 MAPI & Autodiscover

3.3 Targeted Exchange Admin Roles

3.4 DEMO

- 3.4.1 Persistence via Mailbox Delegation
- 3.4.2 Application Impersonate Role
- 3.4.3 Import/Export Mailbox Role
- 3.4.4 Backdoor Transport Rule

IV. Attack Surface of ESXi integrated with AD

4.1 Introduction

4.2 Why ESXi are domain joined

4.3 Attack Scenarios in AD integrated ESXi

4.4 [DEMO] Administrator Role

V. AD-RTS Cyber Range Lab Part 1

5.1 Case Studies

- 5.1.1 Code Injection Attacks using publicly disclosed IIS machine Keys
- 5.1.2 Exchange “ApplicationImpersonation” Role Abuse
- 5.1.3 Command Execution to Guest VMs in ESXi Hypervisor
- 5.1.4 Introduction to CyberWarFare Labs AD-RTS Cyber Range Lab

V. AD-RTS Cyber Range Lab Part 1

5.2 Simulating Unauthenticated Adversary

5.2.1 Initial Access: DNS Abuse, Anonymous Recon (LDAP), Kerberos PREAUTH & ACL abuse.

5.2.2 Privilege Escalation: Compromise SQL Server → SYSTEM → Credential Dumping.

5.2.3 Lateral Movement: Exploit ESC misconfigurations in Certificate Server → Impersonation → RCE on Domain Controller.

5.2.4 Data Exfiltration: Discover/Execute commands on ESXi Host and Guest VMs.

VI. AD-RTS Cyber Range Lab - Part 2

6.1 Emulating Authenticated Adversary - Part 2

- 6.1.1 Initial Access: Exploit Internet-facing IIS Server (Pillaging keys, VIEWSTATE abuse) → Command Execution.
- 6.1.2 Privilege Escalation: Decrypt DPAPI blobs → Certificate Impersonation → Domain Administrator.
- 6.1.3 Lateral Movement:
  - A. Domain Controller: Direct pivot.
  - B. Exchange Server: Enumerate/Abuse "AppImpersonate" privileges → Access & pillage mailboxes.
- 6.1.4 Data Exfiltration: Stealthy compression and exfiltration via encrypted channels.

CWL
CyberWarFare Labs

CWL

CyberWarFare Labs

Thank You

Cyberwarfare.live