БЕЗОПАСНОСТЬ ACTIVE DIRECTORY

Цель программы — сформировать у слушателей всесторонние знания и практические навыки по управлению и защите Active Directory, включая основы архитектуры, групповые политики, методы аудита и защиты от атак, а также инструменты мониторинга и hardening для обеспечения безопасности доменных сред.

Выпускники курса получают свидетельство о повышении квалификации государственного образца, а также именной сертификат учебного центра ROZUM.

Целевая аудитория:

- руководители и специалисты центров обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;
- инженеры и аналитики по информационной безопасности;
- специалисты, участвующие в обеспечении защиты информационных сетей и систем организаций.

Форма обучения — очно с ИКТ (онлайн).
Стоимость обучения одного слушателя — 3100 рублей.

Продолжительность программы —60 академических часов (3 недели).

Учебный план курса

№ п/п	Название тем курса
	Основы Active Directory и групповые политики
1.	Архитектура Active Directory
2.	DNS, репликация и объекты Active Directory
3.	Групповые политики (GPO) и политики безопасности
4.	Лабораторная работа № 1. Развёртывание домена corp.local
5.	Лабораторная работа № 2. Объекты AD и ввод машин в домен
6.	Лабораторная работа № 3. Настройка групповых политик
7.	Вебинар № 1. Разбор модуля 1
	Модель привилегий, разведка и базовый hardening
8.	Модель прав доступа: Access Token, SID, ACL/ACE
9.	MachineAccountQuota, LAPS и gMSA
10.	Лабораторная работа № 4. Разведка и аудит домена в BloodHound
11.	Лабораторная работа № 5. Поиск и эксплуатация мисконфигураций ACL
12.	Лабораторная работа № 6. Базовый hardening и аудит PingCastle
13.	Вебинар № 2. Разбор модуля 2
	Атаки на аутентификацию: Kerberos и NTLM
14.	Протокол Kerberos и атаки на него
15.	NTLM, Pass-the-Hash и DCSync
16.	Лабораторная работа № 7. Kerberoasting и AS-REP Roasting
17.	Лабораторная работа № 8. Pass-the-Hash и обнаружение DCSync
18.	Вебинар № 3. Разбор модуля 3
	NTLM Relay и инфраструктура сертификатов (AD CS)

19.	NTLM Relay и принуждение к аутентификации (Coercion)
20.	Инфраструктура сертификатов AD CS и атаки ESC1–ESC8
21.	Лабораторная работа № 9. NTLM Relay с принуждением (PetitPotam)
22.	Лабораторная работа № 10. Эксплуатация AD CS (ESC1)
23.	Вебинар № 4. Разбор модулей 3–4
	Боковое перемещение и закрепление в системе
24.	Боковое перемещение (Lateral Movement) и механизмы закрепления (Persistence)
25.	Лабораторная работа № 11. Обнаружение бокового перемещения
26.	Лабораторная работа № 12. Поиск и устранение механизмов закрепления
	Мониторинг (SIEM) и комплексный hardening AD
27.	Advanced Audit Policy и ключевые Event ID
28.	SIEM Wazuh для детектирования атак на AD
29.	Комплексный hardening Active Directory
30.	Лабораторная работа № 13. Мониторинг атак в Wazuh
31.	Лабораторная работа № 14. Финальный hardening и контроль PingCastle
32.	Вебинар № 5. Разбор модулей 5–6 и подготовка к экзамену
	Итоговая аттестация
33.	Итоговый экзамен. Аудит и hardening «грязной» AD-инфраструктуры