ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Cyber range csapat

Előadók: Kövesdi Gábor Verasztó Balázs Kraudy Richárd

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Cyber range

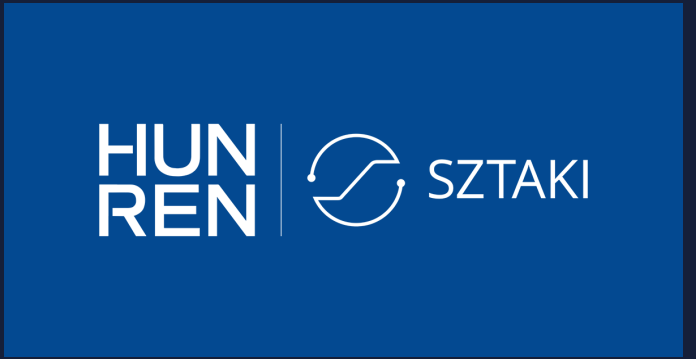
- Valós idejű gyakorló tér
- Nem csak piros a kék ellen

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

A csapat

- Hallgatók, tanárok, külsős segítők
- Támogatók: NKI, Andrews, HUN-REN SZTAKI



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Kék csapat

- Feladatunk a védelem
  - Ennek tervezése
  - felállítása
- Felkészülés és stratégia
- Monitoring, logelemzés, csapatmunka
- Wazuh, Ansible, TheHive

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

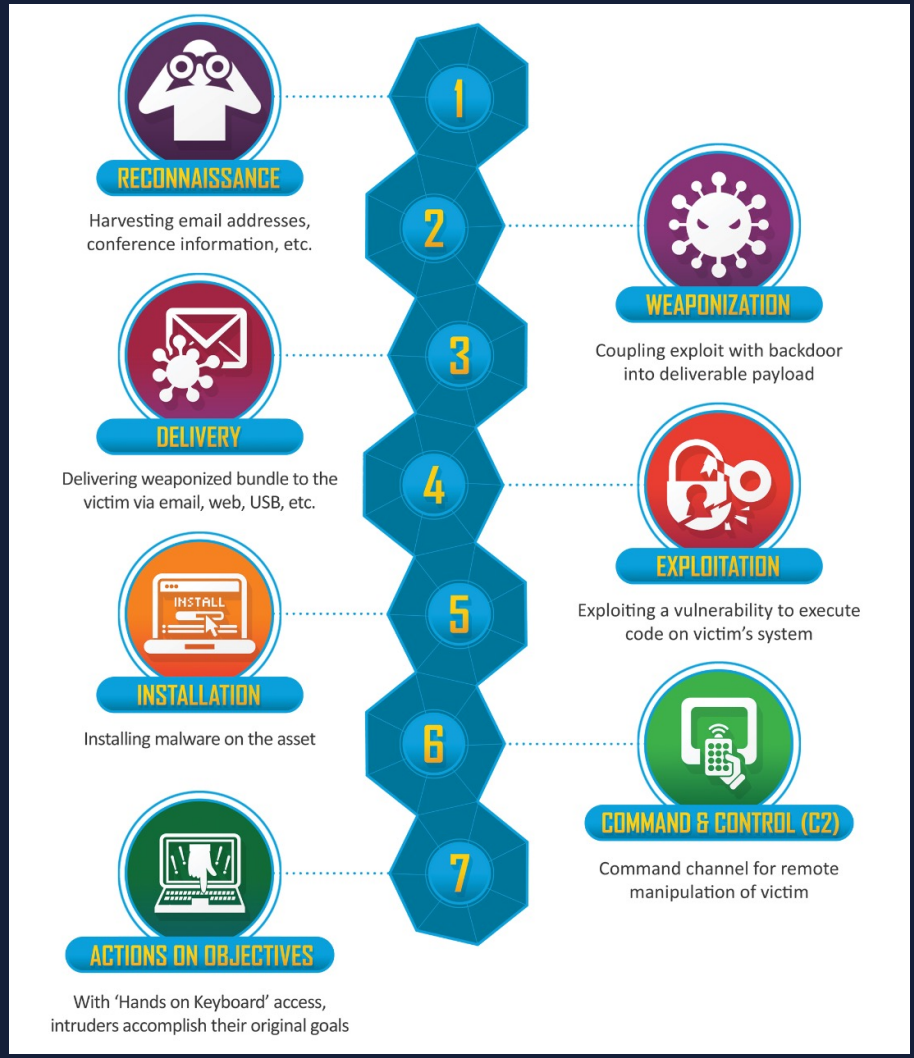
Piros csapat

Valós támadások szimulálása
Sérülékenységek feltárása és kihasználása
Zöld csapattal való munka

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

A támadás hét lépcsőfoka

- 1: Kutatás, feltérképezés
- 2: Gyártás, előállítás
- 3: Szállítás, terjesztés
- 4: Használhatóvá tétel
- 5: Beágyazás, beültetése
- 6: Irányítás, irányítás
- 7: Megvalósítás, végrehajtás



ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Forgatókönyv

Phishing támadás utáni intézkedések elvégzése

Érintett felhasználók kikutatása, fiókjaik “biztonságossá tétele”

- Érintett felhasználók megtalálása
- Fiókok tiltása, új jelszavak beállítása

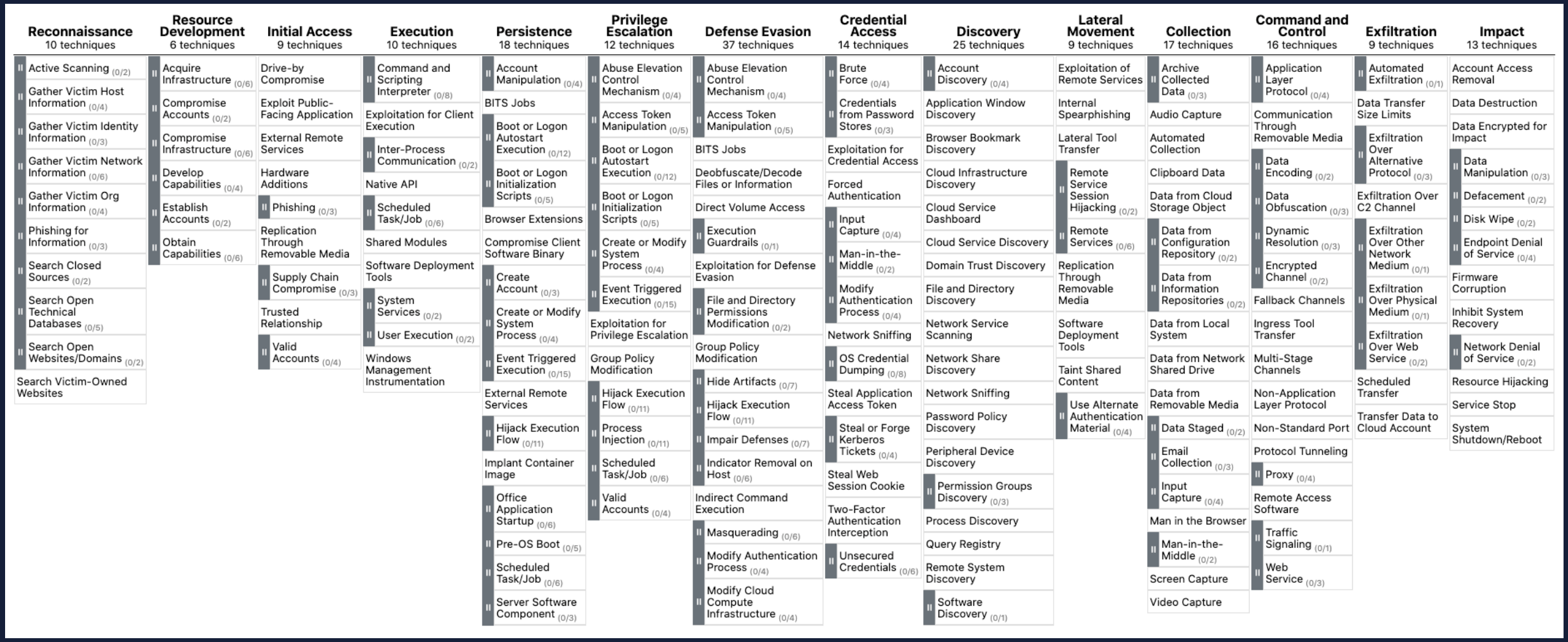
Phising oldal elérhetőségének tiltása

Érintett állományok visszaállítása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Mitre ATT&CK®

- Keretrendszer
- Taktikák
- Technikák
- Folyamatosan frissülő


Reconnaissance
10 techniques
Active Scanning (0/2)
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases (0/5)
Search Open Websites/Domains (0/2)
Search Victim-Owned Websites
Resource Development
6 techniques
Acquire Infrastructure (0/6)
Compromise Accounts (0/2)
Compromise Infrastructure (0/6)
Develop Capabilities (0/4)
Establish Accounts (0/2)
Obtain Capabilities (0/6)
Initial Access
9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted Relationship
Valid Accounts (0/4)
Execution
10 techniques
Command and Scripting Interpreter (0/8)
Exploitation for Client Execution
Inter-Process Communication (0/2)
Native API
Scheduled Task/Job (0/6)
Shared Modules
Software Deployment Tools
System Services (0/2)
User Execution (0/2)
Windows Management Instrumentation
Persistence
18 techniques
Account Manipulation (0/4)
BITS Jobs
Boot or Logon Autostart Execution (0/12)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or Modify System Process (0/4)
Event Triggered Execution (0/15)
External Remote Services
Hijack Execution Flow (0/11)
Implant Container Image
Office Application Startup (0/6)
Pre-OS Boot (0/5)
Scheduled Task/Job (0/6)
Server Software Component (0/3)
Privilege Escalation
12 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/12)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Event Triggered Execution (0/15)
Exploitation for Privilege Escalation
Group Policy Modification
Hijack Execution Flow (0/11)
Process Injection (0/11)
Scheduled Task/Job (0/6)
Valid Accounts (0/4)
Defense Evasion
37 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Deobfuscate/Decode Files or Information
Direct Volume Access
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Group Policy Modification
Hide Artifacts (0/7)
Hijack Execution Flow (0/11)
Impair Defenses (0/7)
Indicator Removal on Host (0/6)
Indirect Command Execution
Masquerading (0/6)
Modify Authentication Process (0/4)
Modify Cloud Compute Infrastructure (0/4)
Credential Access
14 techniques
Brute Force (0/4)
Credentials from Password Stores (0/3)
Exploitation for Credential Access
Forced Authentication
Input Capture (0/4)
Man-in-the-Middle (0/2)
Modify Authentication Process (0/4)
Network Sniffing
OS Credential Dumping (0/8)
Steal Application Access Token
Steal or Forge Kerberos Tickets (0/4)
Steal Web Session Cookie
Two-Factor Authentication Interception
Unsecured Credentials (0/6)
Discovery
25 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (0/3)
Process Discovery
Query Registry
Remote System Discovery
Software Discovery (0/1)
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (0/4)
Collection
17 techniques
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (0/2)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Input Capture (0/4)
Man in the Browser
Man-in-the-Middle (0/2)
Screen Capture
Video Capture
Command and Control
16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access Software
Traffic Signaling (0/1)
Web Service (0/3)
Exfiltration
9 techniques
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/2)
Scheduled Transfer
Transfer Data to Cloud Account
Impact
13 techniques
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Caldera

- Támadó szimulálás
- Mitre ATT&CK
- Nyílt forráskodú
- Flexibilis

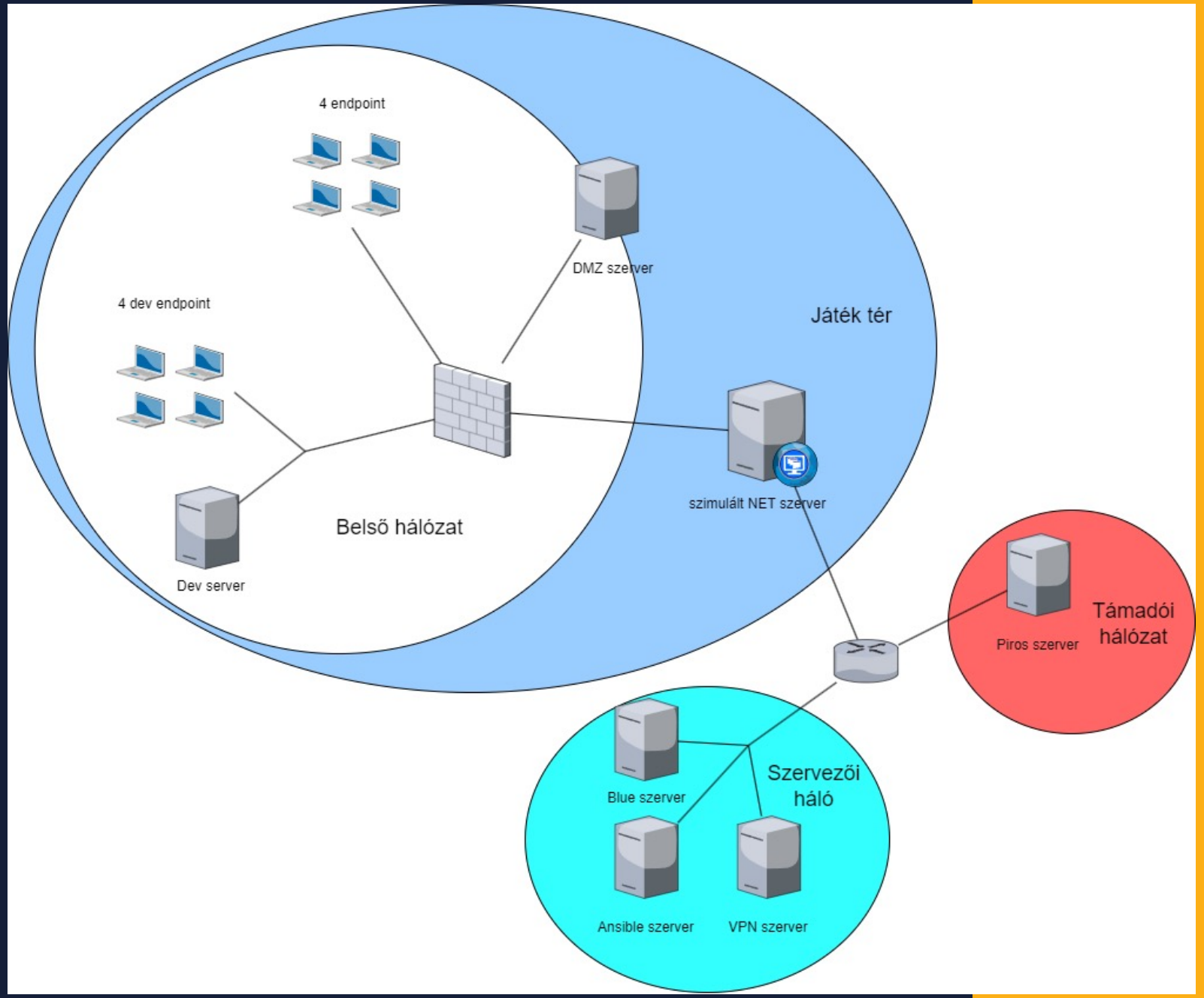
Exploit DB

- Sérülékenységek gyűjteménye
- Ingyenes
- Sérülékenységek kihasználása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Zöld csapat feladata

- Mi az a zöld csapat?
- Hálózat automatukus kreálása
  - Újra használható
  - Moduláris
  - Felhő alapú
  - Bővíthető
- Hálózat alapvető konfigurálása (állandó elemek)


4 endpoint
DMZ szerver
4 dev endpoint
Játék tér
szimulált NET szerver
Belső hálózat
Dev server
Támadói hálózat
Piros szerver
Szervezői háló
Blue szerver
Ansible szerver
VPN szerver

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Használt eszközök






and more..

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Továbbfejlesztési lehetőségek

- Új forgatókönyvek létrehozása
- Új eszközök beépítése
- Feladatok bonyolítása
- Játékos csapat növelése

WE WANT YOU!

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Köszönjük a figyelmet!