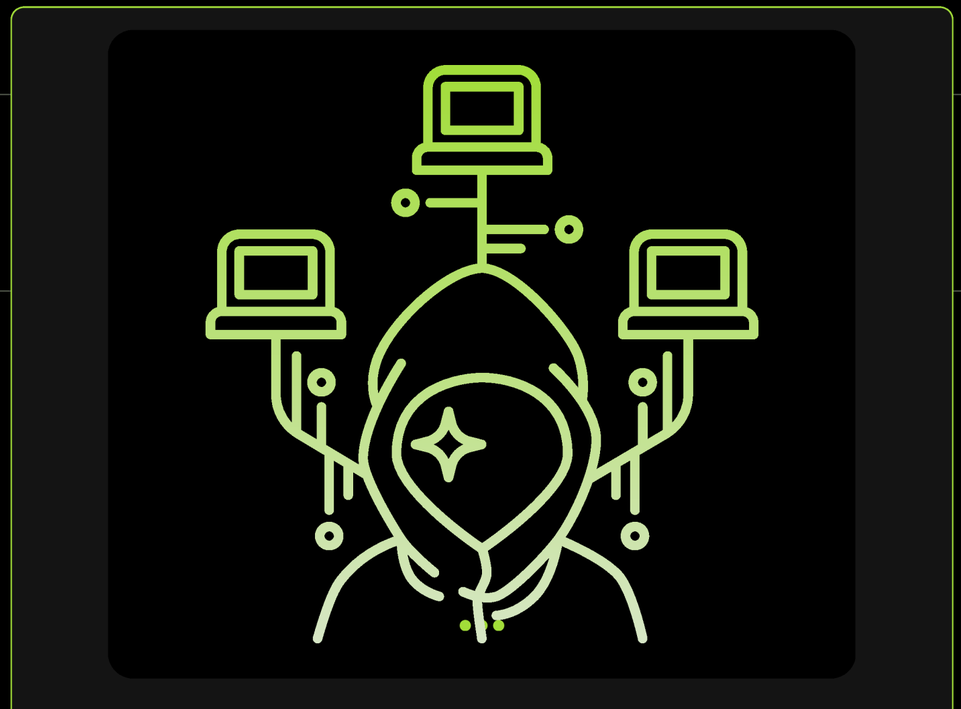
Evan Hosinski
KrakenTech LLC

10.03.2025

HOW RED TEAM EFFORTS CAN FUEL BLUE TEAM CAPABILITIES

CRACK. TRACK. REACT.



Evan Hosinski
KrakenTech LLC

10.03.2025

GCON> WHOAMI

Evan Hosinski
KrakenTech LLC

10.03.2025

WHO IS THIS NERD

Actual Quote

Everyone: “Just use Impacket”

Me: “No thanks, I’ll just rewrite DCERPC/SMB in Go”

Fun Facts About Me

- 6 Years of telling companies their passwords suck
- Have more tools built than friends
- Still not blacklisted from my talk last year at GrrCon
- PostgreSQL was too slow for me
- I forked and fixed GoCat because it existed
- I’m not paranoid you’re paranoid
- Haven’t touched grass in weeks
- No wheel is round enough
- If Microsoft invented it I’ve probably already rage ported it in Go

But Why

Some people like 0-days I like rpc null binds

Evan Hosinski
KrakenTech LLC

10.03.2025

AS A PASSION

HASH CRACKING

Evan Hosinski
KrakenTech LLC

10.03.2025

THE PROBLEM

Evan Hosinski
KrakenTech LLC

10.03.2025

UNDERSTANDING

THE PROBLEM

Threat Actors

Recent Breaches

07-19-2019	**Citrix**	**Password Spray**
05-07-2021	**Colonial Pipeline**	**Password Reuse**
10-12-2023	23andMe	Credential Stuffing
01-12-2024	Microsoft	Password Spray
06-?-2024	Ticketmaster, Santander, AT&T	Credential Stuffing

APT Groups

- APT33 (Iran)
- APT34 (Iran)
- APT28 (Russia, GRU)
- APT29 (Russia, SVR)
- APT35 (Iran)
- APT40 (China)
- Nobelium (Russia, SVR)

Evan Hosinski
KrakenTech LLC

10.03.2025

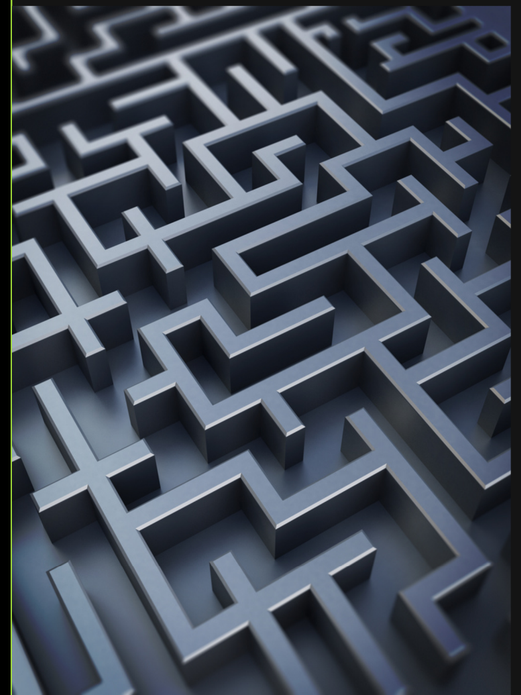
UNDERSTANDING

THE PROBLEM

Passwords

Possible Problems

- Weak password policy
- Complex but compromised
- Password reuse
  - Local
  - Active Directory
- Permutations of compromised credentials
- Company details used in credentials



MSDN Password Complexity

- May not contain samAccontName
- Contains characters from:
  - Uppercase
  - Lowercase
  - Base 10 digits (0-9)
  - Non-alphanumeric Characters

Evan Hosinski
KrakenTech LLC

10.03.2025

PASSWORDS

EXISTING TOOLS

Evan Hosinski
KrakenTech LLC

10.03.2025

DETECTING PASSWORD ISSUES

Getting the Data

- Local
  - hashes live in the SAM Hive
  - Protected by key in SYSTEM Hive
- Active Directory
  - Live in NTDS.dit on DC's
- Can be extracted and decrpyted with admin privileges

Using the Data

- Hash Cracking
  - Weak or Predictable
- Raw hashes
    - Password Reuse
    - Reuse Patterns
      - Accounts
      - Systems
- Both
  - Identify High-Risk Credential Configurations
  - Determine risk and mitigate blast radius

Creating a Process

- Only a single point-in-time view
- Active Directory environments are constantly changing
  - New Users
  - Service Accounts
  - Group Membership Shifts
- Without monitoring, weaknesses can creep back in

Evan Hosinski
KrakenTech LLC

PASS-POL

10.03.2025

Attribute	Description	Vulnerability
Machine Account Quota	Permit any authenticated user create up to N computer accounts (Default 10)	Non-admin users can create computer accounts, enabling attck paths such as RBCD
Reversible Encryption	Stores passwords with reversible encryption (decryptable) to support legacy protocols	Any compromise of systems or accounts that can read those attributes produces direct password disclosure
Complexity Requirement	Enforce Micorosft Defined Password Complexity	Low entropy passwords are vulnerable to guessing, dictionary attacks, offline cracking and high-scess-rate password spray campaigns
Min. Password Length	Minimum number of characters required.	Short minimum lengths reduce entropy, making passwords vulnerable to guessing, dictionary attacks, offline cracking, and high-success-rate password-spray campaigns
Lockout Counter	Number of failed sign-ins before an account is locked	Too permissive → brute-force/spray success; too strict → easy DoS
Timeout Observation	How long the account stays locked	Poorly chosen timers undermine the lockout mechanism: short counters let attackers brute at scale with low friction
Lockout Reset	Number of minutes before the failed-attempt counter resets to 0	Poorly chosen timers undermine the lockout mechanism: short counters let attackers brute at scale with low friction

Evan Hosinski
KrakenTech LLC

10.03.2025

UNAUTHENTICATED ATTACKS

Evan Hosinski
KrakenTech LLC

10.03.2025

AUTHENTICATED

ATTACKS

Evan Hosinski
KrakenTech LLC

10.03.2025

UNDERSTANDING

THE PROBLEM

Remediation

Post-Op Paralysis

The stage after a pentest where organizations receive actionable findings but lack the people, processes, or prioritization to convert those findings into timely, measurable remediation

---

- Lack of Tools
- Unclear Prioritiziation
- Lack of Understanding
- More than one right answer

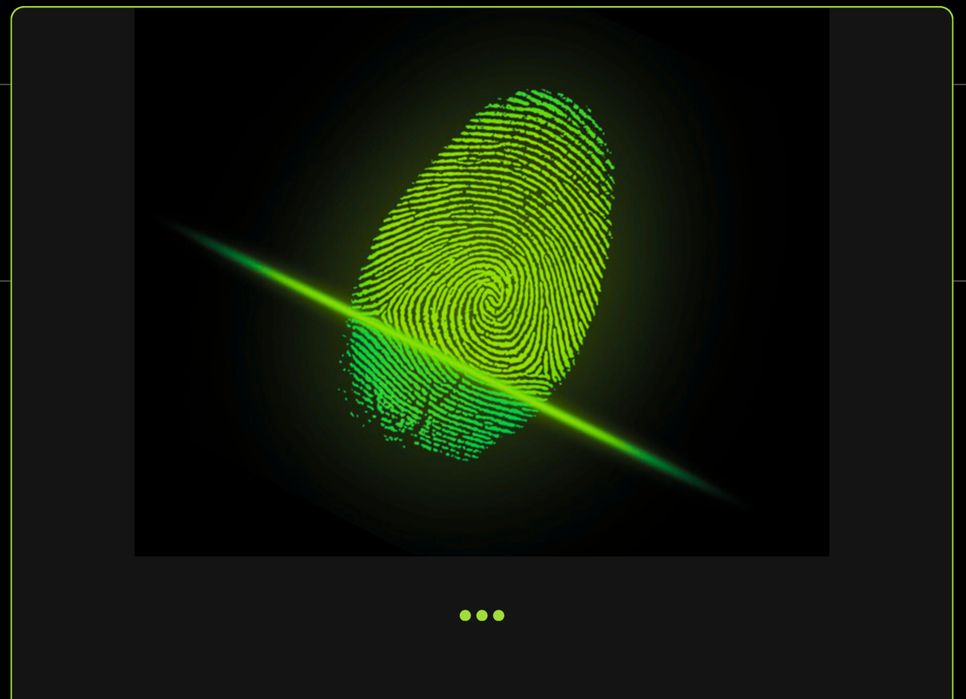
Verification

- Unfit Tooling
- Potential to break things in environment

Evan Hosinski
KrakenTech LLC

10.03.2025

THE VISION



Evan Hosinski
KrakenTech LLC

10.03.2025

TOOLS

Evan Hosinski
KrakenTech LLC

10.03.2025

VAULTY

Vaulty

KEY-VALUE DATABASE

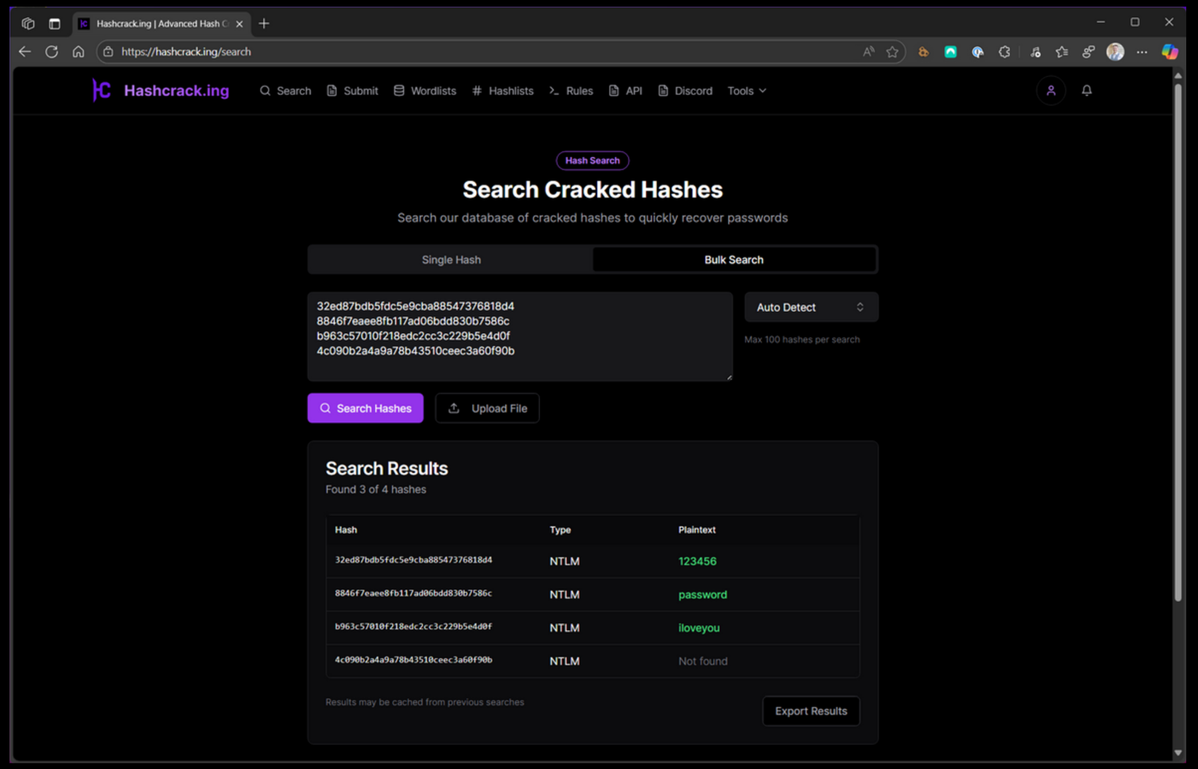
Evan Hosinski
KrakenTech LLC

10.03.2025

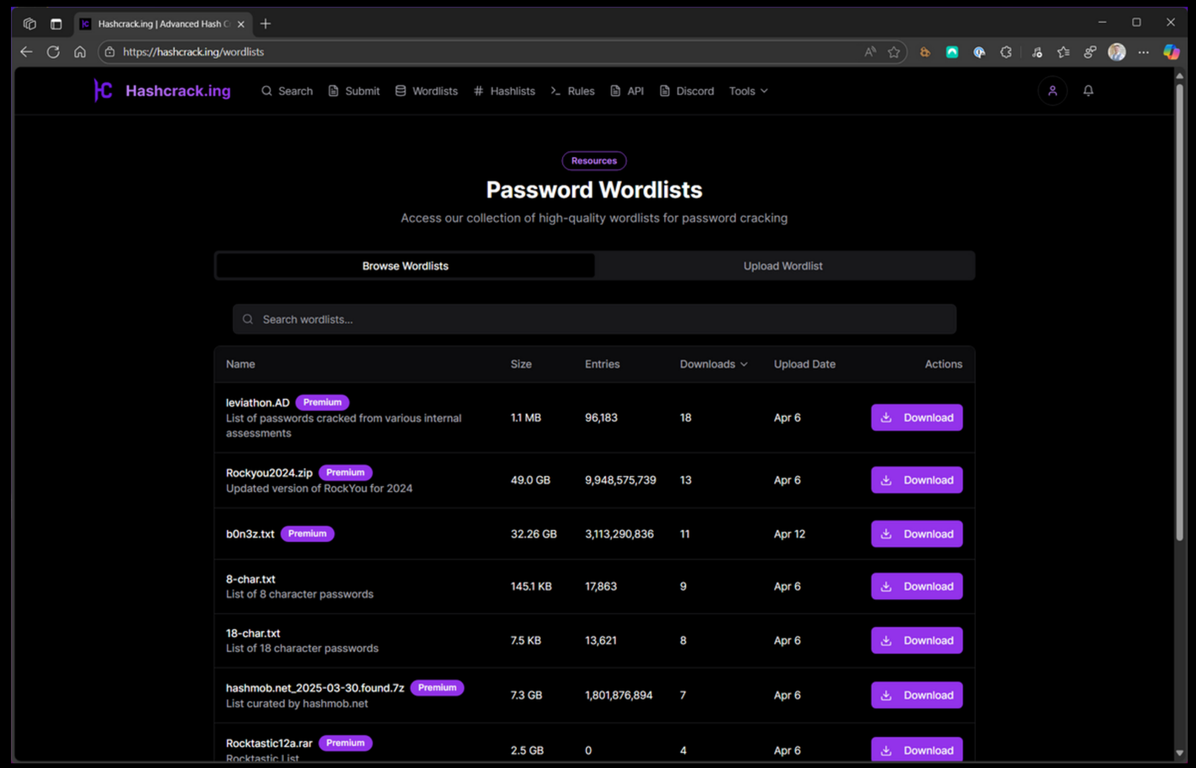
HASHCRACK.ING

HashCrack.ing

QUERIES



LISTS



Evan Hosinski
KrakenTech LLC

10.03.2025

KCAT

```
TION [16] Generated bitmap tables
SK INFO -> {29 29 1}
TION [161] Initializing device kernels and memory
TION [160] Initialized device kernels and memory
TION [1] Starting Autotune threads
TION [0] Autotune threads have started..
TION [240] Approaching final keyspace, workload adjusted
NAL STATUS -> &{hashcat Exhausted NTLM /root/.local/share/bounty/temp/GXKYEwHKDf.txt Tue Sep  9 19:55:51
ecutor adding results
ecutor adding cracked hash:  c22b315c040ae6e0efee3518d830362b  password:  123456789
ecutor adding cracked hash:  259745cb123a52aa2e693aaacca2db52  password:  12345678
ecutor adding cracked hash:  e16fda02030a134736ed66c155987b40  password:  footballV
ecutor adding cracked hash:  dff1dbd0d5695f1b2c8a3536a7ed3771  password:  h3ll0!
ecutor adding cracked hash:  cff972e0f6c705ad125d11cafde83d85  password:  f00tb@ll
ecutor adding cracked hash:  31fc0dc8f7dfad0e8bd7ccc3842f2ce9  password:  football
ecutor adding cracked hash:  8846f7eaee8fb117ad06bdd830b7586c  password:  password
ecutor adding cracked hash:  49b3ff5a96dc5b8cbf6406e533fdbc18  password:  iloveyou5I
ecutor adding cracked hash:  b963c57010f218edc2cc3c229b5e4d0f  password:  iloveyou
ecutor adding cracked hash:  31c72c210ecc03d1eae94fa496069448  password:  sunshine
ecutor adding cracked hash:  e10aaa254a72012bc80a289f2d8d5c4e  password:  Team123!
ecutor adding cracked hash:  fb4bf3ddf37cf6494a9905541290cf51  password:  princess
rforming attack: ?a?a
ecutor writing uncracked ntlm hashes to file
ecutor getting uncracked ntlm hashes
ecutor getting cracked hashes
ecutor got cracked hashes with 272 entries
ecutor got uncracked ntlm hashes with 18 entries
ecutablePath: /opt/hashcat
_LIBRARY_PATH: /usr/local/cuda-13.0/compat:
TION [86] Sorting salts...
TION [85] Sorted salts...
TION [17] Generating bitmap tables
TION [16] Generated bitmap tables
SK INFO -> {17 17 1}
TION [161] Initializing device kernels and memory
TION [160] Initialized device kernels and memory
TION [1] Starting Autotune threads
TION [0] Autotune threads have started..
TION [240] Approaching final keyspace, workload adjusted
NAL STATUS -> &{hashcat Exhausted NTLM /root/.local/share/bounty/temp/omwkAM3iFO.txt Tue Sep  9 19:55:57
ecutor adding results
ecutor adding cracked hash:  c75489b8e03046f743c1cc030df8be6a  password:  pr1nc3$$
ecutor adding cracked hash:  10e6b4a8fe7c3a9850d9077cda333e51  password:  hellofno
ecutor adding cracked hash:  3d59ec952f99fbcb0eb18d7a92dc40fb  password:  adminfL
rforming attack: ?a?a?a
ecutor writing uncracked ntlm hashes to file
ecutor getting uncracked ntlm hashes
ecutor getting cracked hashes
ecutor got cracked hashes with 275 entries
ecutor got uncracked ntlm hashes with 15 entries
ecutablePath: /opt/hashcat
_LIBRARY_PATH: /usr/local/cuda-13.0/compat:
```

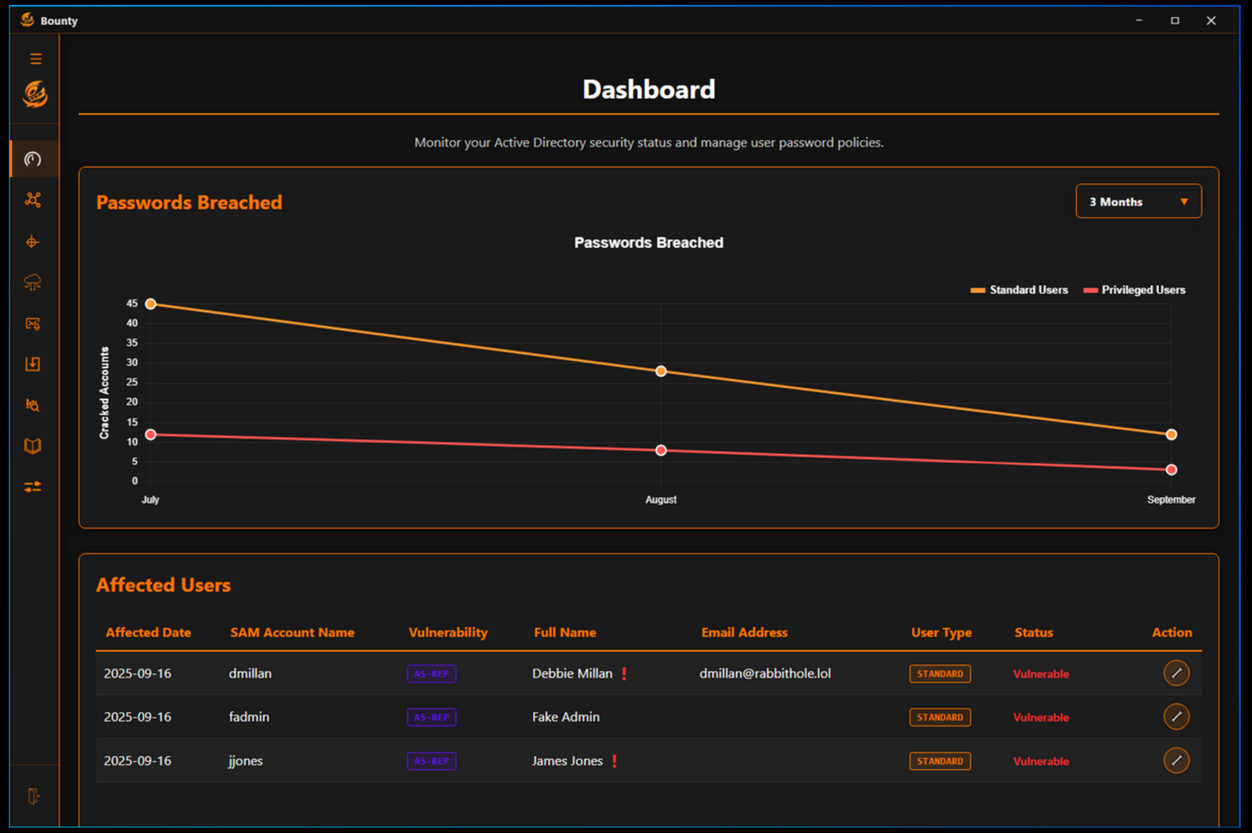
```
Cracking NTLM Hashes
Performing increment attack
Writing uncracked NTLM Hashes to file: /root/.local/share/bounty/temp/o2uV9Yrwe3.txt
Executor writing uncracked ntlm hashes to file
Executor getting uncracked ntlm hashes
Executor getting cracked hashes
Executor got cracked hashes with 244 entries
Executor got uncracked ntlm hashes with 46 entries
ExecutablePath: /opt/hashcat
LD_LIBRARY_PATH: /usr/local/cuda-13.0/compat:
ACTION [86] Sorting salts...
ACTION [85] Sorted salts...
ACTION [17] Generating bitmap tables
ACTION [16] Generated bitmap tables
TASK INFO -> {45 45 1}
ACTION [161] Initializing device kernels and memory
ACTION [160] Initialized device kernels and memory
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
ACTION [1] Starting Autotune threads
ACTION [0] Autotune threads have started..
ACTION [240] Approaching final keyspace, workload adjusted
FINAL STATUS -> &{hashcat Exhausted NTLM /root/.local/share/bounty/temp/o2uV9Yrwe3.txt Tue Sep  9 19:49:27 2025
Executor adding results
Executor adding cracked hash:  066ddfd4ef0e9cd7c256fe77191ef43c  password:  hello
Executor adding cracked hash:  2330f2ff9fbdf5b962fcb26ae337974a  password:  dr4g0n
Executor adding cracked hash:  6d9a5acc174877e1cdd45147af1de804  password:  w3lc0me
Executor adding cracked hash:  2d20d252a479f485cdf5e171d93985bf  password:  qwerty
Executor adding cracked hash:  f9e37e83b83c47a93c2f09f66408631b  password:  abc123
Executor adding cracked hash:  32ed87bdb5fdc5e9cba88547376818d4  password:  123456
Executor adding cracked hash:  0c12cc2b593eb9ab466a79a907cbac73  password:  m0nk3y
Executor adding cracked hash:  f7eb9c06fafaa23c4bcf22ba6781c1e2  password:  dragon
Executor adding cracked hash:  f2477a144dff4f216ab81f2ac3e3207d  password:  monkey
Executor adding cracked hash:  328727b81ca05805a68ef26acb252039  password:  1234567
Executor adding cracked hash:  7a21990fcd3d759941e45c490f143d5f  password:  12345
Executor adding cracked hash:  209c6174da490caeb422f3fa5a7ae634  password:  admin
```

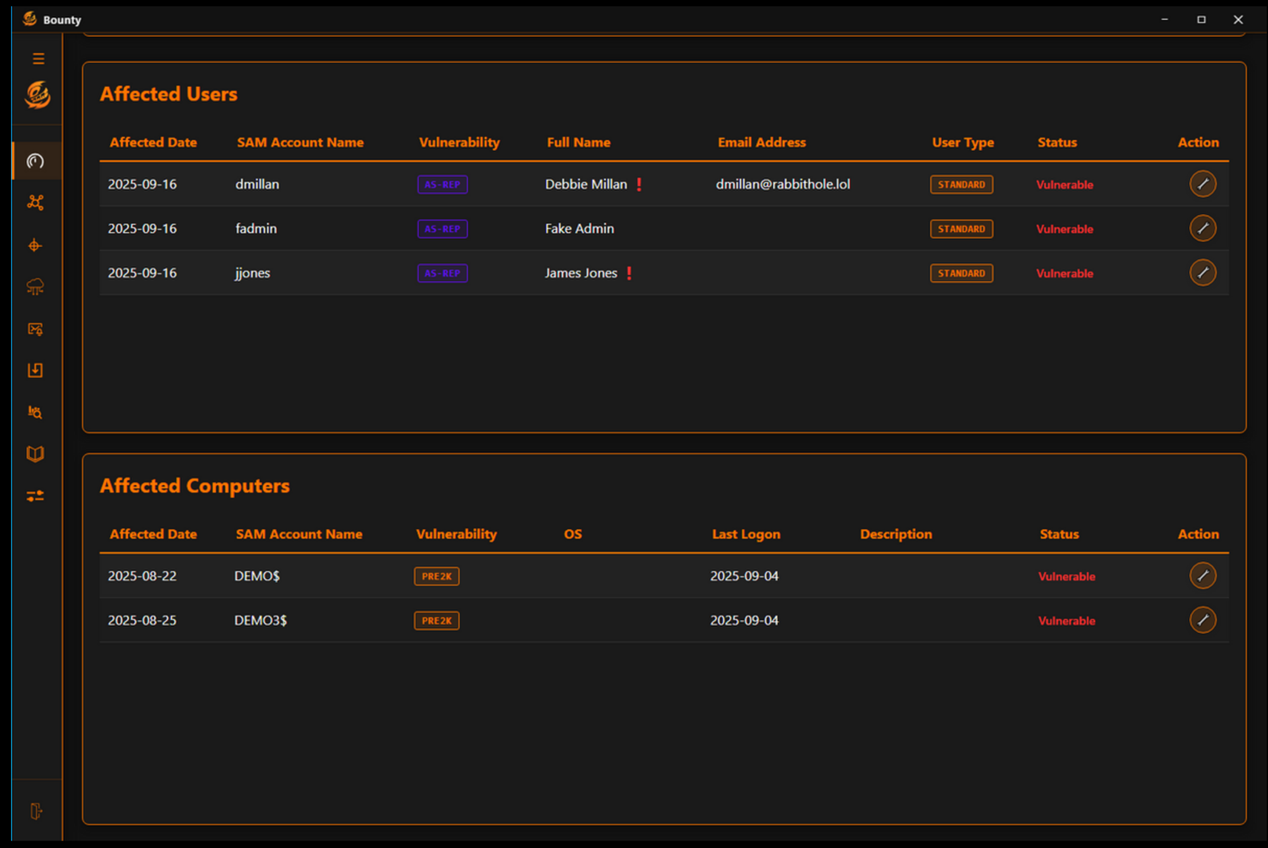
Evan Hosinski
KrakenTech LLC

10.03.2025

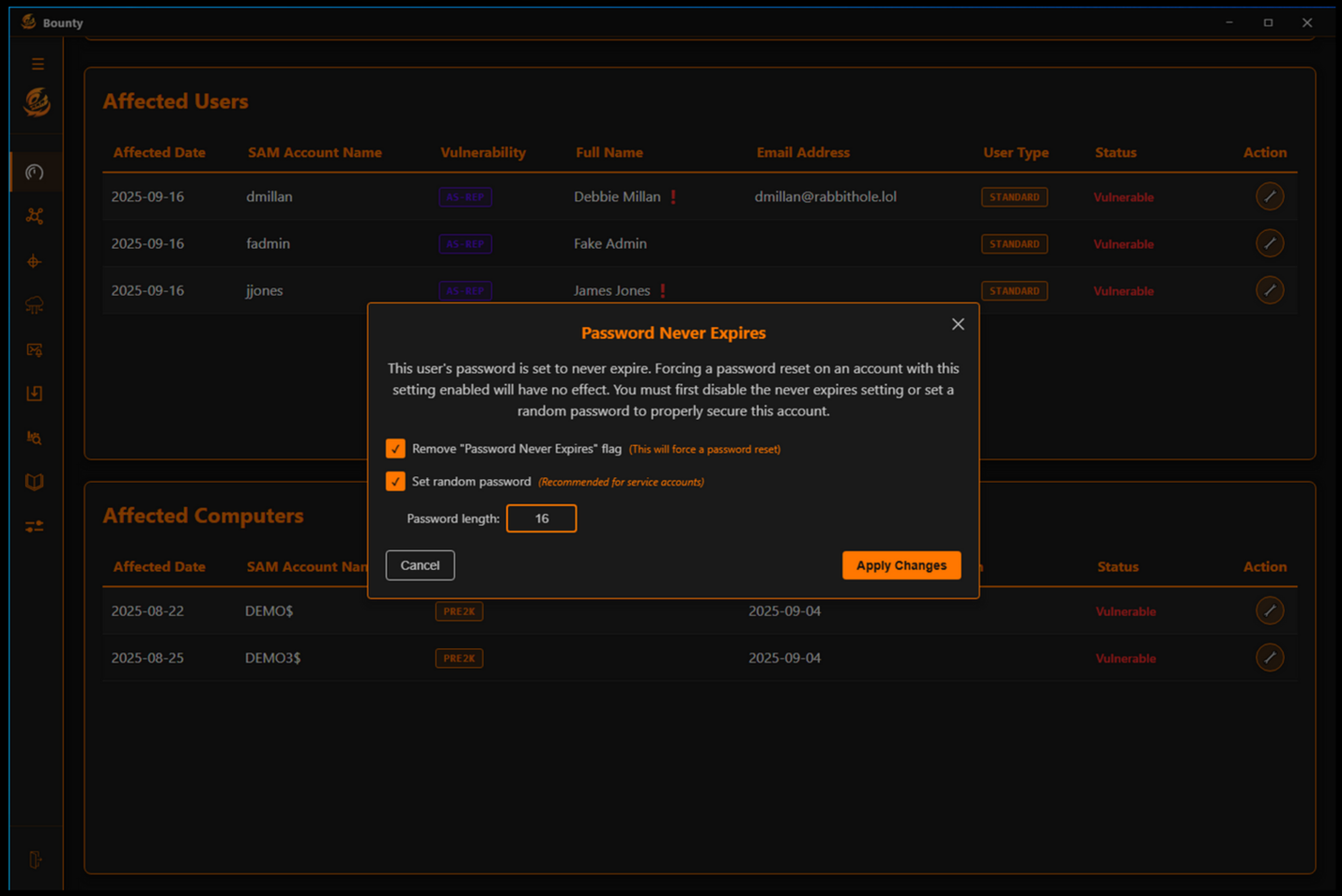
BOUNTY

DASHBOARD

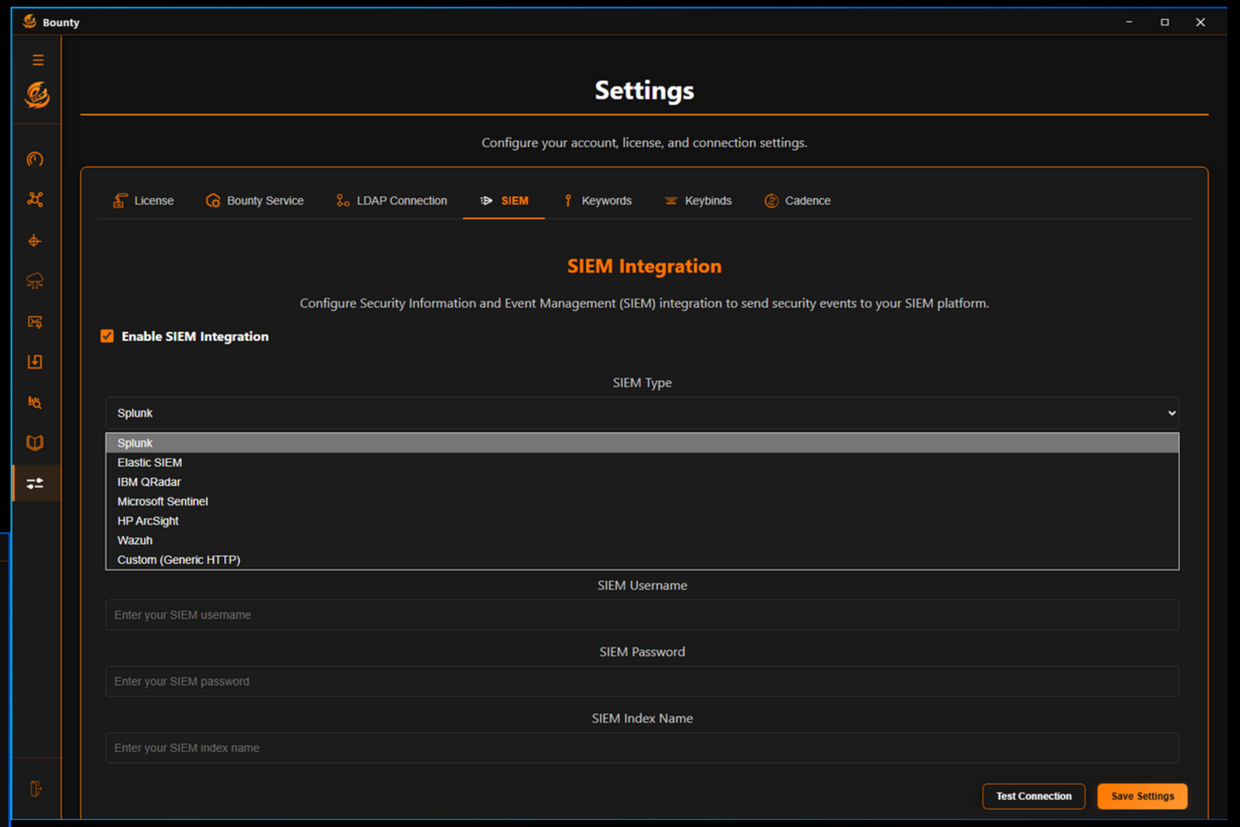

Bounty
Dashboard
Monitor your Active Directory security status and manage user password policies.
Passwords Breached
3 Months
Passwords Breached
Standard Users
Privileged Users
Cracked Accounts
45
40
35
30
25
20
15
10
5
0
July
August
September
Affected Users
Affected Date
SAM Account Name
Vulnerability
Full Name
Email Address
User Type
Status
Action
2025-09-16
dmillan
AS-REP
Debbie Millan
dmillan@rabbithole.lol
STANDARD
Vulnerable
2025-09-16
fadmin
AS-REP
Fake Admin
STANDARD
Vulnerable
2025-09-16
jjones
AS-REP
James Jones
STANDARD
Vulnerable

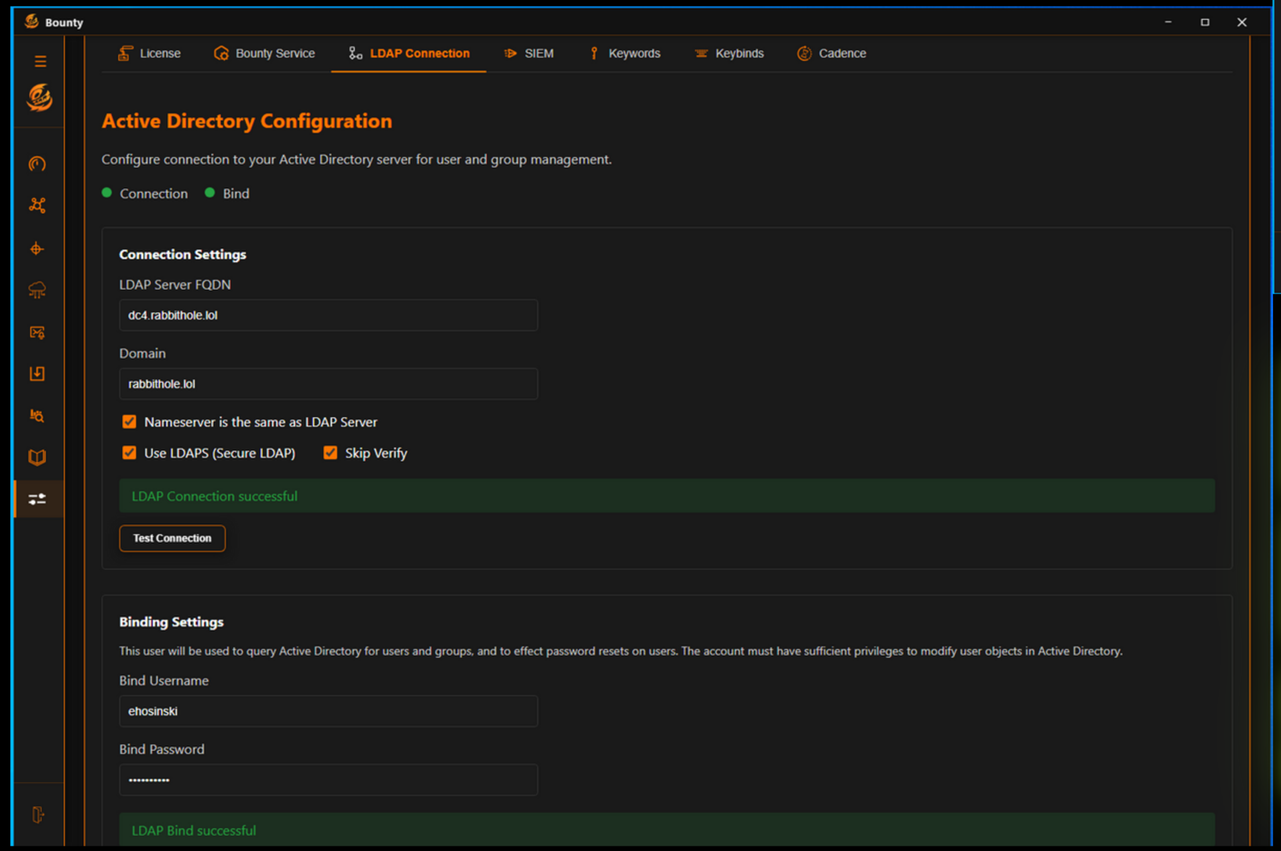

Bounty
Affected Users
Affected Date
SAM Account Name
Vulnerability
Full Name
Email Address
User Type
Status
Action
2025-09-16
dmillan
AS-REP
Debbie Millan
dmillan@rabbithole.lol
STANDARD
Vulnerable
2025-09-16
fadmin
AS-REP
Fake Admin
STANDARD
Vulnerable
2025-09-16
jjones
AS-REP
James Jones
STANDARD
Vulnerable
Affected Computers
Affected Date
SAM Account Name
Vulnerability
OS
Last Logon
Description
Status
Action
2025-08-22
DEMO$
PRE2K
2025-09-04
Vulnerable
2025-08-25
DEMO3$
PRE2K
2025-09-04
Vulnerable

NO EXPIRY


Bounty
Affected Users
Affected Date
SAM Account Name
Vulnerability
Full Name
Email Address
User Type
Status
Action
2025-09-16
dmillan
AS-REP
Debbie Millan
dmillan@rabbithole.lol
STANDARD
Vulnerable
2025-09-16
fadmin
AS-REP
Fake Admin
STANDARD
Vulnerable
2025-09-16
jjones
AS-REP
James Jones
STANDARD
Vulnerable
Password Never Expires
This user's password is set to never expire. Forcing a password reset on an account with this setting enabled will have no effect. You must first disable the never expires setting or set a random password to properly secure this account.
Remove "Password Never Expires" flag (This will force a password reset)
Set random password (Recommended for service accounts)
Password length:
16
Cancel
Apply Changes
Affected Computers
Affected Date
SAM Account Nam
Status
Action
2025-08-22
DEMO$
PRE2K
2025-09-04
Vulnerable
2025-08-25
DEMO3$
PRE2K
2025-09-04
Vulnerable

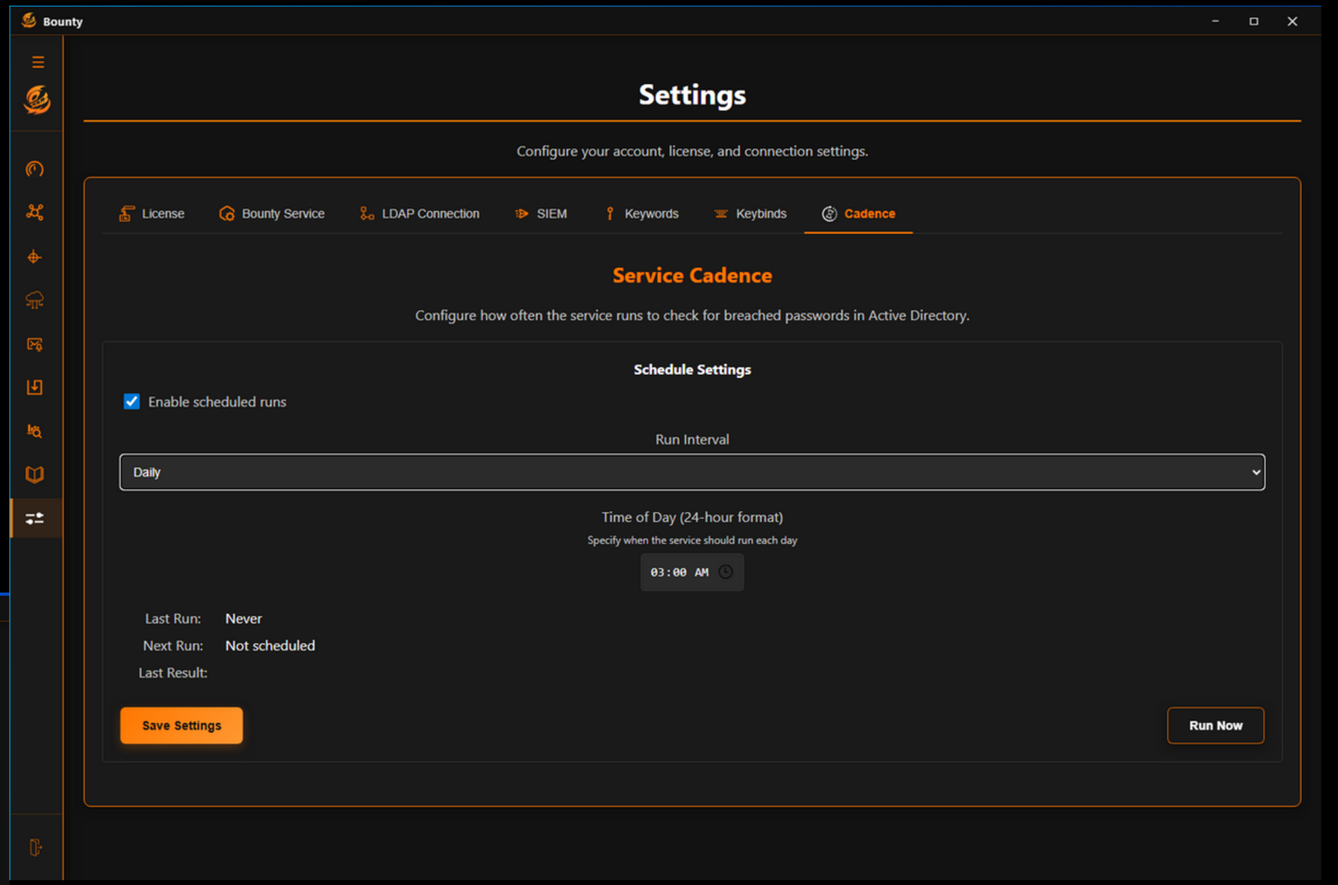
SIEM INTEGRATION

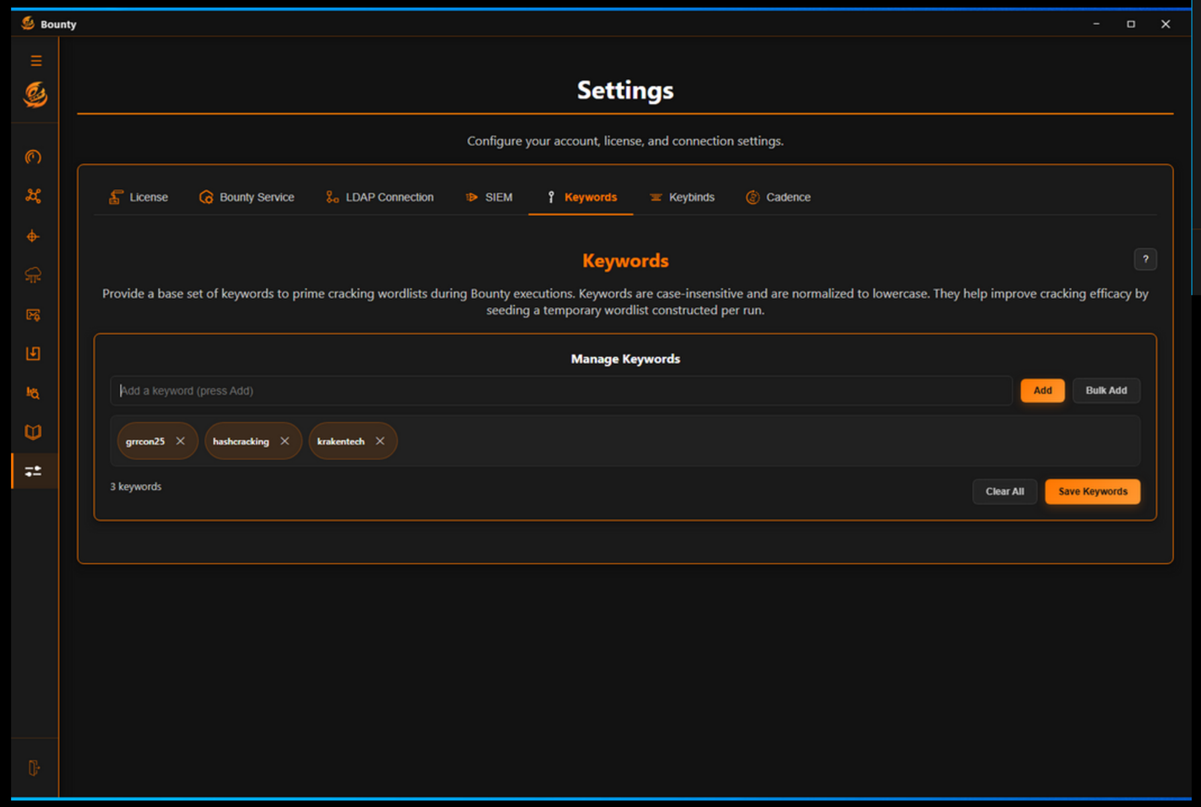




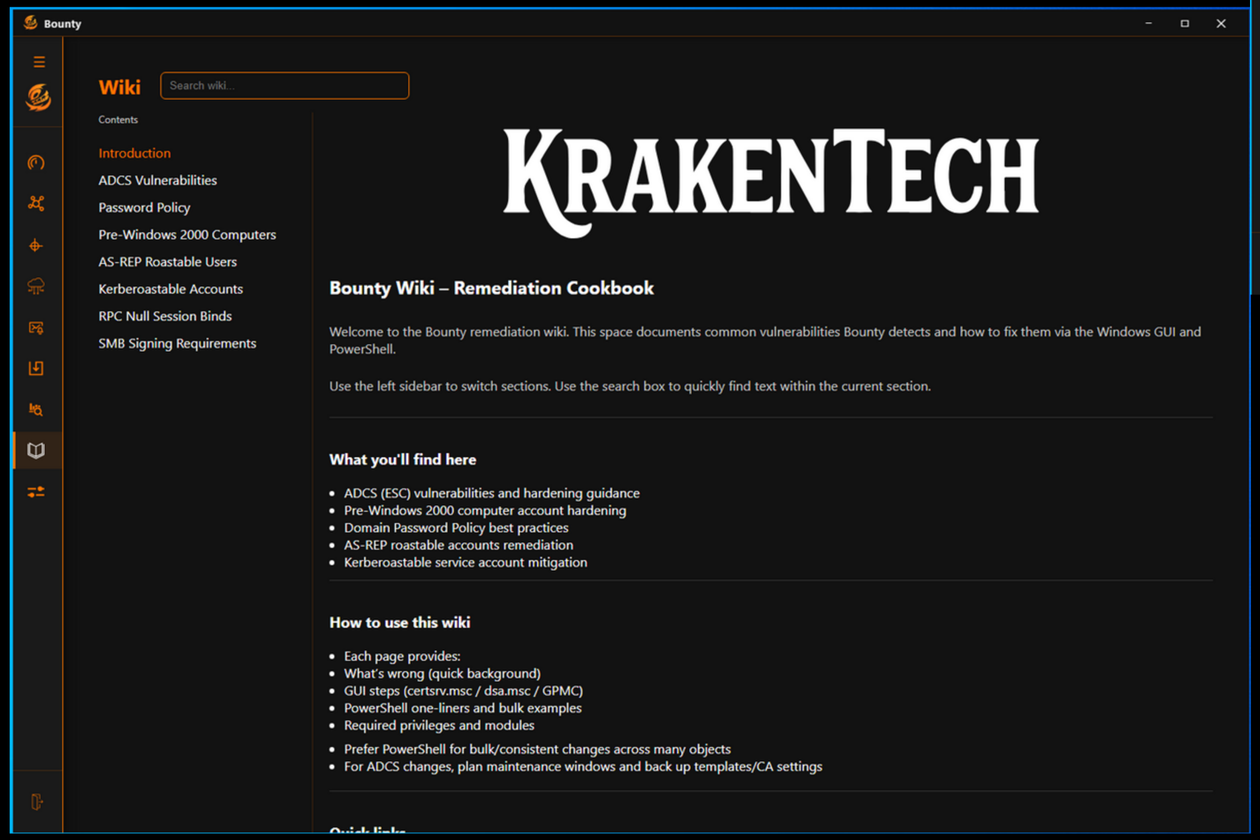
LDAP CONNECTION & BIND

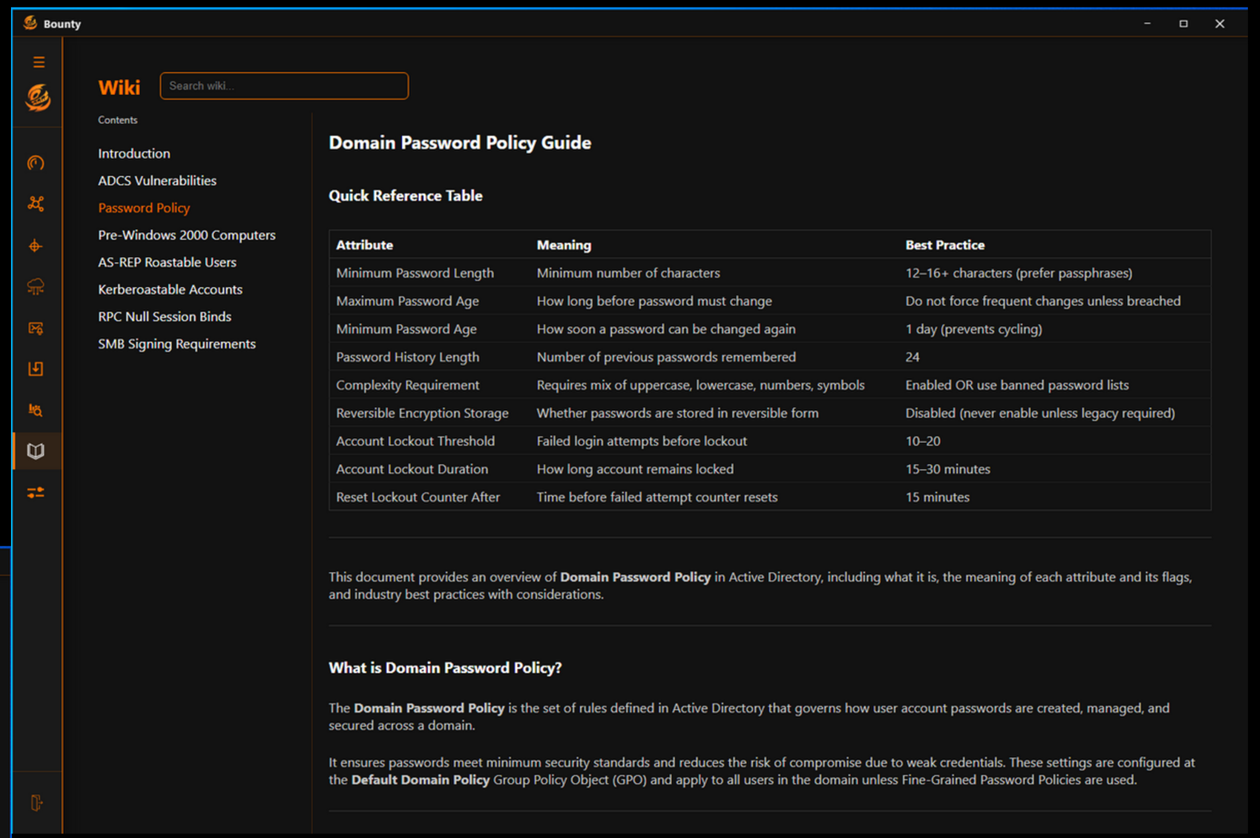
CADENCE





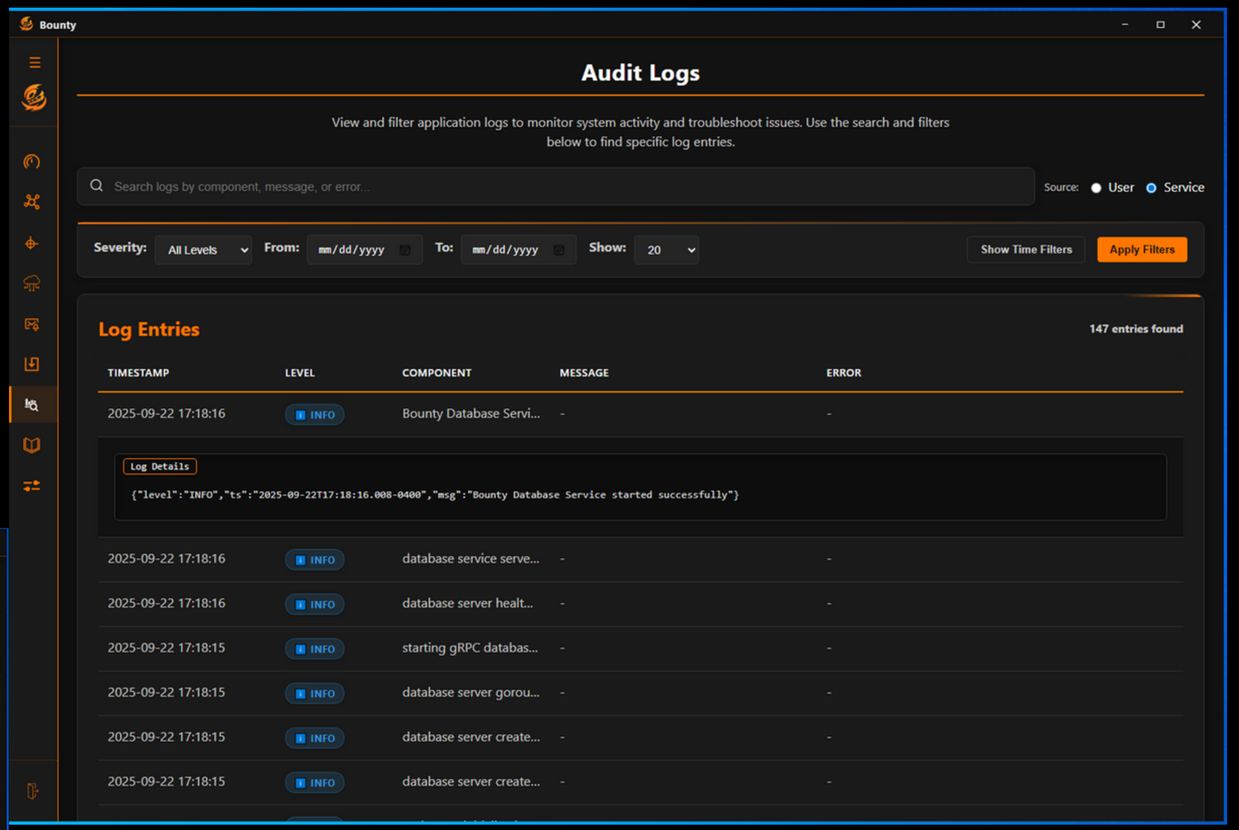
KEYWORDS

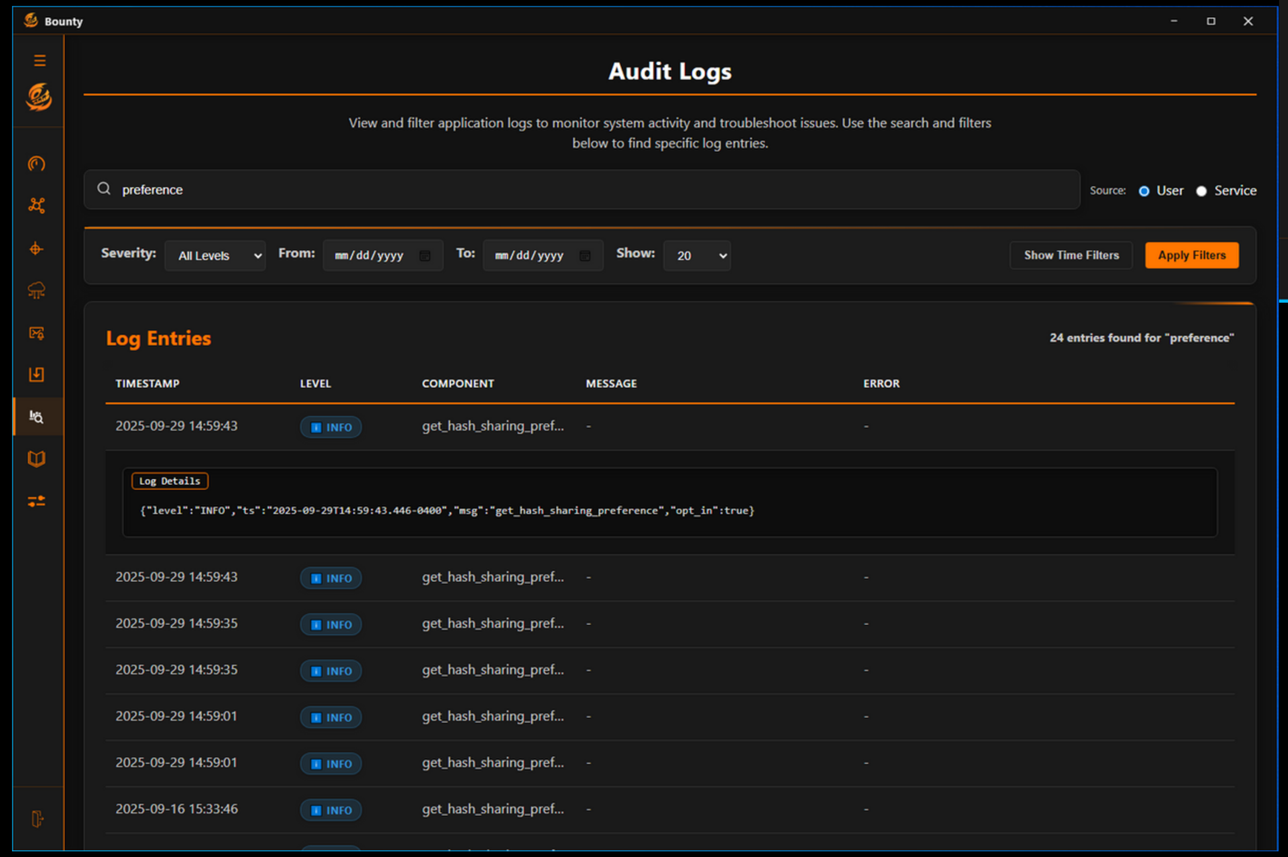

Bounty
Wiki
Search wiki...
Contents
Introduction
ADCS Vulnerabilities
Password Policy
Pre-Windows 2000 Computers
AS-REP Roastable Users
Kerberoastable Accounts
RPC Null Session Binds
SMB Signing Requirements
KRAKENTECH
Bounty Wiki – Remediation Cookbook
Welcome to the Bounty remediation wiki. This space documents common vulnerabilities Bounty detects and how to fix them via the Windows GUI and PowerShell.
Use the left sidebar to switch sections. Use the search box to quickly find text within the current section.
What you'll find here
ADCS (ESC) vulnerabilities and hardening guidance
Pre-Windows 2000 computer account hardening
Domain Password Policy best practices
AS-REP roastable accounts remediation
Kerberoastable service account mitigation
How to use this wiki
Each page provides:
What's wrong (quick background)
GUI steps (certsrv.msc / dsa.msc / GPMC)
PowerShell one-liners and bulk examples
Required privileges and modules
Prefer PowerShell for bulk/consistent changes across many objects
For ADCS changes, plan maintenance windows and back up templates/CA settings


Bounty
Wiki
Search wiki...
Contents
Introduction
ADCS Vulnerabilities
Password Policy
Pre-Windows 2000 Computers
AS-REP Roastable Users
Kerberoastable Accounts
RPC Null Session Binds
SMB Signing Requirements
Domain Password Policy Guide
Quick Reference Table
Attribute
Meaning
Best Practice
Minimum Password Length
Minimum number of characters
12–16+ characters (prefer passphrases)
Maximum Password Age
How long before password must change
Do not force frequent changes unless breached
Minimum Password Age
How soon a password can be changed again
1 day (prevents cycling)
Password History Length
Number of previous passwords remembered
24
Complexity Requirement
Requires mix of uppercase, lowercase, numbers, symbols
Enabled OR use banned password lists
Reversible Encryption Storage
Whether passwords are stored in reversible form
Disabled (never enable unless legacy required)
Account Lockout Threshold
Failed login attempts before lockout
10–20
Account Lockout Duration
How long account remains locked
15–30 minutes
Reset Lockout Counter After
Time before failed attempt counter resets
15 minutes
This document provides an overview of Domain Password Policy in Active Directory, including what it is, the meaning of each attribute and its flags, and industry best practices with considerations.
What is Domain Password Policy?
The Domain Password Policy is the set of rules defined in Active Directory that governs how user account passwords are created, managed, and secured across a domain.
It ensures passwords meet minimum security standards and reduces the risk of compromise due to weak credentials. These settings are configured at the Default Domain Policy Group Policy Object (GPO) and apply to all users in the domain unless Fine-Grained Password Policies are used.

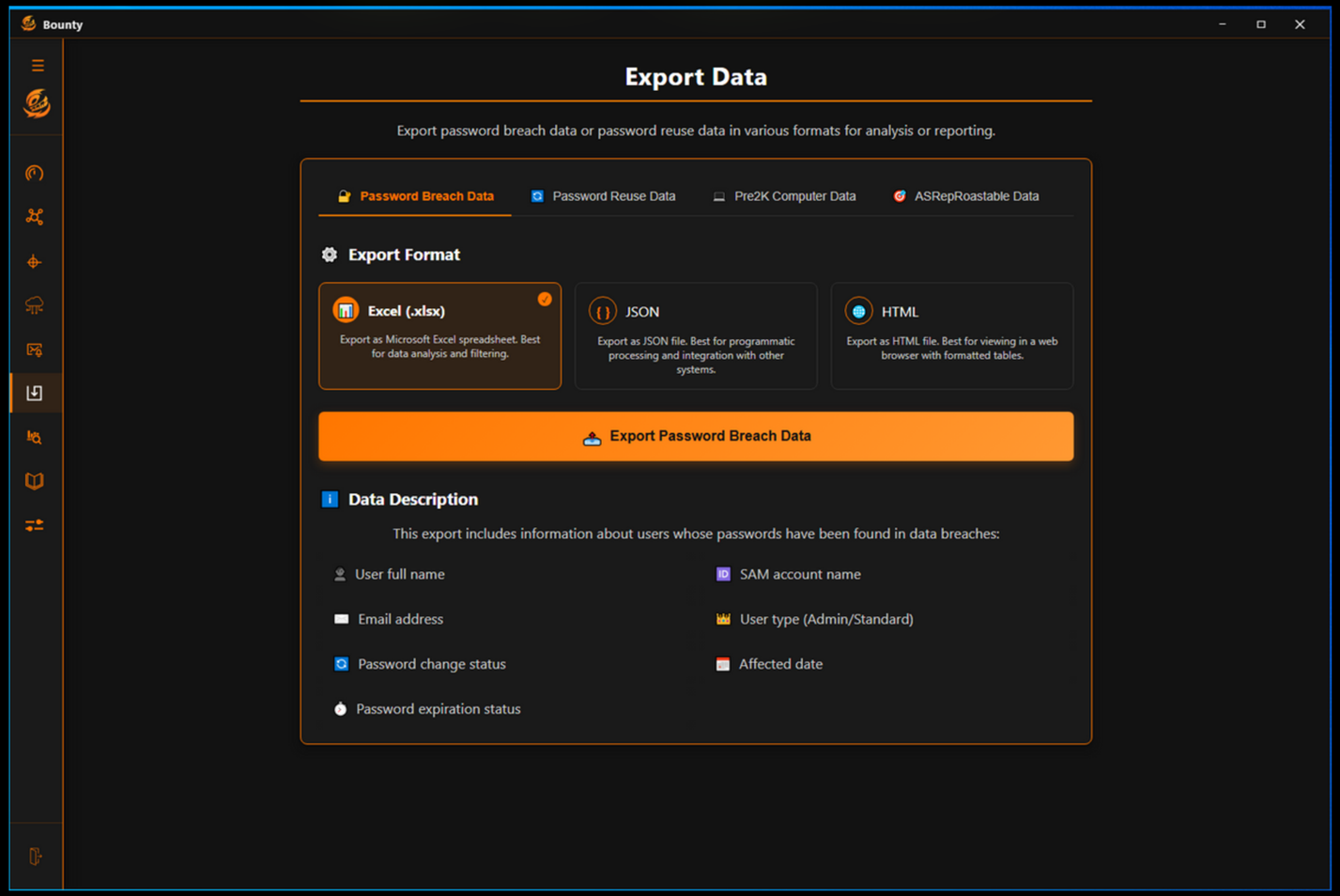
WIKI

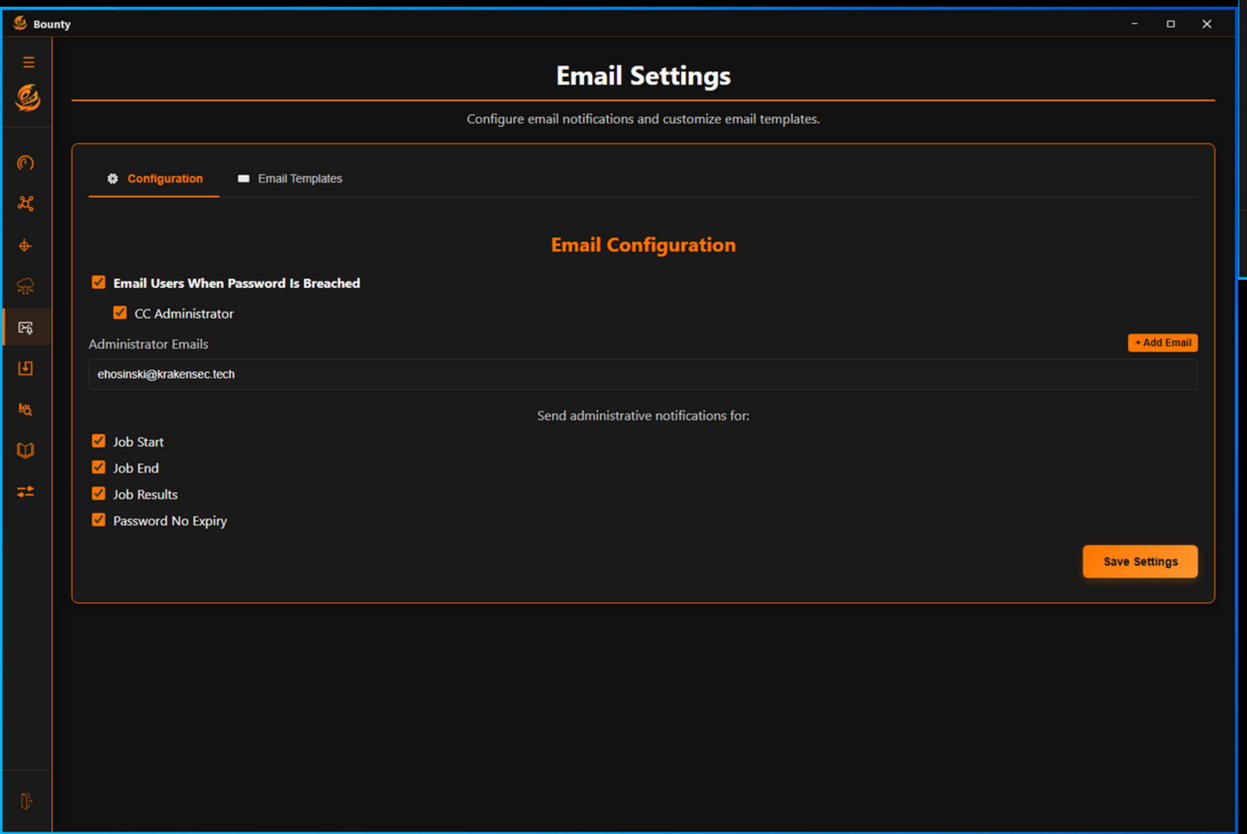
LOGGING

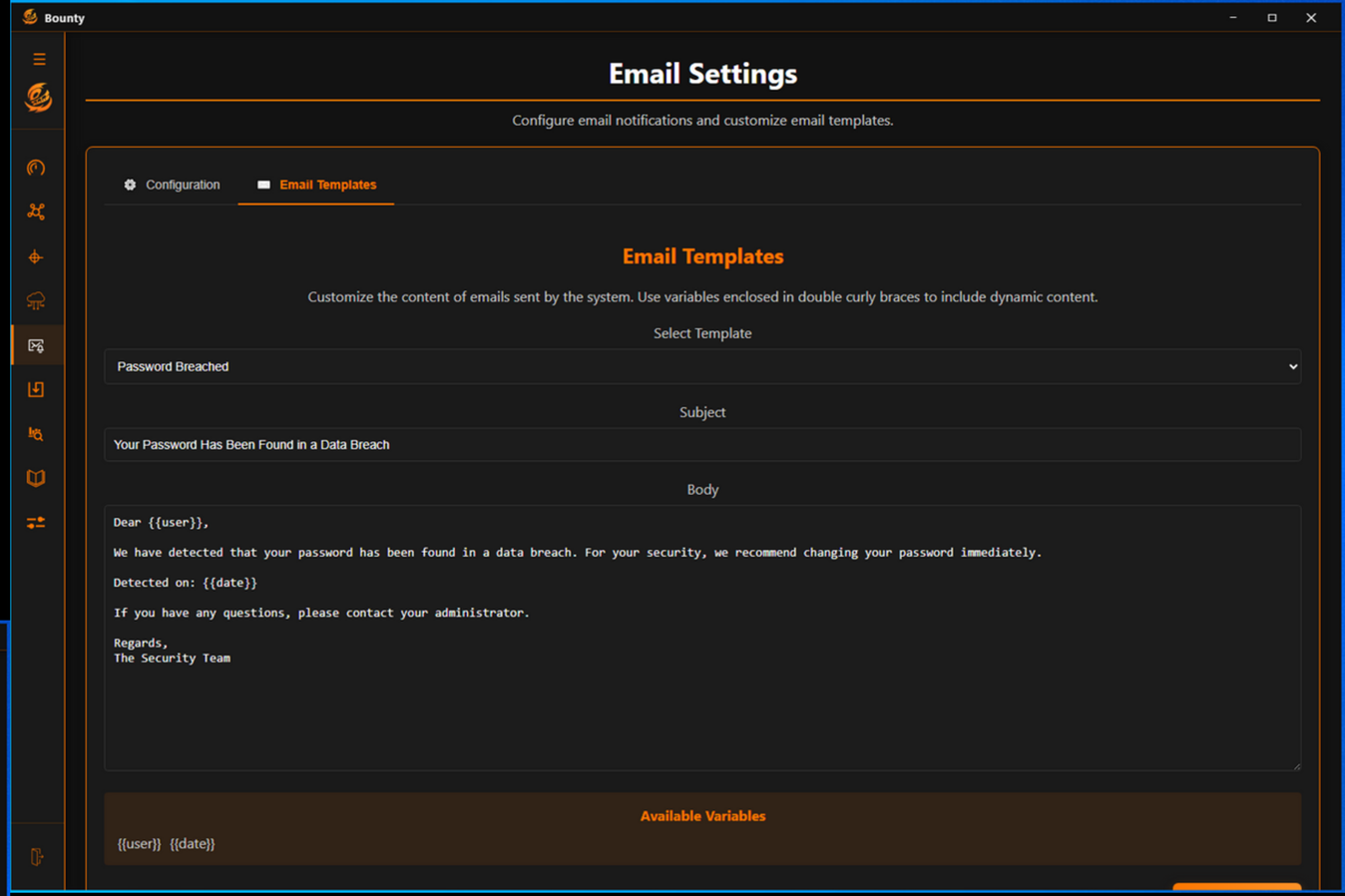

Bounty
Audit Logs
View and filter application logs to monitor system activity and troubleshoot issues. Use the search and filters below to find specific log entries.
Search logs by component, message, or error...
Source: User Service
Severity: All Levels From: mm/dd/yyyy To: mm/dd/yyyy Show: 20
Show Time Filters
Apply Filters
Log Entries
147 entries found
TIMESTAMP LEVEL COMPONENT MESSAGE ERROR
2025-09-22 17:18:16 INFO Bounty Database Servi... - -
Log Details
{"level":"INFO","ts":"2025-09-22T17:18:16.008-0400","msg":"Bounty Database Service started successfully"}
2025-09-22 17:18:16 INFO database service serve... - -
2025-09-22 17:18:16 INFO database server healt... - -
2025-09-22 17:18:15 INFO starting gRPC databas... - -
2025-09-22 17:18:15 INFO database server gorou... - -
2025-09-22 17:18:15 INFO database server create... - -
2025-09-22 17:18:15 INFO database server create... - -


Bounty
Audit Logs
View and filter application logs to monitor system activity and troubleshoot issues. Use the search and filters below to find specific log entries.
preference
Source: User Service
Severity: All Levels From: mm/dd/yyyy To: mm/dd/yyyy Show: 20
Show Time Filters
Apply Filters
Log Entries
24 entries found for "preference"
TIMESTAMP LEVEL COMPONENT MESSAGE ERROR
2025-09-29 14:59:43 INFO get_hash_sharing_pref... - -
Log Details
{"level":"INFO","ts":"2025-09-29T14:59:43.446-0400","msg":"get_hash_sharing_preference","opt_in":true}
2025-09-29 14:59:43 INFO get_hash_sharing_pref... - -
2025-09-29 14:59:35 INFO get_hash_sharing_pref... - -
2025-09-29 14:59:35 INFO get_hash_sharing_pref... - -
2025-09-29 14:59:01 INFO get_hash_sharing_pref... - -
2025-09-29 14:59:01 INFO get_hash_sharing_pref... - -
2025-09-16 15:33:46 INFO get_hash_sharing_pref... - -

EXPORT

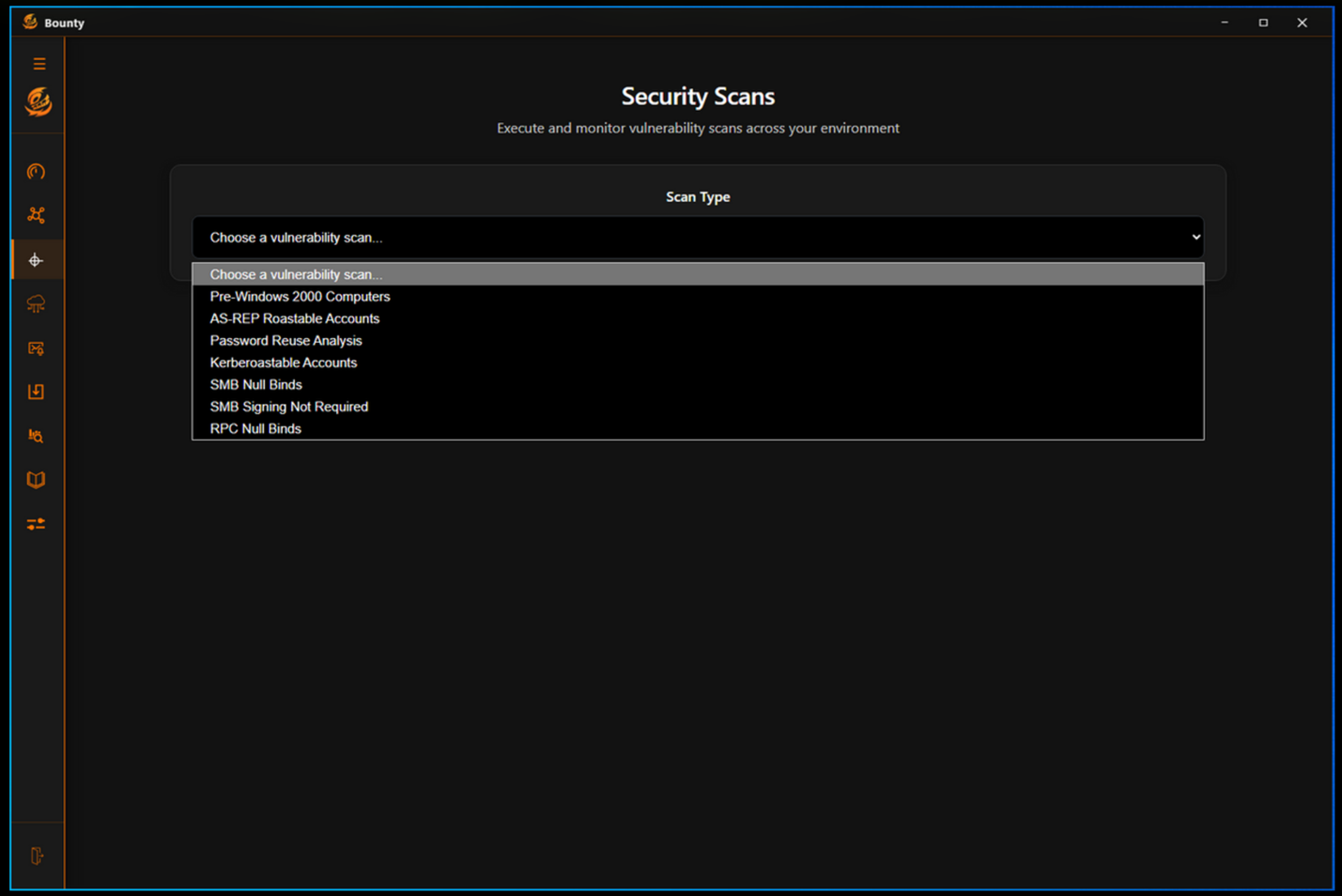

Bounty
Export Data
Export password breach data or password reuse data in various formats for analysis or reporting.
Password Breach Data
Password Reuse Data
Pre2K Computer Data
ASRepRoastable Data
Export Format
Excel (.xlsx)
Export as Microsoft Excel spreadsheet. Best for data analysis and filtering.
JSON
Export as JSON file. Best for programmatic processing and integration with other systems.
HTML
Export as HTML file. Best for viewing in a web browser with formatted tables.
Export Password Breach Data
Data Description
This export includes information about users whose passwords have been found in data breaches:
User full name
SAM account name
Email address
User type (Admin/Standard)
Password change status
Affected date
Password expiration status



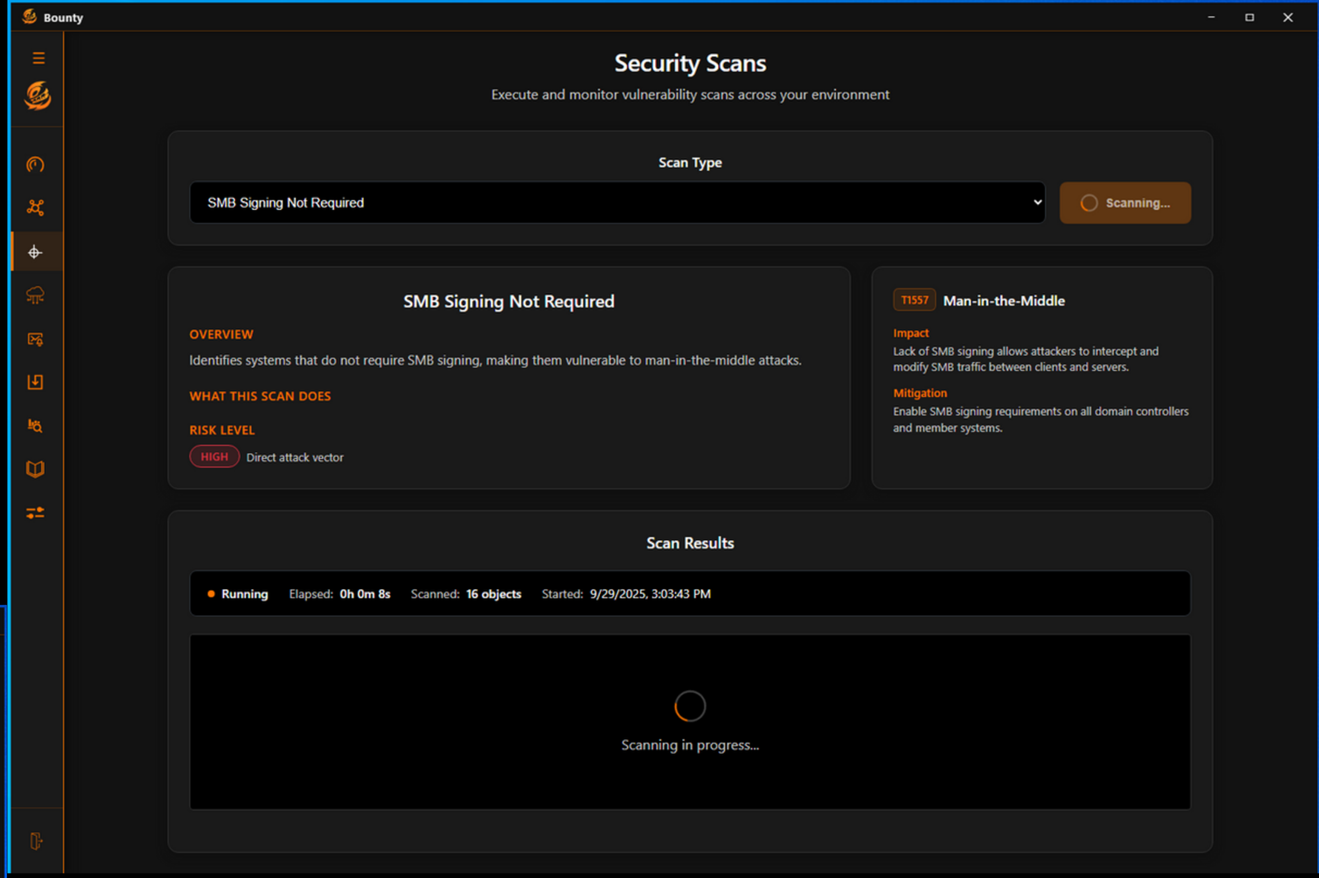


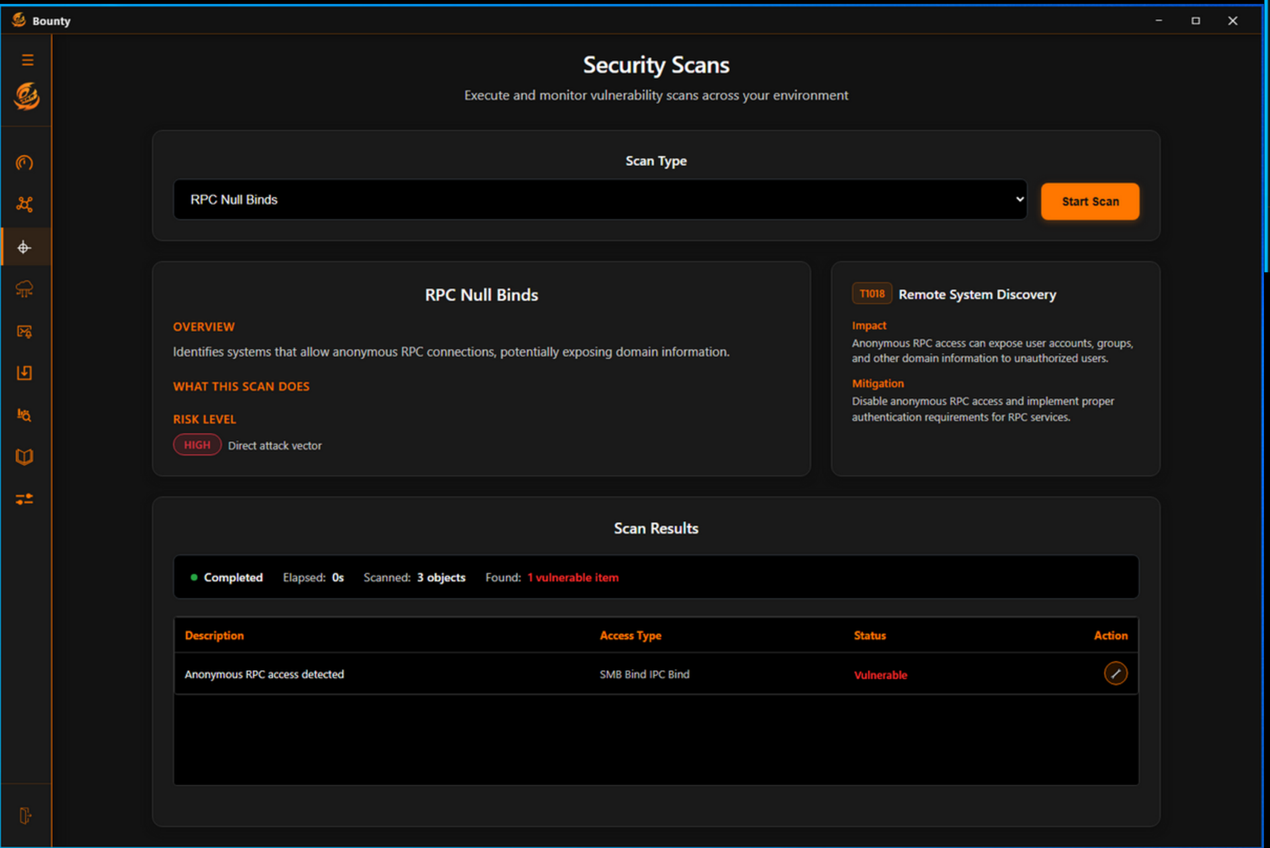
ALERT EMAILS

AD HOC SCANNING



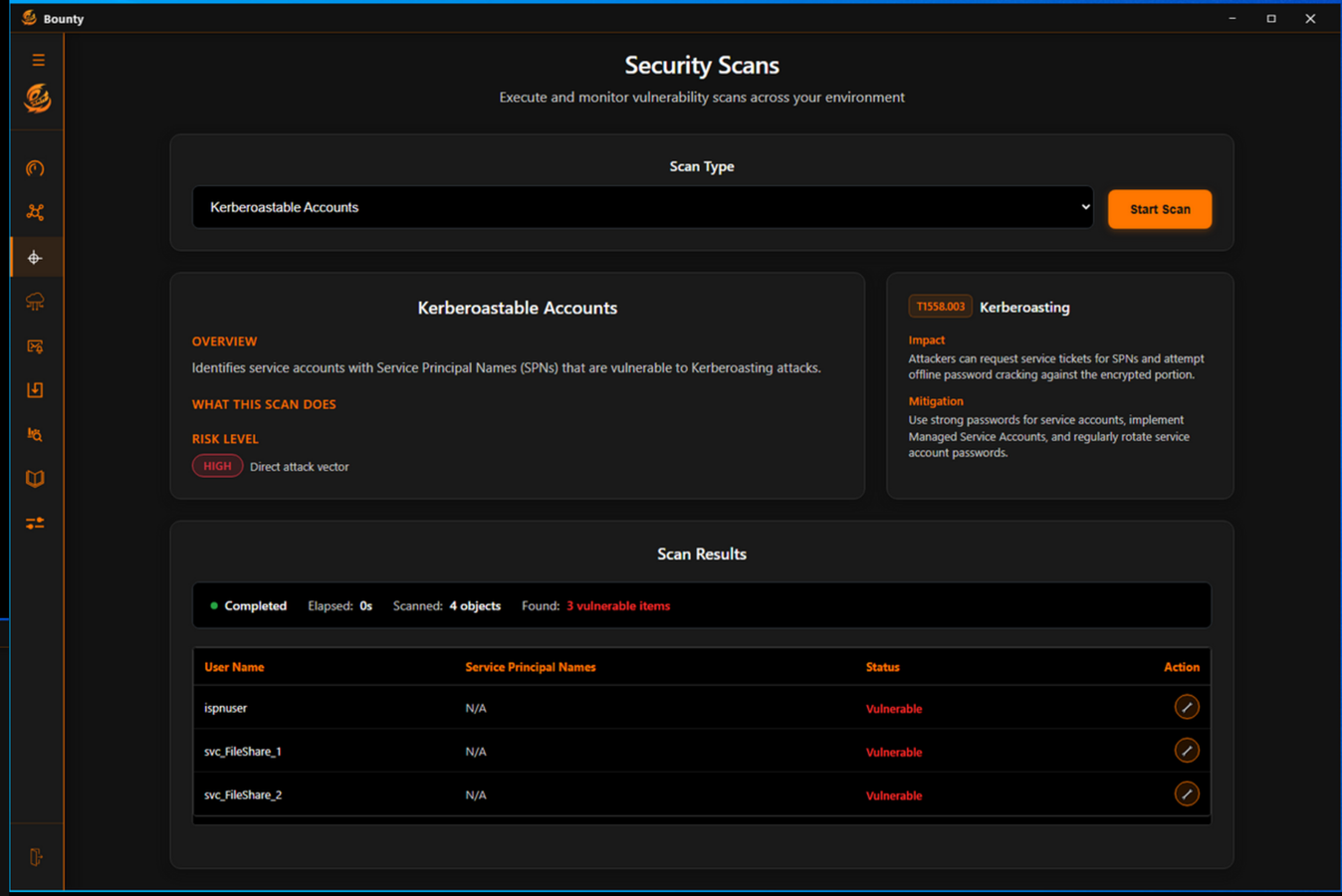
SMB SIGNING

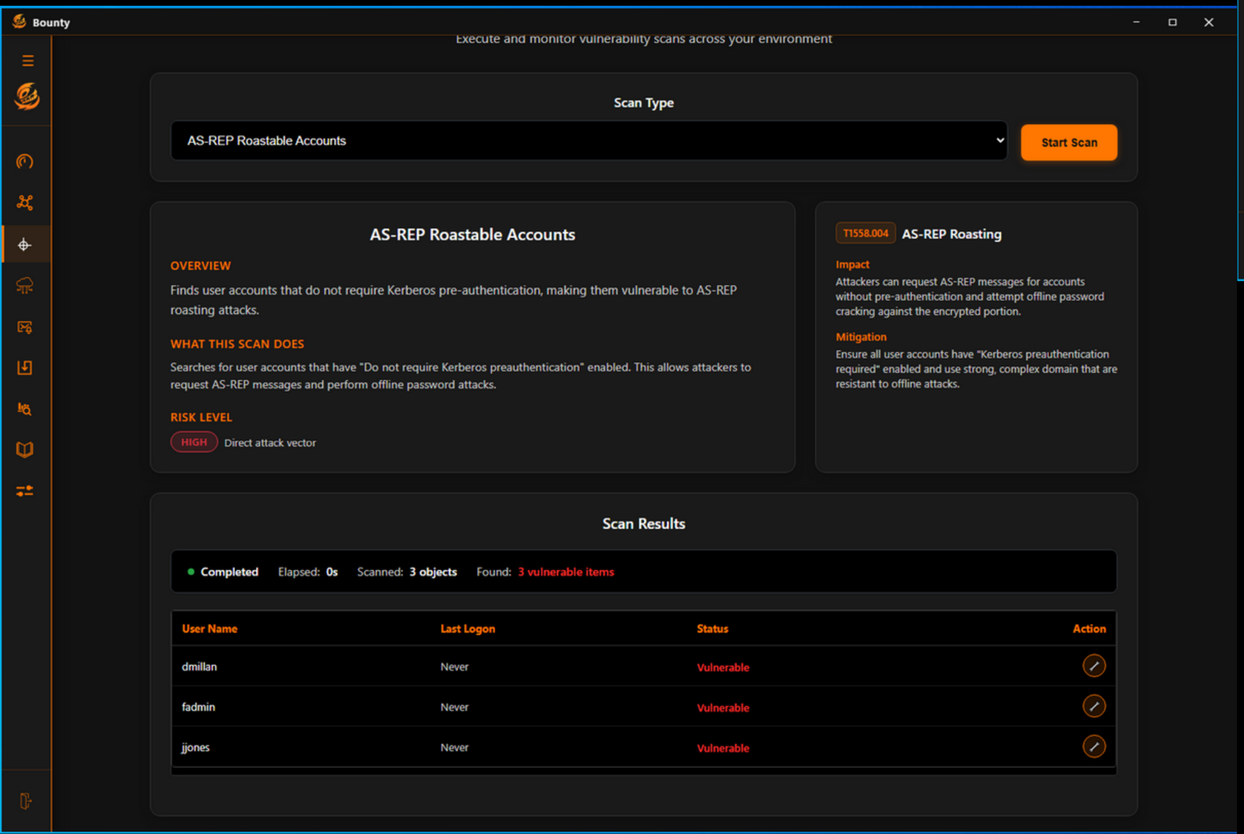




RPC NULL BIND

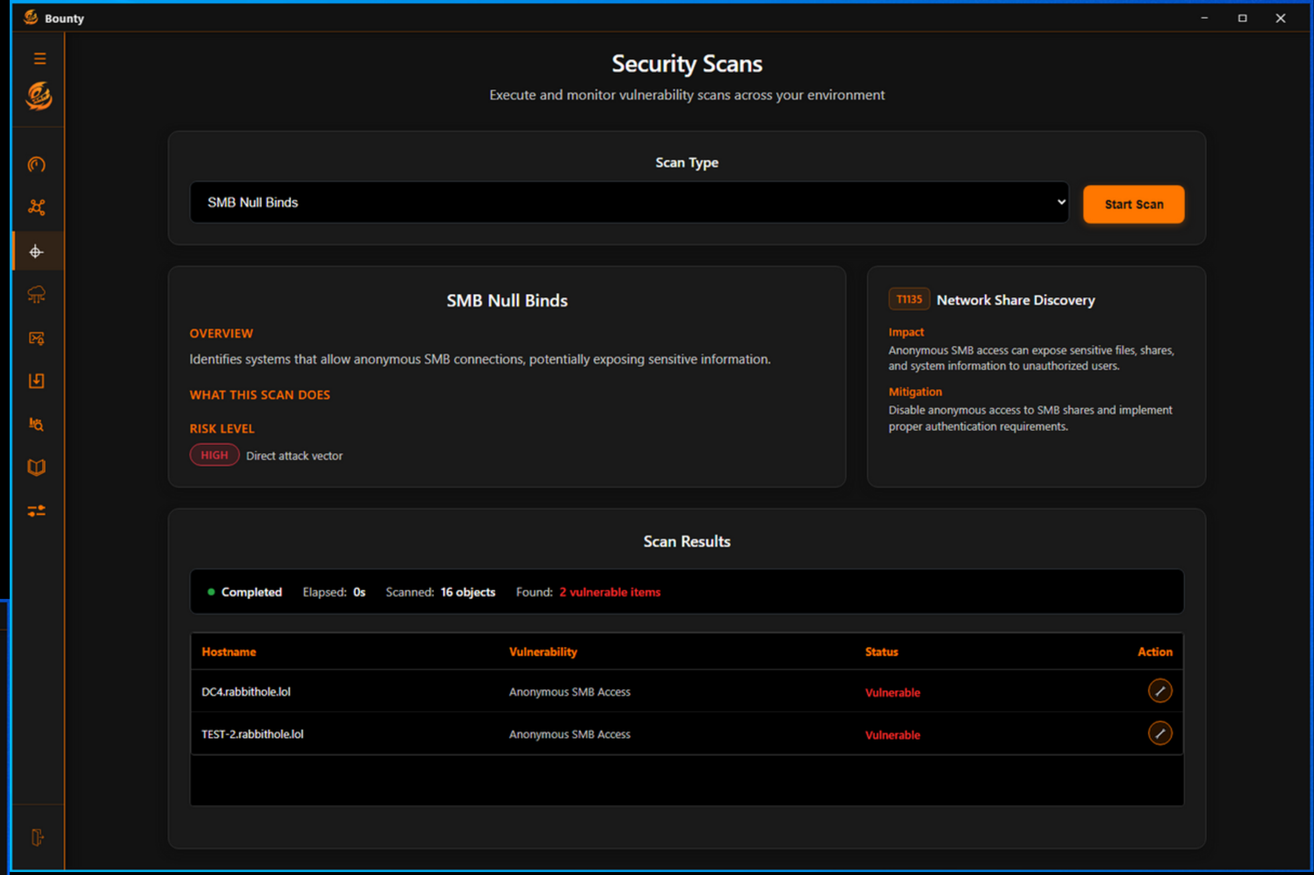
KERBEROAST

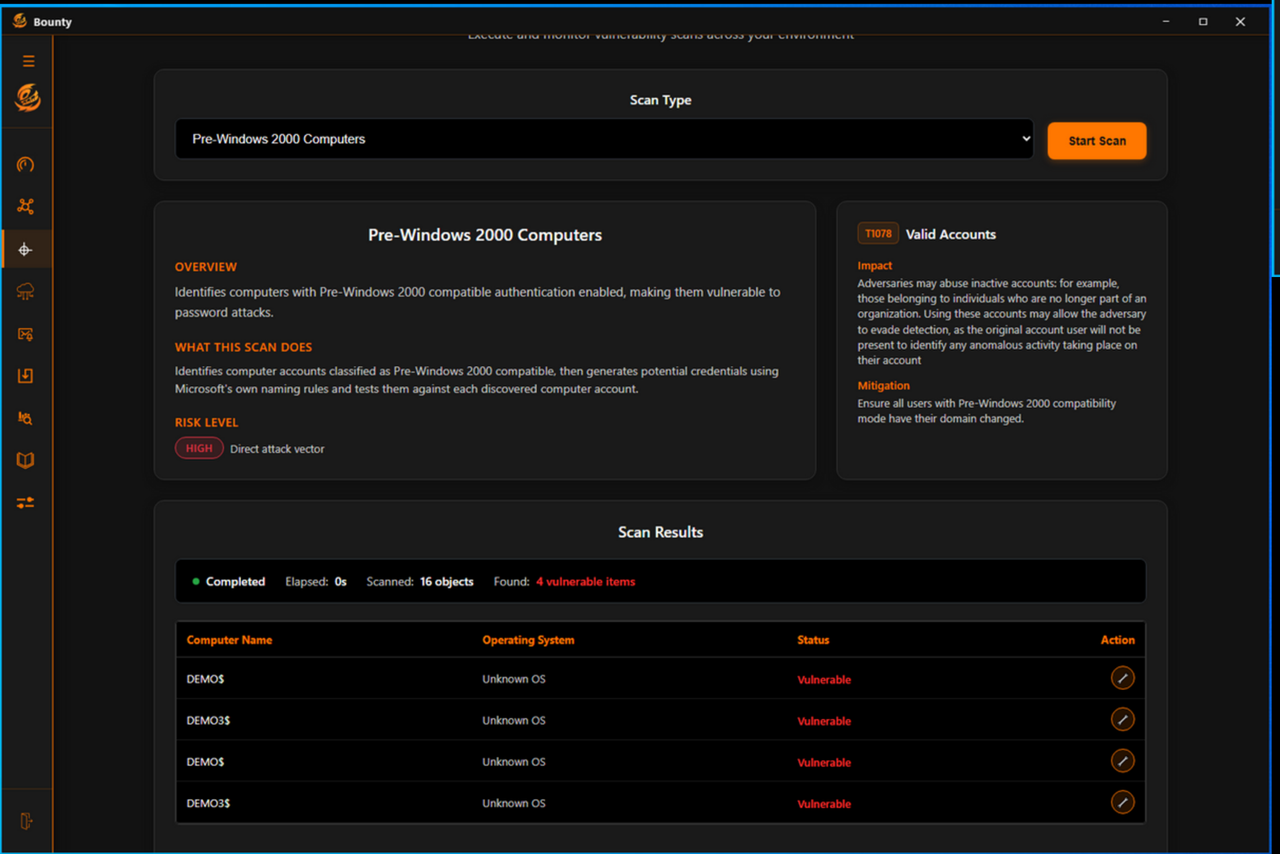




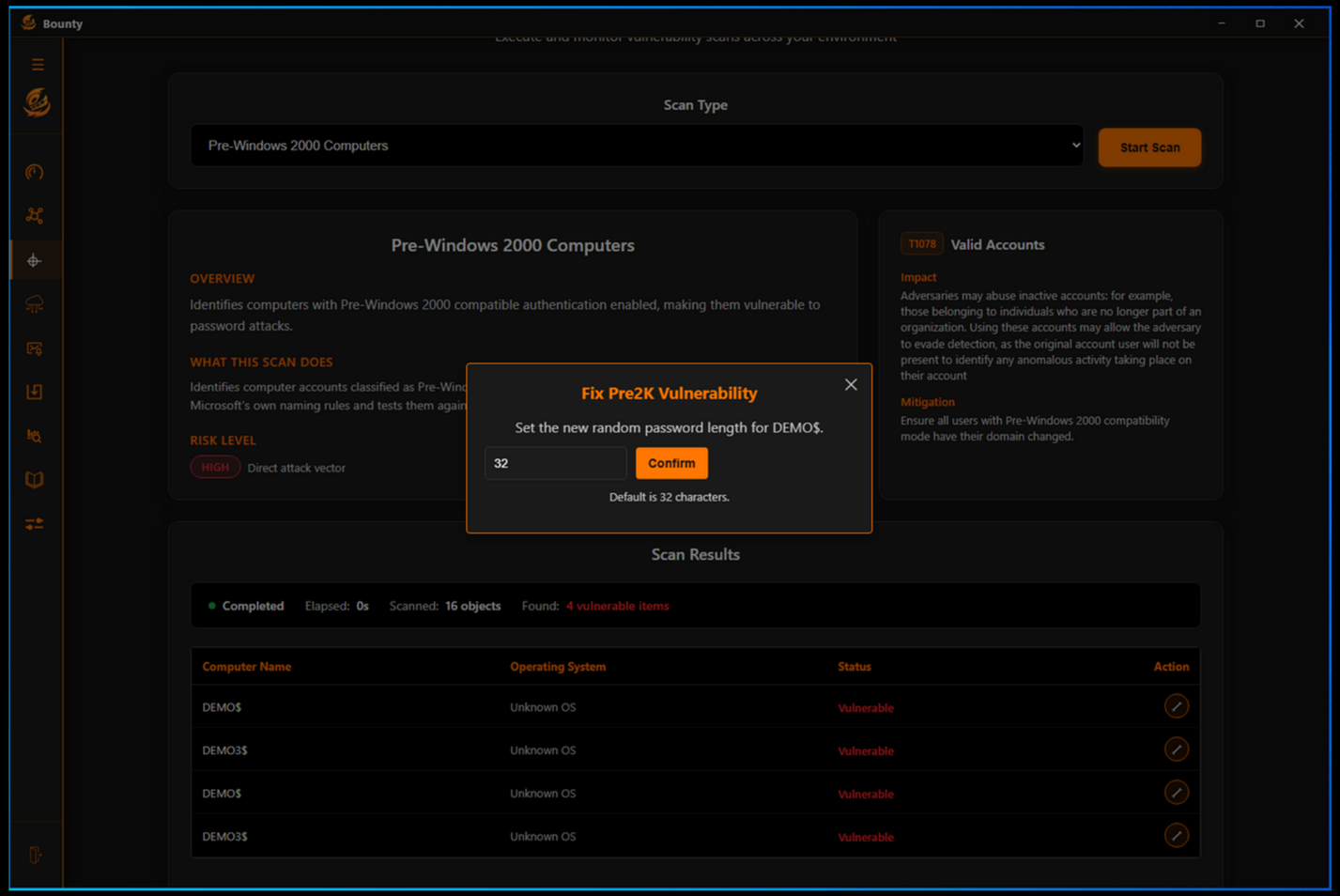
ASREPROAST

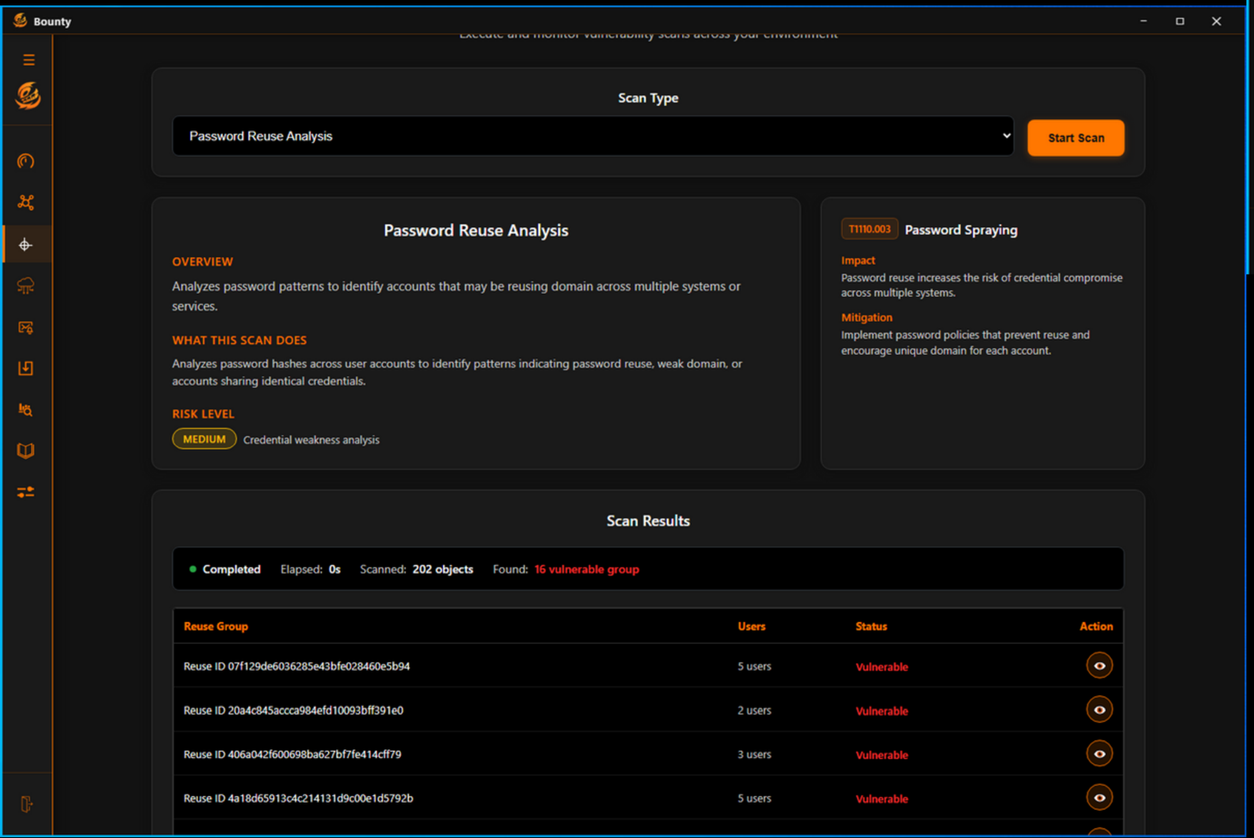
SMB NULL BINDS

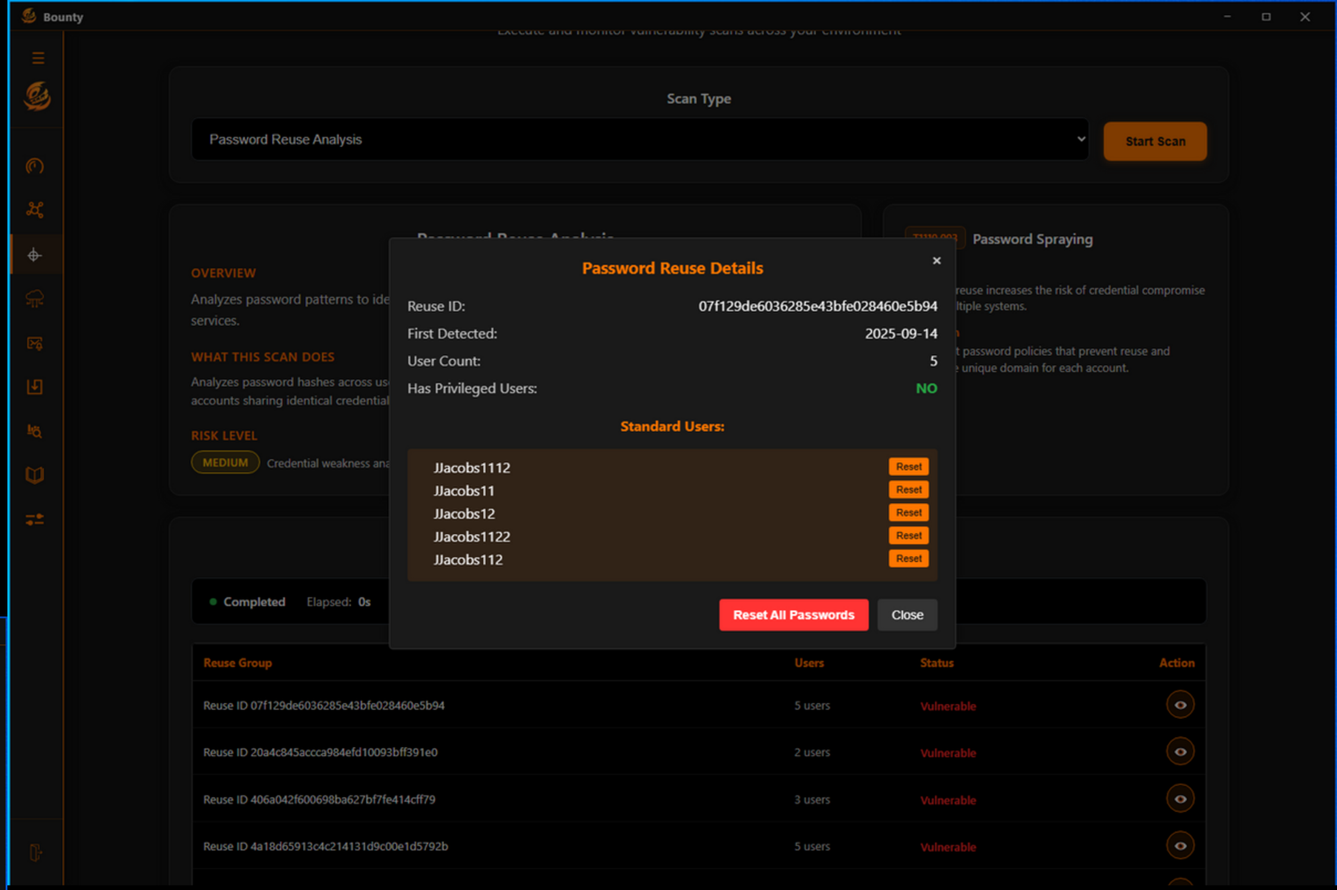




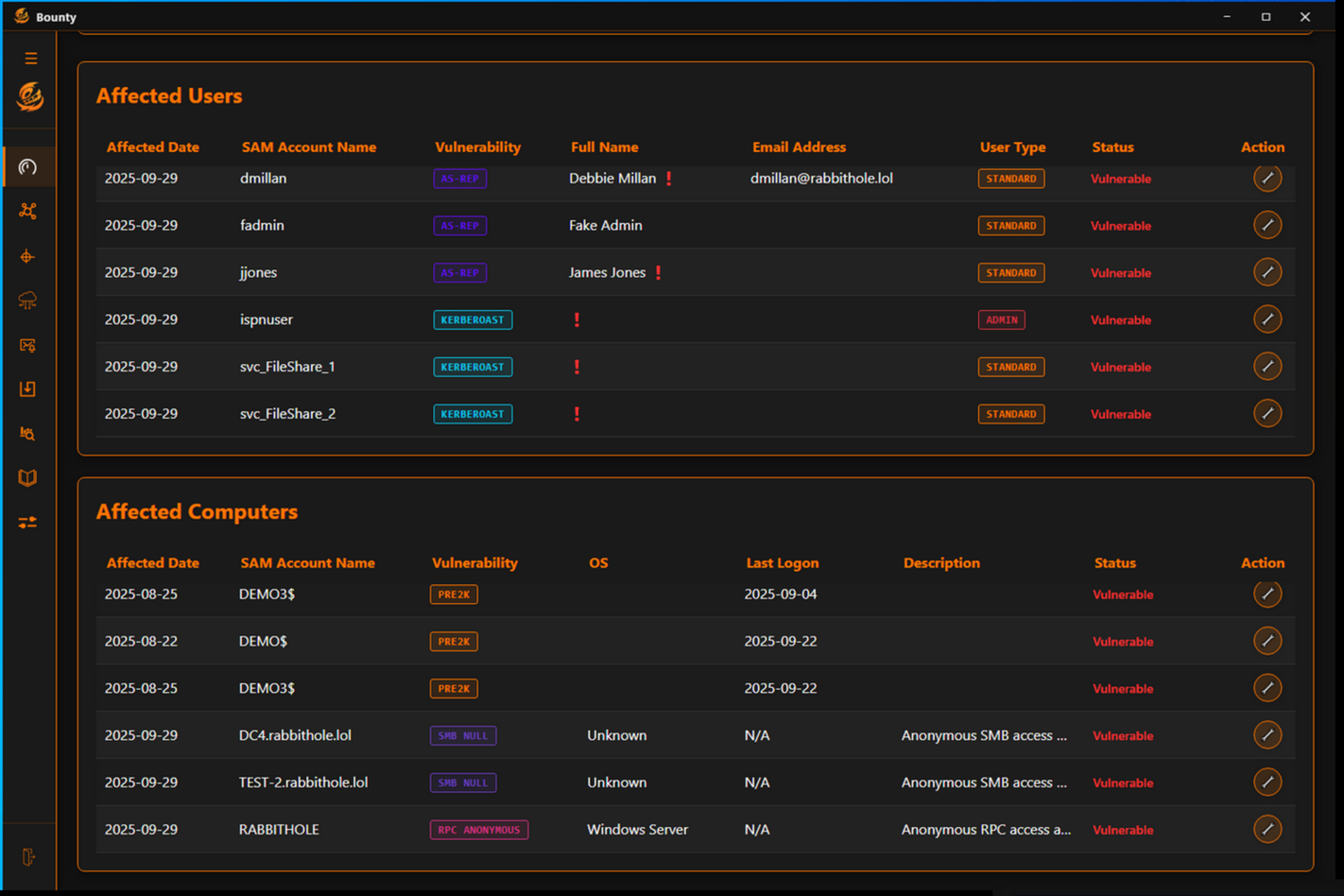
PRE2K COMPUTERS


Bounty
Scan Type
Pre-Windows 2000 Computers
Start Scan
Pre-Windows 2000 Computers
OVERVIEW
Identifies computers with Pre-Windows 2000 compatible authentication enabled, making them vulnerable to password attacks.
WHAT THIS SCAN DOES
Identifies computer accounts classified as Pre-Win
Microsoft's own naming rules and tests them agai
RISK LEVEL
HIGH
Direct attack vector
T1078
Valid Accounts
Impact
Adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account
Mitigation
Ensure all users with Pre-Windows 2000 compatibility mode have their domain changed.
Fix Pre2K Vulnerability
Set the new random password length for DEMO$.
32
Confirm
Default is 32 characters.
Scan Results
Completed
Elapsed: 0s
Scanned: 16 objects
Found: 4 vulnerable items
Computer Name
Operating System
Status
Action
DEMO$
Unknown OS
Vulnerable
DEMO3$
Unknown OS
Vulnerable
DEMO$
Unknown OS
Vulnerable
DEMO3$
Unknown OS
Vulnerable





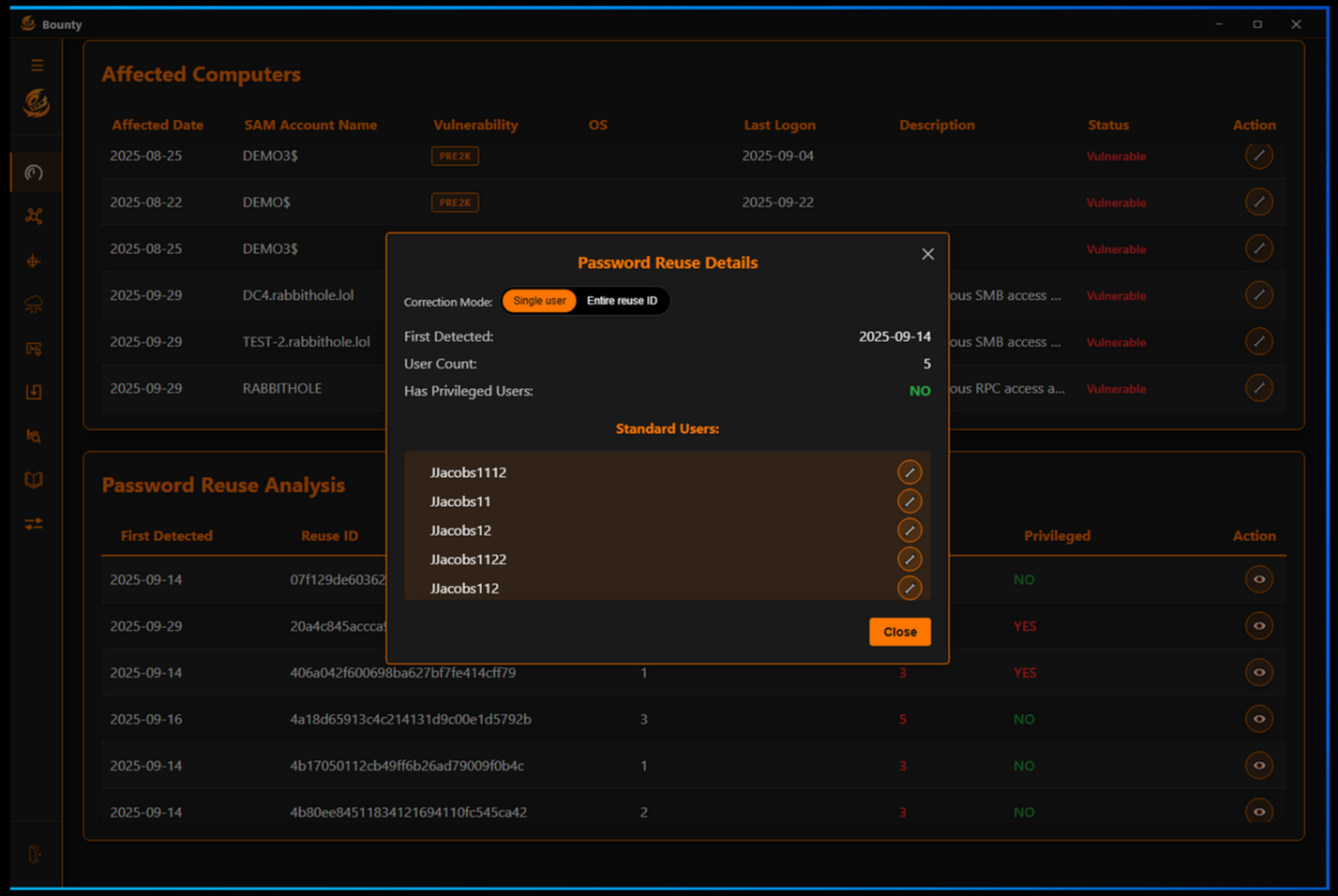
PASSWORD REUSE



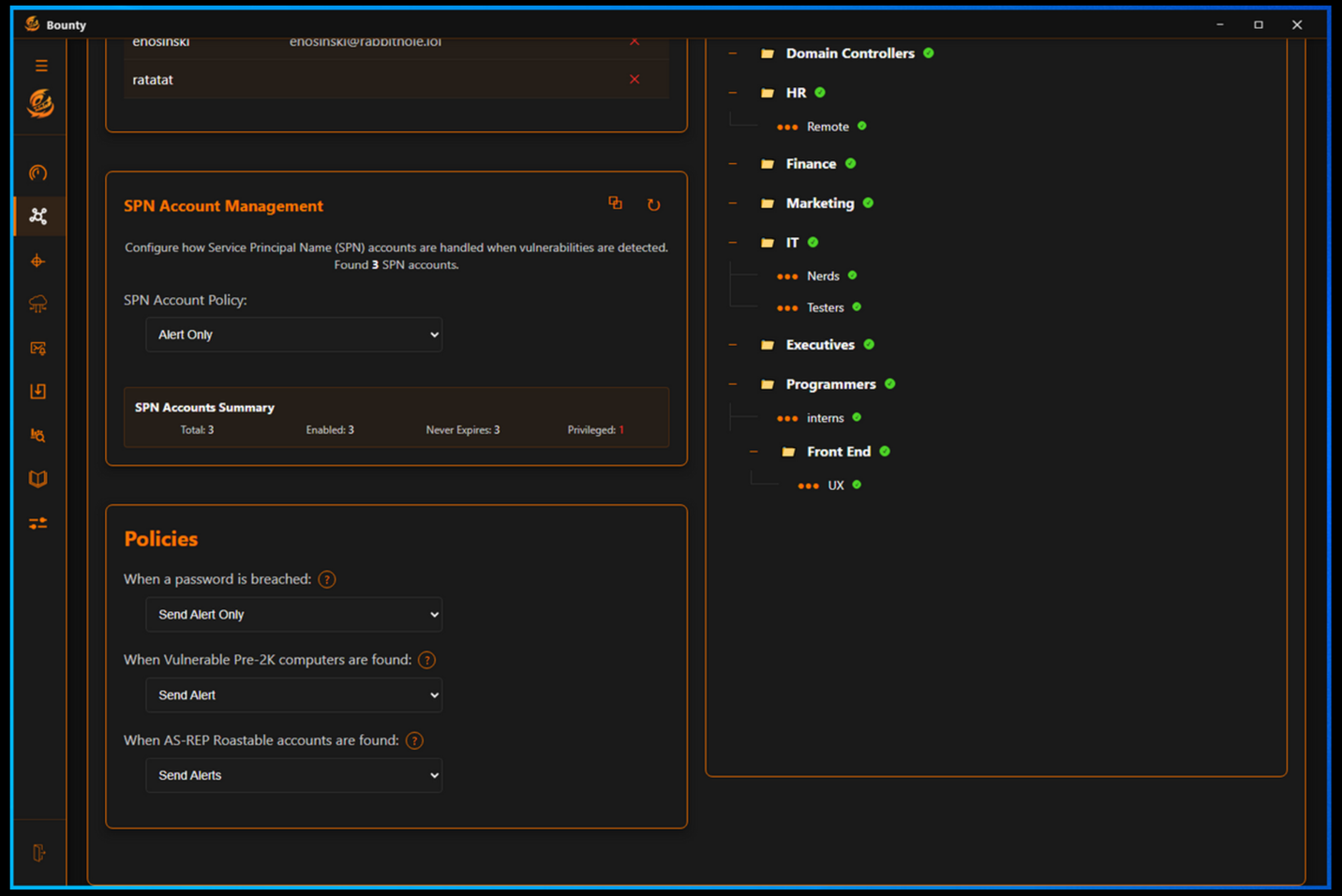
SCAN RESULTS DASHBOARD

Password Reuse Analysis

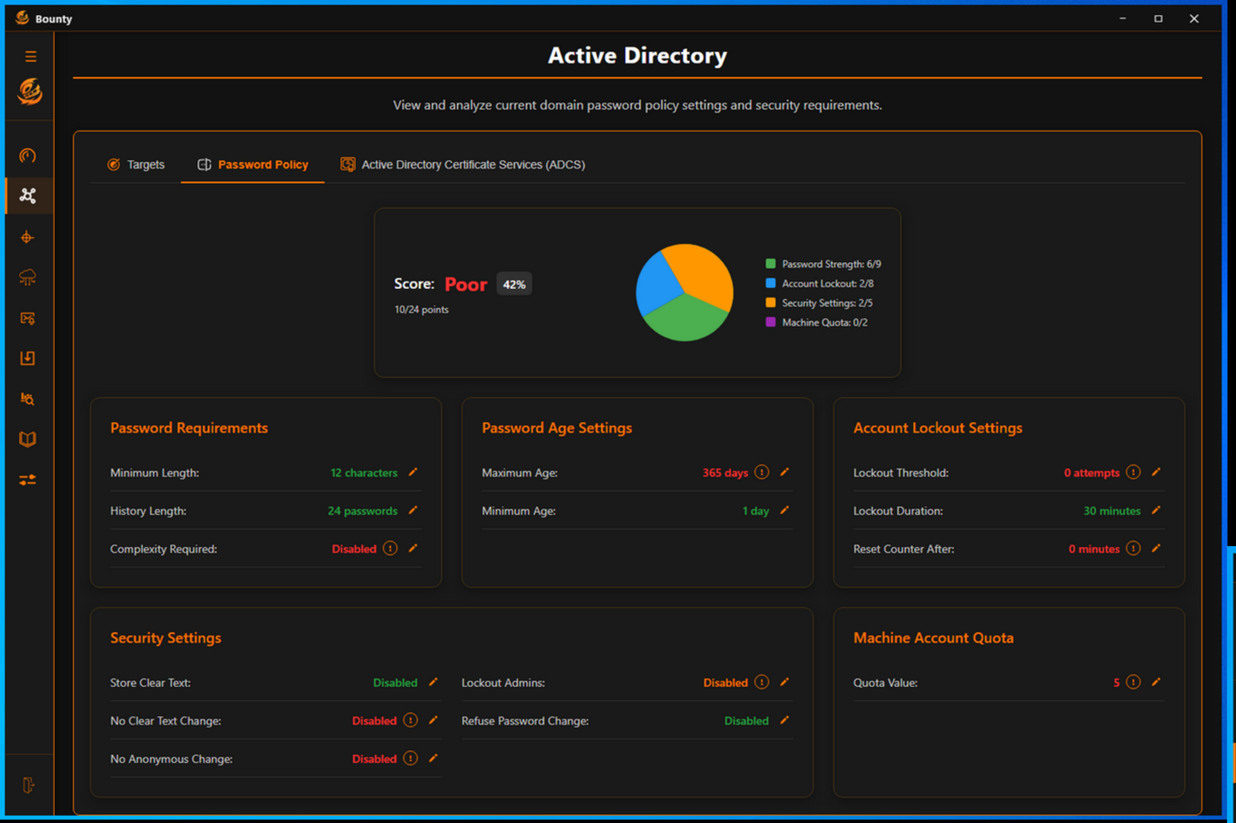
First Detected	Reuse ID	Scan ID	Count	Privileged	Action
2025-09-14	07f129de6036285e43bfe028460e5b94	1	5	NO	
2025-09-29	20a4c845accca984efd10093bff391e0	4	2	YES	
2025-09-14	406a042f600698ba627bf7fe414cff79	1	3	YES	
2025-09-16	4a18d65913c4c214131d9c00e1d5792b	3	5	NO	
2025-09-14	4b17050112cb49ff6b26ad79009f0b4c	1	3	NO	
2025-09-14	4b80ee84511834121694110fc545ca42	2	3	NO	

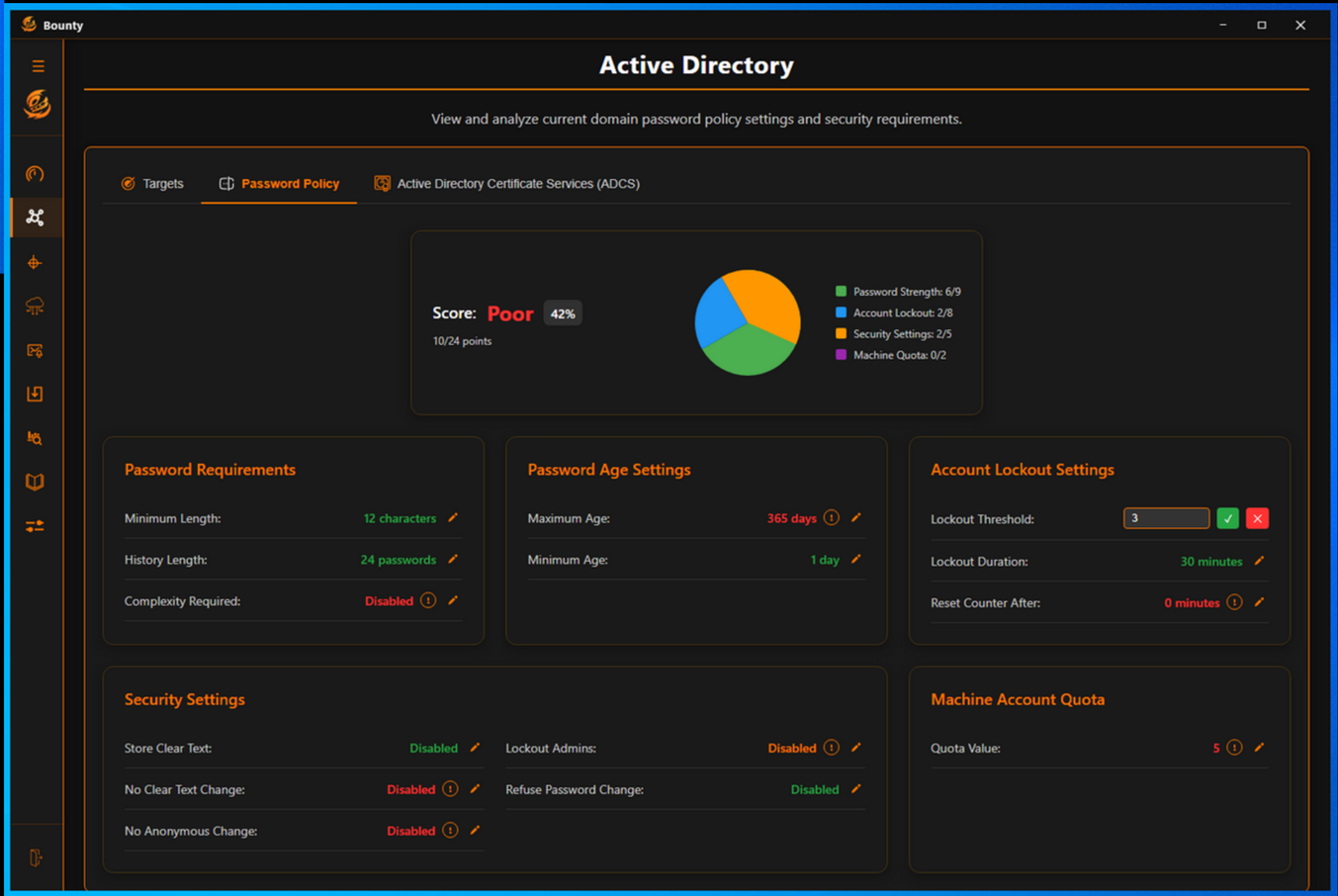

Bounty
Affected Computers
Affected Date
SAM Account Name
Vulnerability
OS
Last Logon
Description
Status
Action
2025-08-25
DEMO3$
PRE2K
2025-09-04
Vulnerable
2025-08-22
DEMO$
PRE2K
2025-09-22
Vulnerable
2025-08-25
DEMO3$
Vulnerable
2025-09-29
DC4.rabbithole.lol
ous SMB access ...
Vulnerable
2025-09-29
TEST-2.rabbithole.lol
ous SMB access ...
Vulnerable
2025-09-29
RABBITHOLE
ous RPC access a...
Vulnerable
Password Reuse Analysis
First Detected
Reuse ID
Privileged
Action
2025-09-14
07f129de60362
NO
2025-09-29
20a4c845accca
YES
2025-09-14
406a042f600698ba627bf7fe414cff79
1
3
YES
2025-09-16
4a18d65913c4c214131d9c00e1d5792b
3
5
NO
2025-09-14
4b17050112cb49ff6b26ad79009f0b4c
1
3
NO
2025-09-14
4b80ee84511834121694110fc545ca42
2
3
NO
Password Reuse Details
Correction Mode:
Single user
Entire reuse ID
First Detected:
2025-09-14
User Count:
5
Has Privileged Users:
NO
Standard Users:
JJacobs1112
JJacobs11
JJacobs12
JJacobs1122
JJacobs112
Close

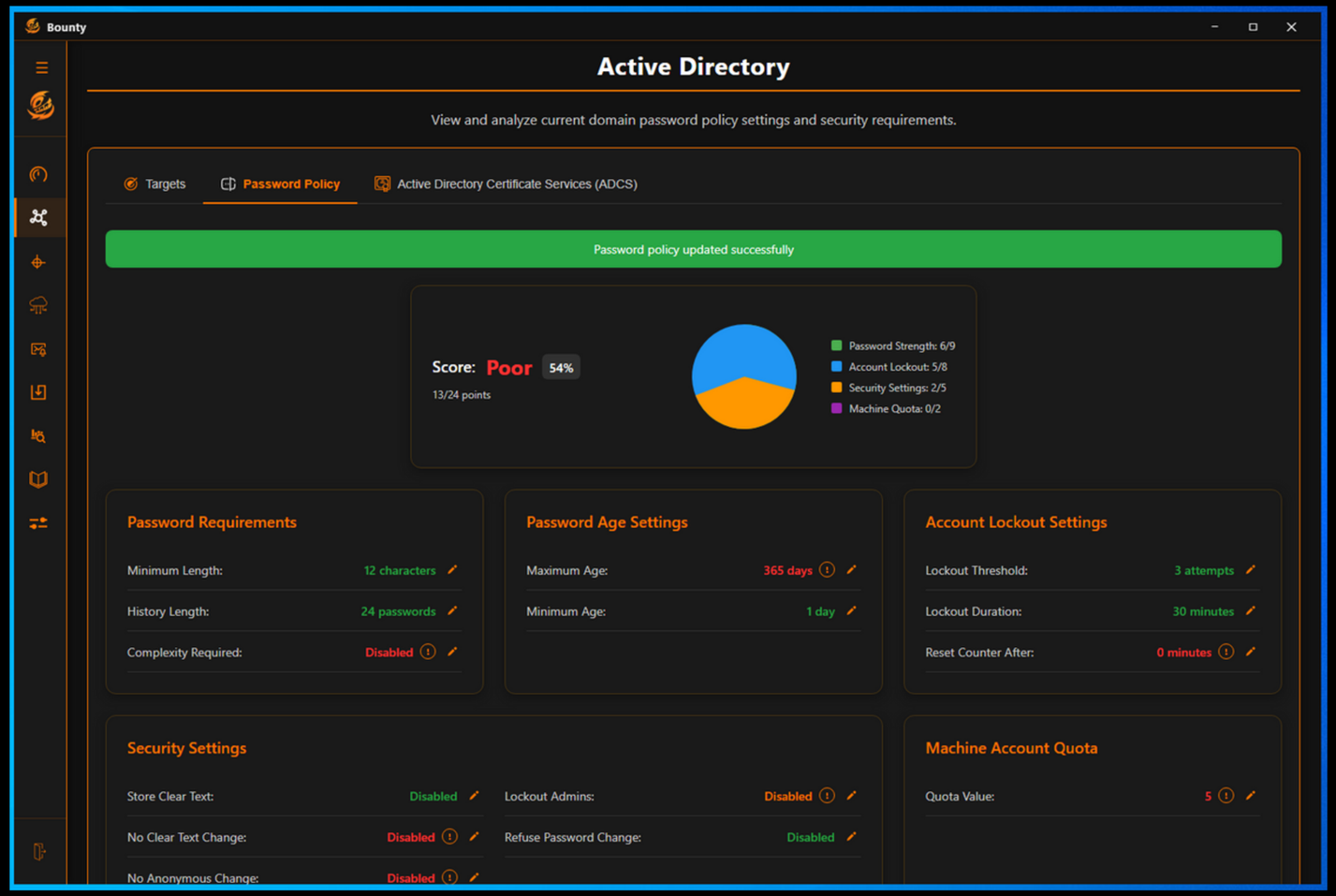
ACTIVE DIRECTORY

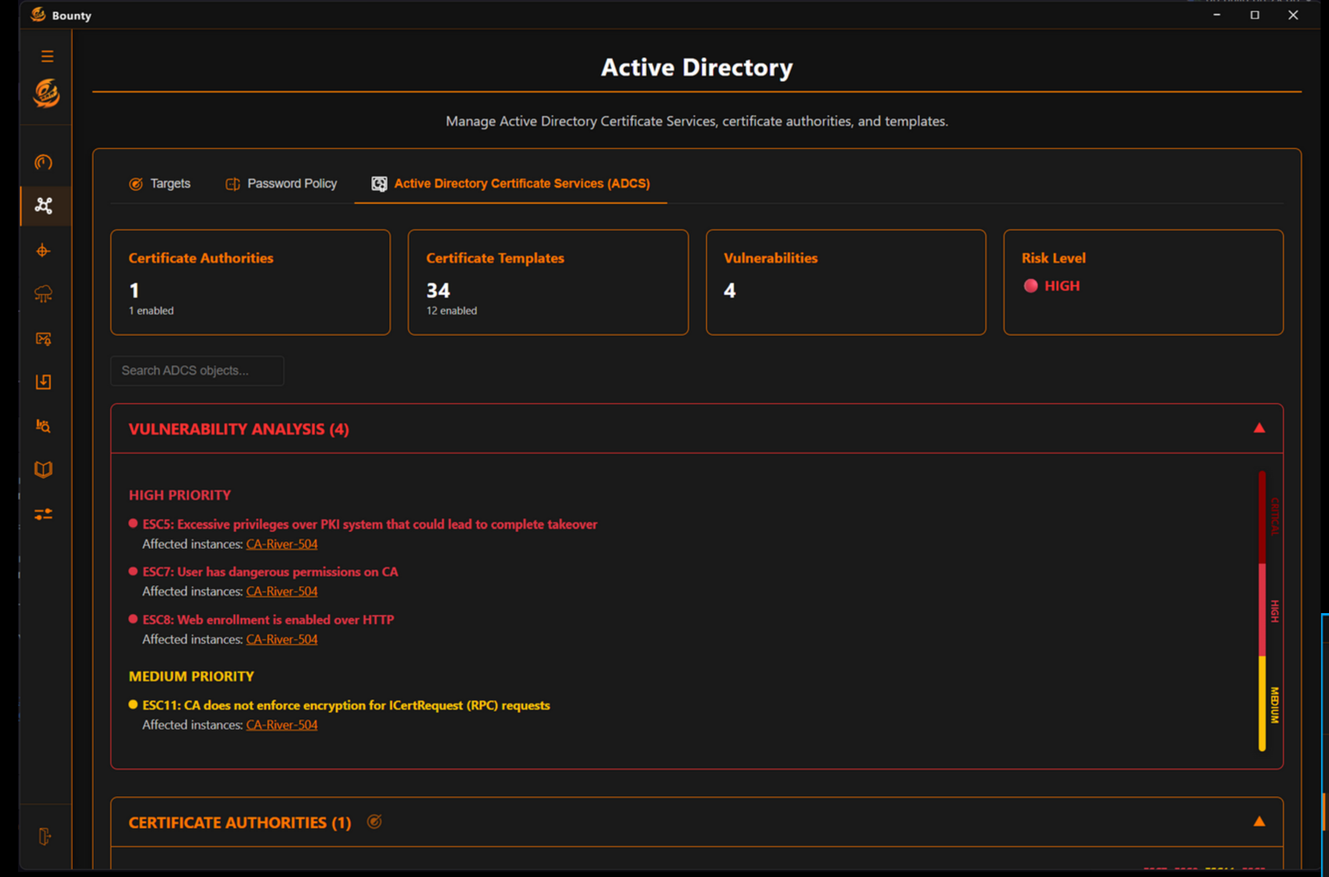


PASSWORD POLICY

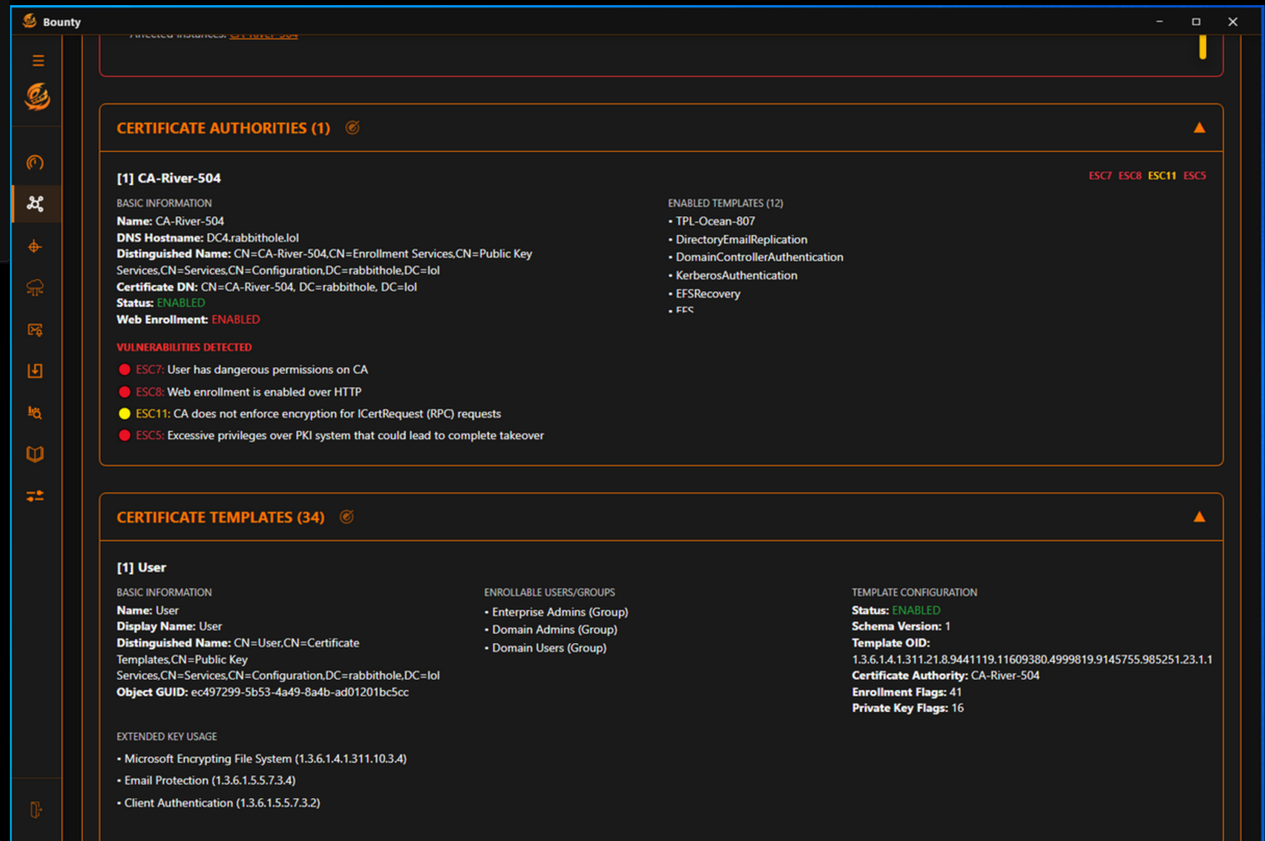


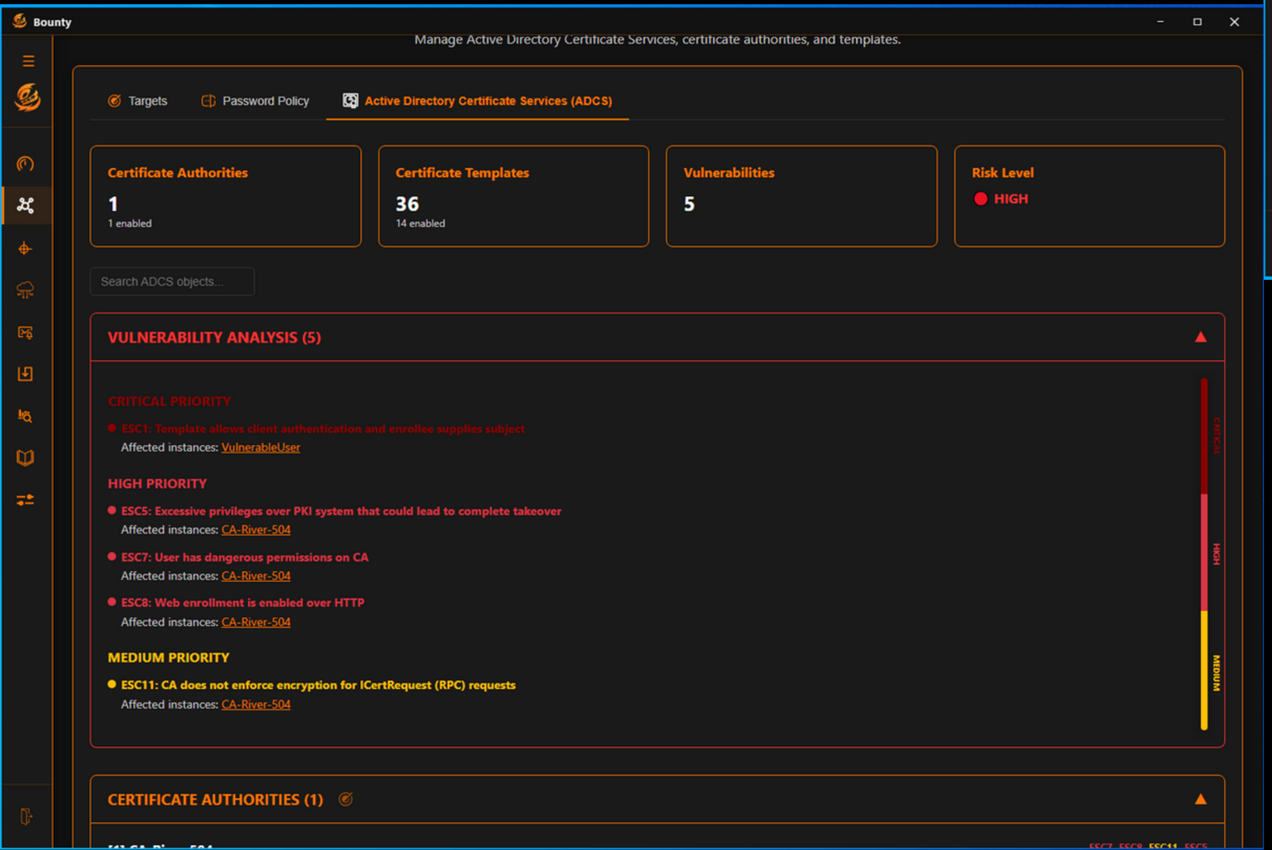


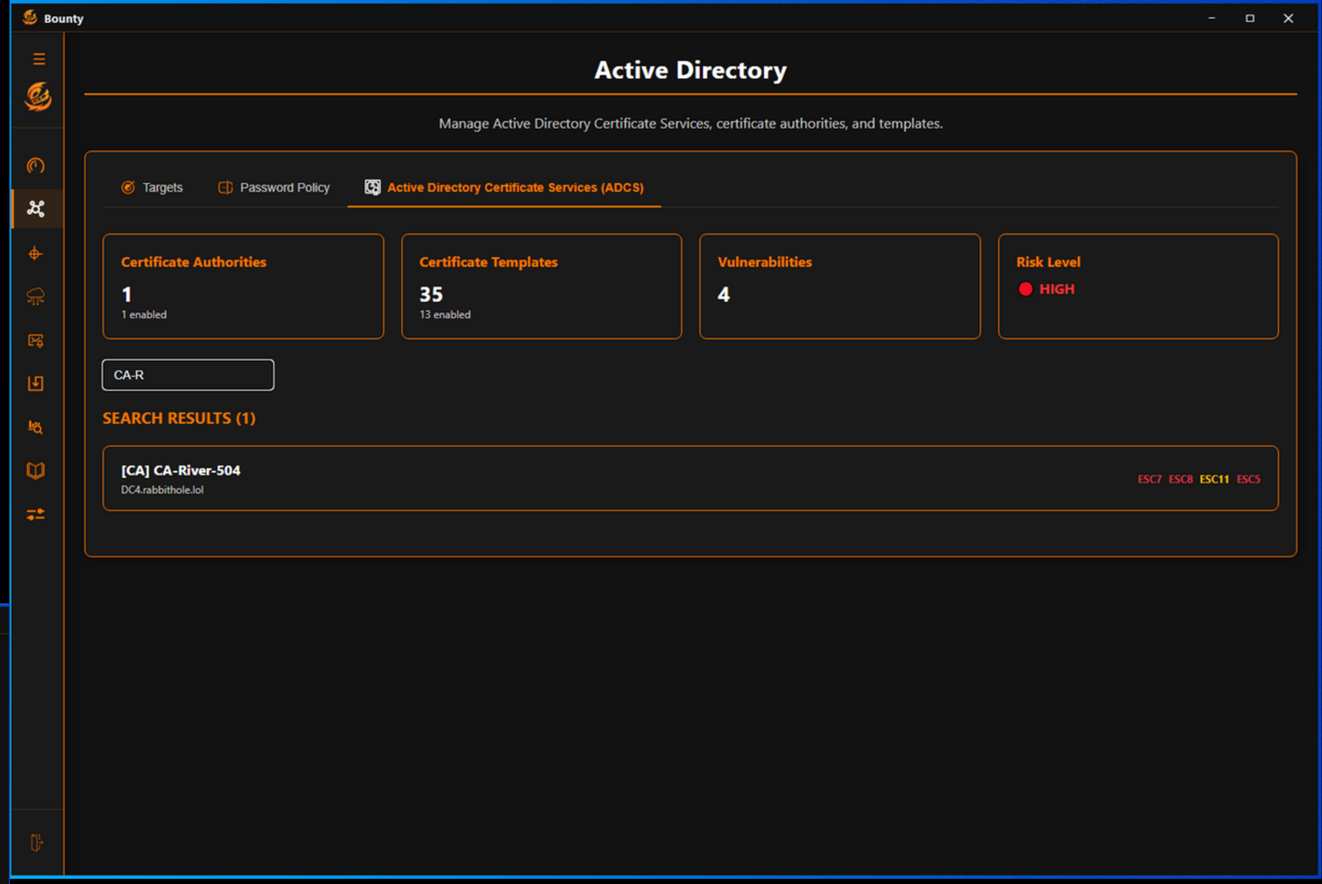

Bounty
Active Directory
View and analyze current domain password policy settings and security requirements.
Targets
Password Policy
Active Directory Certificate Services (ADCS)
Password policy updated successfully
Score: Poor 54%
13/24 points
Password Strength: 6/9
Account Lockout: 5/8
Security Settings: 2/5
Machine Quota: 0/2
Password Requirements
Minimum Length: 12 characters
History Length: 24 passwords
Complexity Required: Disabled
Password Age Settings
Maximum Age: 365 days
Minimum Age: 1 day
Account Lockout Settings
Lockout Threshold: 3 attempts
Lockout Duration: 30 minutes
Reset Counter After: 0 minutes
Security Settings
Store Clear Text: Disabled
No Clear Text Change: Disabled
No Anonymous Change: Disabled
Lockout Admins: Disabled
Refuse Password Change: Disabled
Machine Account Quota
Quota Value: 5



ACTIVE DIRECTORY CERTIFICATE SERVICES




Bounty
Manage Active Directory Certificate Services, certificate authorities, and templates.
Targets
Password Policy
Active Directory Certificate Services (ADCS)
Certificate Authorities
1
1 enabled
Certificate Templates
36
14 enabled
Vulnerabilities
5
Risk Level
HIGH
Search ADCS objects...
VULNERABILITY ANALYSIS (5)
CRITICAL PRIORITY
ESC1: Template allows client authentication and enrollee supplies subject
Affected instances: VulnerableUser
HIGH PRIORITY
ESC5: Excessive privileges over PKI system that could lead to complete takeover
Affected instances: CA-River-504
ESC7: User has dangerous permissions on CA
Affected instances: CA-River-504
ESC8: Web enrollment is enabled over HTTP
Affected instances: CA-River-504
MEDIUM PRIORITY
ESC11: CA does not enforce encryption for ICertRequest (RPC) requests
Affected instances: CA-River-504
CRITICAL
HIGH
MEDIUM
CERTIFICATE AUTHORITIES (1)


Bounty
Active Directory
Manage Active Directory Certificate Services, certificate authorities, and templates.
Targets
Password Policy
Active Directory Certificate Services (ADCS)
Certificate Authorities
1
1 enabled
Certificate Templates
35
13 enabled
Vulnerabilities
4
Risk Level
HIGH
CA-R
SEARCH RESULTS (1)
[CA] CA-River-504
DC4.rabbithole.lol
ESC7 ESC8 ESC11 ESC5

[CA] CA-River-504

Certificate Authority Information

Name: CA-River-504

DNS Host: DC4.rabbithole.lol

Status: ENABLED

Web Enrollment: ENABLED

Distinguished Name

```
CN=CA-River-504,CN=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration,DC=rabbithole,DC=lol
```

Certificate DN

```
CN=CA-River-504, DC=rabbithole, DC=lol
```

Security Vulnerabilities

ESC5
Excessive privileges over PKI system that could lead to complete takeover

ESC7
User has dangerous permissions on CA

ESC8
Web enrollment is enabled over HTTP

ESC11
CA does not enforce encryption for ICertRequest (RPC) requests

Enabled Templates (13)

- TPL-Stone-178
- TPL-Ocean-807
- DirectoryEmailReplication
- DomainControllerAuthentication
- KerberosAuthentication

[Template] Vulnerable User

Certificate Template Information

Name: VulnerableUser

Display Name: Vulnerable User

Status: ENABLED

Schema Version: 2

Certificate Authority: CA-River-504

Distinguished Name

```
CN=VulnerableUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=rabbithole,DC=lol
```

Template Configuration

Template OID: 1.3.6.1.4.1.311.21.8.9441119.11609380.4999819.9145755.985251.23.7159938.5272627

Object GUID: a244b9fe-afef-438a-b462-323bc9fb407c

Enrollment Flags: 9

Private Key Flags: 16842768

ESC1

Security Vulnerabilities

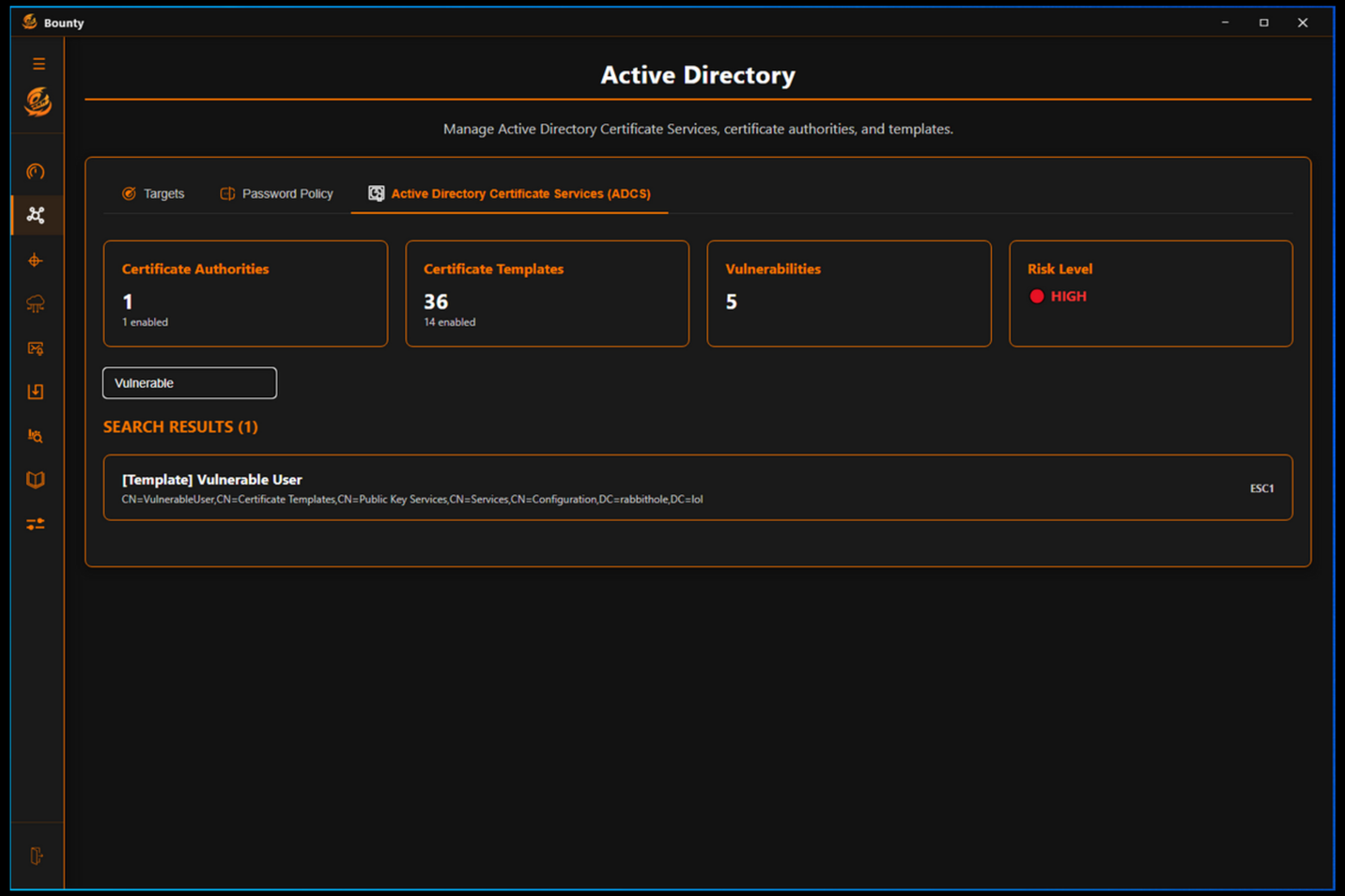
Template Vulnerability Detected
This certificate template has been identified as vulnerable to privilege escalation attacks.

Enrollable Users/Groups (4)

- Domain Users (Group)
- Domain Admins (Group)
- Enterprise Admins (Group)
- Authenticated Users (Well-Known)

Extended Key Usage (3)

- Client Authentication (1.3.6.1.5.5.7.3.2)
  1.3.6.1.5.5.7.3.2
- Email Protection (1.3.6.1.5.5.7.3.4)
  1.3.6.1.5.5.7.3.4
- Microsoft Encrypting File System (1.3.6.1.4.1.311.10.3.4)
  1.3.6.1.4.1.311.10.3.4


Bounty
Active Directory
Manage Active Directory Certificate Services, certificate authorities, and templates.
Targets
Password Policy
Active Directory Certificate Services (ADCS)
Certificate Authorities
1
1 enabled
Certificate Templates
36
14 enabled
Vulnerabilities
5
Risk Level
HIGH
Vulnerable
SEARCH RESULTS (1)
[Template] Vulnerable User
CN=VulnerableUser,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=rabbithole,DC=lol
ESC1

Evan Hosinski
KrakenTech LLC

10.03.2025

INFRASTRUCTURE

Evan Hosinski
KrakenTech LLC

10.03.2025

BOUNTY ENGINE

Evan Hosinski
KrakenTech LLC

10.03.2025

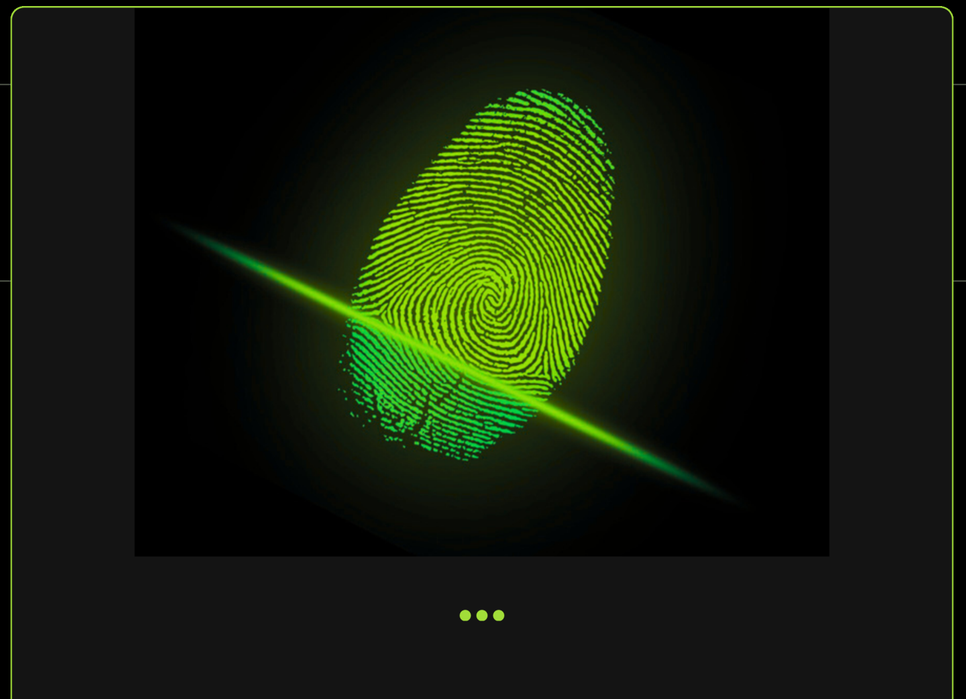
BY DESIGN

SECURITY

Evan Hosinski
KrakenTech LLC

10.03.2025

GROWING PAINS



Evan Hosinski
KrakenTech LLC

10.03.2025

THE LOOP

CRACK→TRACK→REACT

Evan Hosinski
KrakenTech LLC

10.03.2025

LESSONS LEARNED

Evan Hosinski
KrakenTech LLC

10.03.2025

THE TAKEAWAY

Evan Hosinski
KrakenTech LLC

10.03.2025

FINAL THOUGHTS

& CALL TO ACTION

Recap

You have the data you need to become more formidable

One small mistake can lead to a big breach

www.reallygreatsite.com

Take action today

Update passwords, stay informed, be alert

more information at:

https://krakensec.tech/tools/bounty