HTB Sauna - Red Team Report with Explanations & Mitigations

1. Lab Overview

Machine: Sauna

IP: 10.10.10.175

Domain: EGOTISTICAL-BANK.LOCAL

OS: Windows 10 / Server 2019 Build 17763 x64

This lab simulates an internal Windows AD environment where the objective is to escalate from a domain user to Domain Admin using common AD abuse techniques.

2. Reconnaissance & Initial Enum

Nmap revealed a range of ports typically found on AD environments: Kerberos (88), LDAP (389), WinRM (5985), HTTP (80), etc.

IIS 10.0 was running on port 80 with a homepage for Egotistical Bank. No null sessions were allowed, and rpcclient failed.

LDAP anonymous bind, however, succeeded and provided some information about users and AD structure.

3. Username Harvesting from Website

From the Team section of the website, we enumerated a list of potential usernames. These were used for Kerberos-based attacks.

4. AS-REP Roasting & Password Cracking

Using kerbrute, we found that user 'fsmith' had pre-authentication disabled, allowing AS-REP roasting.

Captured the hash and cracked it with john -> Password: Thestrokes23.

Mitigation: Ensure all accounts have Kerberos pre-authentication enabled.

5. Initial Access via Evil-WinRM

Used Evil-WinRM to authenticate as fsmith. Captured user.txt and began post-exploitation enumeration.

No interesting privileges, but additional user accounts were identified.

HTB Sauna - Red Team Report with Explanations & Mitigations

6. BloodHound Recon & Kerberoasting

Ran BloodHound to map attack paths. Found two kerberoastable users: hsmith and krbtgt.

Extracted SPNs and cracked hsmith's password: reused same password (Thestrokes23).

Mitigation: Enforce strong, unique passwords and regularly rotate service account credentials.

7. SVC Account Discovery via AutoLogon

Found stored autologon credentials in registry for svc_loanmanager: Moneymakestheworldgoround!

This user had elevated domain privileges including replication rights.

8. DCSync Attack for Domain Admin

With svc_loanmanager's privileges, executed DCSync using secretsdump.py to retrieve NTLM hashes from the Domain Controller.

This included the Administrator hash.

Mitigation: Limit replication permissions strictly, especially for service accounts.

9. Final Exploitation and Root Access

Used PSExec with the Administrator hash to get a SYSTEM shell.

Captured root.txt and confirmed Domain Admin access.

10. Final Notes & Mitigations

Summary of key mitigations:

- Disable AS-REP roasting by enforcing pre-auth on all users
- Regularly rotate and audit service account passwords
- Restrict replication permissions to DCs only
- Use LSASS protection to prevent credential theft
- Monitor for BloodHound-related behaviors and SPN enumeration