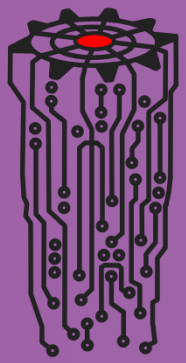


LAB OUTLINE

Description

RastaLabs is a virtual Red Team Simulation environment, designed to be attacked as a means of learning and honing your engagement skills.

The focus of the lab is operating within a Windows Active Directory environment where players must gain a foothold, elevate their privilege, be persistent and move laterally to reach the goal of Domain Admin.

There are flags to be captured along the way - some are on the attack chain, others you must go looking for and solve challenges to obtain. Submitting flags will earn you a place in the Hall of Fame and as you progress, rewarded with badges.

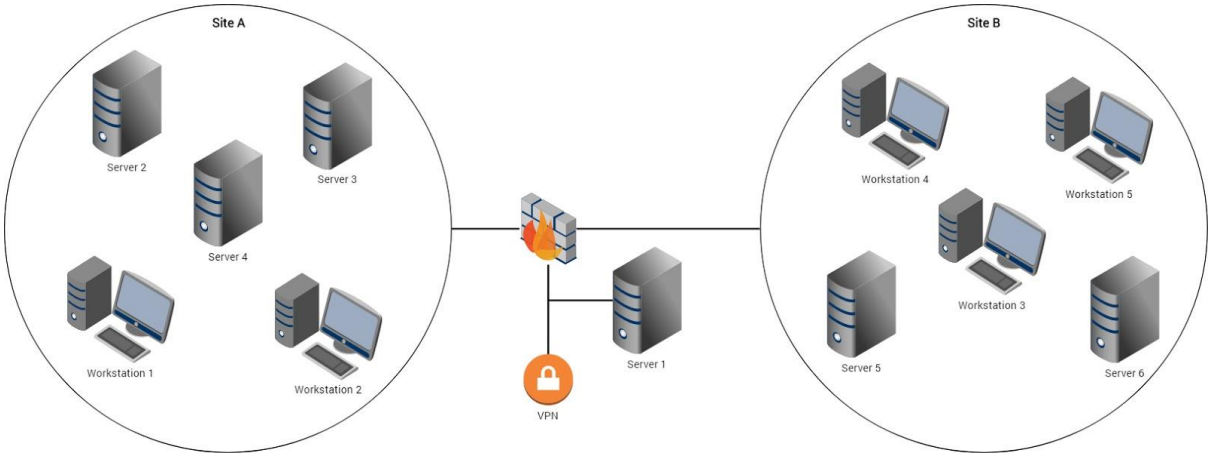
PO Box 505
TELFORD
TF2 2HS
Company No. 11131806

Design

Architecture

RastaLabs is designed to simulate a true-to-life corporate environment, based heavily on Microsoft Windows systems. Elements include Active Directory (with a Server 2016 functional domain level), Exchange, Internet Information Services, and SQL Server.

Machines are also segregated across multiple subnets.



Bleeding Edge

Only Server 2016 and Windows 10 are in use - all machines and AV are patched up to a reasonable level. You'll have a hard time winning with CVE's.

Simulated Users

As they go about their day-to-day work, employees carry out various activities whilst logged into their workstations. There are business users (such as HR) and IT users (such as Helpdesk), each with their own unique access to systems and data.

PO Box 505
TELFORD
TF2 2HS
Company No. 11131806

Target Audience

RastaLabs is not a beginner-friendly experience. However, it's an excellent opportunity, even for seasoned testers, to "level up" their knowledge in regard to operating within a Windows domain without exploitable software to rely on, and push their ability to "live off the land".

Prerequisites

Skills / Knowledge

- Familiarity of penetration testing tools and techniques
- Working knowledge of the Windows Operating System
- Decent understanding of Active Directory
- Practical PowerShell knowledge

Attitude

- Patience and perseverance
- A willingness to do extensive research
- Accept that you will fail more times than you will succeed :)

PO Box 505
TELFORD
TF2 2HS
Company No. 11131806

What Players Will Learn

Players will leave the lab having covered a range of general Red Team TTPs (Tools, Techniques, Procedures), including:

- OSINT gathering
- Phishing
- Situational awareness
- Various Active Directory weaknesses
- Password cracking
- Credential theft
- Token impersonation & pass-the-hash
- Lateral movement & pivoting

PO Box 505
TELFORD
TF2 2HS
Company No. 11131806

The Game

To help players immerse themselves in the lab, the following narrative is available.

Narrative

Established in 2017, RastaLabs is a leading provider of IT security and penetration testing services. Our consultants offer expertise, flexibility and extensive support before, during and after each engagement. RastaLabs is an ISO 27001 & 9001 certified organisation, committed to providing an unparalleled service in the Information Security industry.

You have been engaged to conduct a security assessment against the organisation, under the following rules of engagement.

In Scope

Players will start in the RastaLabs DMZ network: 10.10.110.0/24. Your goal is to gain Domain Admin access to their core infrastructure in rastalabs.local.

Out of Scope

Any network or system outside of the RastaLabs environment.

Note: it is not required that you "friend" or "connect" with any of the RastaLabs staff on social media platforms.

Restrictions

- Limit aggressive scanning with Vulnerability Scanning tools
- Denial of service

PO Box 505
TELFORD
TF2 2HS
Company No. 11131806

Need Support?

Ticket

Raise a Support Ticket at:

https://hackthebox.atlassian.net/servicedesk/customer/portal/1

Forum

Visit the RastaLabs Forum at:

https://forum.hackthebox.eu/categories/rastalabs

Slack

Join the #rastalabs channel in NetSecFocus by typing:

!join #rastalabs @<your username>

A NetSecFocus invite can be found here: https://netsecfocus.herokuapp.com

Please don't post spoilers in pubic :)