Red Seer Labs: Unleash Your Potential in Penetration Testing

Are you a student or professional eager to master the art of penetration testing and excel in the cybersecurity field? Red Seer Labs is your ultimate gateway to success. Explore our offerings designed specifically for aspiring penetration testers.

Why Red Seer Labs?

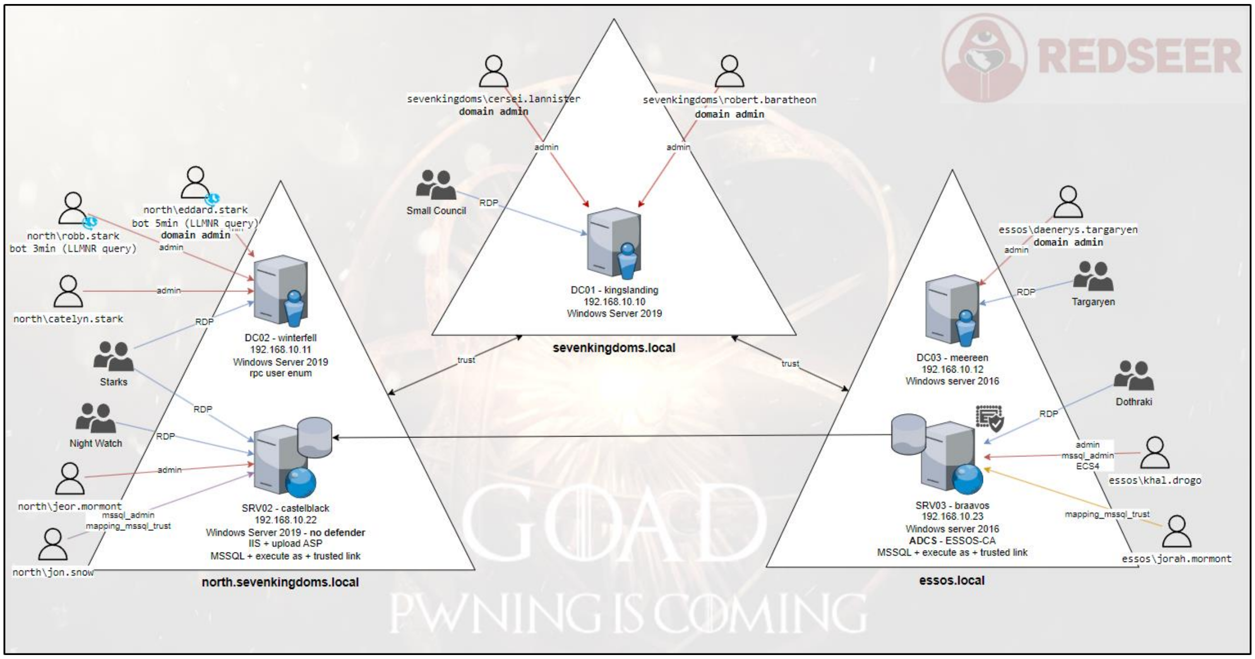
1. **Realistic Testing Scenarios**: Step into the world of real-world attacks with Red Seer Labs. Experience immersive virtualized environments that mirror diverse network architectures, operating systems, and applications. Sharpen your skills by tackling lifelike scenarios without risking actual systems.
2. **Advanced Threat Simulations**: Red Seer Labs offers unparalleled opportunities to simulate advanced cyber-attacks. Test your mettle against network intrusions, social engineering exploits, and malware infections. Uncover vulnerabilities in a controlled environment and gain practical insights into remediation techniques.
3. **Collaborative Learning Platform**: Red Seer Labs provides a dynamic and interactive learning platform where aspiring penetration testers like you can engage in secure communication, knowledge-sharing, and peer collaboration. Exchange ideas, insights, and strategies with fellow students, fostering continuous growth and improvement as you navigate your penetration testing journey.
4. **Partnership with Build Cyber**: Red Seer Security proudly partners with Build Cyber, a respected non-profit organization, to offer you exclusive benefits. As part of this partnership, you gain access to Build Cyber's Apprentice and Mentorship Program, which provides invaluable guidance, mentorship, and hands-on experience in the cybersecurity field. This partnership also aligns with their Cybersecurity Certification Pathway Program, enabling you to advance your skills and knowledge on a structured certification track.

Unleash Your Potential with Red Seer Labs!

Empower yourself with the tools and experiences you need to become a proficient penetration tester. Red Seer Labs offers realistic testing scenarios, advanced threat simulations, a collaborative learning platform, and a partnership with Build Cyber, enabling you to accelerate your growth and excel in the cybersecurity field.

Take the first step towards a successful career in penetration testing. Join Red Seer Labs today and unlock your potential!

Red Seer Labs - Your Path to Penetration Testing Excellence



The Red Seer Labs environment currently comprises five virtual machines, based on the Game of Active Directory V2 open-source project, with each serving a specific purpose:

1. **kingslanding**:
    - Role: Domain Controller (DC01)
    - Operating System: Windows Server 2019
    - Default Configuration: Windows Defender enabled
    - Domain: north.sevenkingdoms.local
2. **winterfell**:
    - Role: Domain Controller (DC02)
    - Operating System: Windows Server 2019
    - Default Configuration: Windows Defender enabled
    - Domain: sevenkingdoms.local
3. **castelblack**:
    - Role: Server (SRV02)
    - Operating System: Windows Server 2019
    - Default Configuration: Windows Defender disabled
    - Services: MSSQL, IIS
    - Domain: sevenkingdoms.local

4. **meereen**:

    - Role: Domain Controller (DC03)
    - Operating System: Windows Server 2016
    - Default Configuration: Windows Defender enabled
    - Domain: sevenkingdoms.local

5. **braavos**:

    - Role: Server (SRV03)
    - Operating System: Windows Server 2016
    - Default Configuration: Windows Defender enabled
    - Services: MSSQL, ADCS (Active Directory Certificate Services)
    - Domain: essos.local

This lab environment provides a hands-on platform for exploring and practicing various scenarios and techniques related to penetration testing, network security, and system vulnerabilities.

The Red Seer Labs environment features various attacks and vulnerabilities associated with the multi-Forest, multi-domain simulated enterprise. Here's a breakdown of the attacks and vulnerabilities specific to different domains, users, groups and machines:

<u>NORTH.SEVENKINGDOMS.LOCAL</u>

STARKS: RDP on Winterfell and Castelblack servers.

- **arya.stark:** Can execute commands as a user on MSSQL.
- **eddard.stark:** Has domain admin privileges for the "north" domain. Can perform LLMNR requests for NTLM relay with responder.
- **robb.stark:** Utilizes a bot for LLMR (Link-Local Multicast Name Resolution) requests every 3 minutes.
- **brandon.stark:** Vulnerable to ASREP_ROASTING attack.
- **jon.snow:** Holds MSSQL admin privileges, performs KERBEROASTING, has cross-domain group access, and exploits a trusted link in MSSQL.
- **hodor:** Vulnerable to PASSWORD SPRAY attacks using "password" as the username.
- **catelyn.stark:**
- **sansa.stark:**
- **rickon.stark:**
- **theon.greyjoy:**

NIGHT WATCH: RDP on Castelblack server.

- **samwell.tarly:** Exploits passwords stored in LDAP descriptions, executes MSSQL commands as a login, and abuses the GPO settings of the "STARKWALLPAPER" GPO.
- **jon.snow:**
- **jeor.mormont:**

MORMONT: RDP on Castelblack server.

- **jeor.mormont:** Holds ACL (Access Control List) permissions to perform RDP on "castelblack" and has write permissions for ACL and ownership on the "Night Watch" group.
- **AcrossTheSea:** Cross-forest group.

<u>SEVENKINGDOMS.LOCAL</u>

LANISTERS:

- **tywin.lannister:** Forces password change for "jaime.lannister" using ACL.
- **jaime.lannister:** Has generic write permissions on the "joffrey.baratheon" user using ACL.
- **tyron.lannister:** ACL self-membership abuse to gain membership in the "Small Council" group.
- **cersei.lannister:** Holds domain admin privileges for the "sevenkingdoms" domain.

BARATHEON: RDP on Kingslanding Domain Controller

- **robert.baratheon:** Holds domain admin privileges for the "sevenkingdoms" domain.
- **joffrey.baratheon:** ACL Write DACL on “tyron.lannister” user.
- **stannis.baratheon:** ACL GenericAll rights on Kingslanding and WriteProperty privileges on Domain Admins group.
- **renly.baratheon:**

SMALL COUNCIL: ACL add Member to dragonstone group and RDP on Kingslanding DC.

- **petyr.baelish:** Abuses ACL to gain write permissions on the "Domain Admins" group.
- **lord.varys:** Holds generic permissions on the "Domain Admins" group and belongs to the "AccrossTheNarrowSea" group.
- **maester.pycelle:** Has write ownership permissions on the "Domain Admins" group.

DRAGONSTONE: ACL WriteOwner on Kingsguard group.

KINGSGUARD: ACL GenericAll on the “stannis.baratheon” user.

ACROSSTHENARROWSEA: Cross-forest group.

ESSOS.LOCAL

TARGARYEN:

- **daenerys.targaryen:** Holds domain admin privileges for the "essos" domain.
- **Jorah.**mormont: Execute as login and trusted links on MSSQL server, LAPS administrator.
- **viserys.targaryen**

DOTHRAKI:

- **khal.drogo:** Holds MSSQL admin privileges, has generic all permissions on "viserys.targaryen" (shadow credentials), and generic all permissions on "ECS4".

DRAGONSFRIENDS: Cross-forest group.

SPYS: Cross-forest group, read LAPS passwords and GenericAll ACL permissions on “jorah.mormont”.

In addition to the above, the Red Seer Labs environment also includes various attacks on computer users and group permissions. Let's explore these attacks within the context of the different domains and servers:

SEVENKINGDOMS

- **DC01** (kingslanding.sevenkingdoms.local):
    - Administrators: robert.baratheon (User), cersei.lannister (User)
    - RDP Access: Small Council (Group)

NORTH

- **DC02** (winterfell.north.sevenkingdoms.local):
    - Administrators: eddard.stark (User), catelyn.stark (User), robb.stark (User)
    - RDP Access: Stark (Group)
- **SRV02** (castelblack.essos.local):
    - Administrators: jeor.mormont (User)
    - RDP Access: Night Watch (Group), Mormont (Group), Stark (Group)
    - IIS Configuration: Allows ASP upload and runs as NT Authority/Network
    - MSSQL:
        - Admin: jon.snow
        - Impersonation:

  - Execute as Login: samwel.tarlly -> sa
  - Execute as User: arya.stark -> dbo
- Link:
  - to braavos - jon.snow -> sa

ESSOS

- **DC03** (meereen.essos.local):
  - Administrators: daenerys.targaryen (User)
  - RDP Access: Targaryen (Group)
- **SRV03** (braavos.essos.local):
  - Administrators: khal.drogo (User)
  - RDP Access: Dothraki (Group)
  - MSSQL:
    - Admin: khal.drogo
    - Impersonation:
      - Execute as Login: jorah.mormont -> sa
    - Link:
      - to castelblack - jorah.mormont -> sa

These misconfigurations present opportunities for various attacks on computer users and group permissions. These are just a preview of the attacks and vulnerabilities present in the Red Seer Labs environment. Additionally, each user and machine have different privileges and exploits available, enabling you to explore and learn real world penetration testing techniques against an actual enterprise Active Directory environment in a controlled setting.

Red Seer Labs now includes the following additional features, vulnerabilities, and exploitation paths:

1. **Password Reuse between Computers (PTH):** Explore the impact of password reuse across multiple computers within the lab environment.
2. **User Password Spray:** Perform password spraying attacks using the common password "Password" against user accounts.
3. **Password in Description:** Investigate the security implications of passwords stored in user account descriptions.
4. **Anonymous SMB Share:** Analyze the vulnerabilities associated with anonymous access to SMB shares.

5. **SMB Signing Disabled:** Learn about the risks and consequences of SMB signing being disabled.
6. **Responder:** Understand and simulate attacks using the Responder tool for network poisoning and credential theft.
7. **Zerologon:** Explore the vulnerabilities and exploit techniques associated with the Zerologon vulnerability.
8. **Windows Defender:** Assess the effectiveness and limitations of Windows Defender as a security solution.
9. **ASREPRoast:** Exploit the ASREPRoast vulnerability to extract password hashes of service accounts.
10. **Kerberoasting:** Perform Kerberoasting attacks to extract and crack Kerberos ticket hashes.
11. **Active Directory ACL Abuse:** Investigate the impact of abusing Active Directory ACLs to gain unauthorized access.
12. **Unconstrained Delegation:** Understand the risks associated with uncontrolled or misconfigured delegation in Active Directory.
13. **NTLM Relay:** Simulate NTLM relay attacks to gain unauthorized access to targeted systems.
14. **Constrained Delegation:** Explore the configuration and vulnerabilities related to constrained delegation in Active Directory.
15. **MSSQL Installation:** Set up and configure Microsoft SQL Server (MSSQL) within the lab environment.
16. **MSSQL Trusted Link:** Utilize trusted links in MSSQL to establish connections and explore associated risks.
17. **MSSQL Impersonation:** Learn about and simulate impersonation attacks within MSSQL.
18. **IIS Installation:** Install and configure Internet Information Services (IIS) for web application testing.
19. **ASP App Upload:** Practice uploading malicious webshells and explore associated security implications.
20. **Multiple Forests:** Experience and navigate scenarios involving multiple Active Directory forests.
21. **Anonymous RPC User Listing:** Assess the risks and consequences of listing RPC users anonymously.
22. **Child Parent Domain Relationships:** Explore the relationships and potential security implications between child and parent domains.
23. **Certificate Generation and LDAPS:** Generate certificates and enable LDAPS (LDAP over SSL/TLS) for secure communication.

24. **ADCS - ESC (Enterprise Subordinate Certification Authority) 1/2/3/8:** Work with and understand the features and functionalities of ADCS Enterprise Subordinate Certification Authorities.

25. **Certifried:** Utilize Certipy tool for certificate-related operations and analysis.

26. **SamAccountName/NoPac:** Investigate the security implications and risks associated with SamAccountName/NoPac configurations.

27. **PetitPotam Unauthenticated:** Explore and understand the attack techniques and impact of the PetitPotam vulnerability.

28. **PrinterBug:** Learn about and simulate attacks leveraging the PrinterBug vulnerability.

29. **Drop the Mic:** Assess the risks and consequences of "dropping the mic" attack technique in Active Directory.

30. **Shadow Credentials:** Investigate and exploit shadow credentials left behind in the environment.

31. **MITM6:** Simulate and understand Man-in-the-Middle (MITM) attacks using the MITM6 tool.

32. **LAPS Integration:** Add and explore the functionalities of Local Administrator Password Solution (LAPS) within the lab environment.

33. **GPO Abuse:** Understand and exploit Group Policy Object (GPO) misconfigurations and abuse.

34. **WebDAV Integration:** Set up and explore the functionalities and vulnerabilities of WebDAV within the lab environment.

35. **RDP Bot:** Deploy a bot to simulate multiple RDP connections and analyze associated risks.

36. **Full Proxmox Integration:** Leverages the capabilities of Proxmox for full integration and virtualization within the lab environment.

37. **OpenVPN Access:** Lab environment is fully accessible from any remote internet connection.

38. **Command & Control:** Integration with various C2 Frameworks.

These newly added features expand the scope and opportunities for hands-on learning and exploration within the Red Seer Labs penetration testing environment.

Additional vulnerable mock enterprise and custom lab environments are currently under development and will be released soon.