README

SMB Auto Enumeration

SMB RUNNER
Author: Sanalnadh M Kattungal
Envestnet - Offensive Security [RED TEAM]

SMB Auto Enumeration is a Python-based automated SMB enumeration tool designed with offensive security in mind. Tailored for **penetration testers** and **red team operators**, it streamlines the process of discovering and exploiting misconfigured SMB shares during internal network engagements.

The script intelligently detects the attacker's local subnet and scans for SMB services (`ports 139` and `445`) on live hosts. If anonymous access is allowed, it automatically enumerates accessible shares, downloads all exposed files, and recursively scans the dumped content for **sensitive information** using a curated set of regex patterns.

A detailed report is generated in `.txt` , `.json` , and `.html` formats for quick review or integration into larger reports.

SMB Auto Enumeration is fully **cross-platform** and runs seamlessly on both **Windows** and **Linux**, with built-in dependency handling.

USAGE

```
PS > python .\SMB_Auto_Enumeration.py
```

```
$ python ./SMB_Auto_Enumeration.py
```

REQUIREMENTS

1. Python

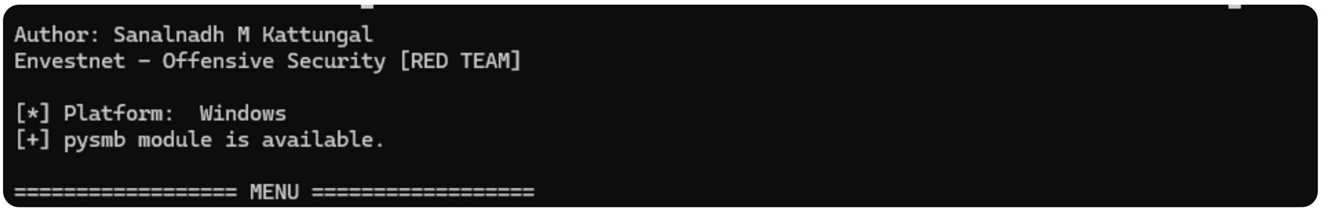
```
Install python on the attacker machine
```

2. pysmb
   The script will auto install the pysmb module, incase if the auto operation breaks, here is the commands to install the module manually.

```
# Windows
pip install pysmb

# Linux
python3 -m pip install pysmb --break-system-packages
```

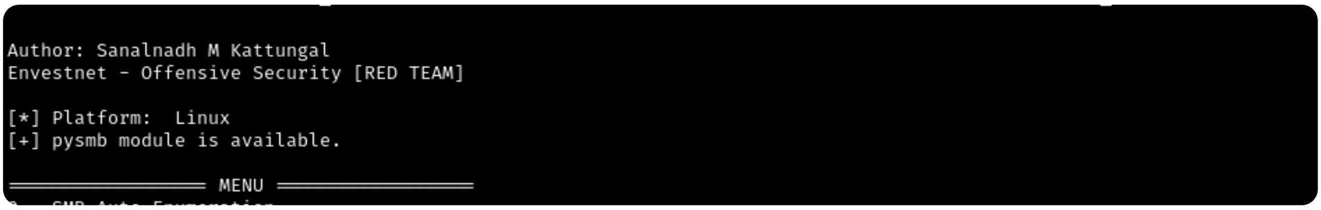
Platform - Attacker Machine

Windows as attacker machine



```
Author: Sanalnadh M Kattungal
Envestnet - Offensive Security [RED TEAM]

[*] Platform:  Windows
[+] pysmb module is available.

================== MENU ==================
```

Linux as attacker machine

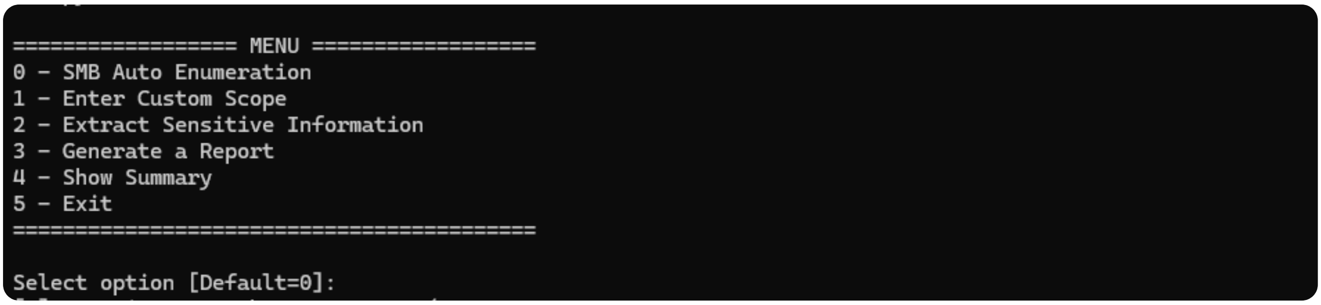


```
Author: Sanalnadh M Kattungal
Envestnet - Offensive Security [RED TEAM]

[*] Platform:  Linux
[+] pysmb module is available.

═══════════════ MENU ═══════════════
```

MENU OPTIONS

```
================== MENU ==================
0 - SMB Auto Enumeration
1 - Enter Custom Scope
2 - Extract Sensitive Information
3 - Generate a Report
4 - Show Summary
5 - Exit
```

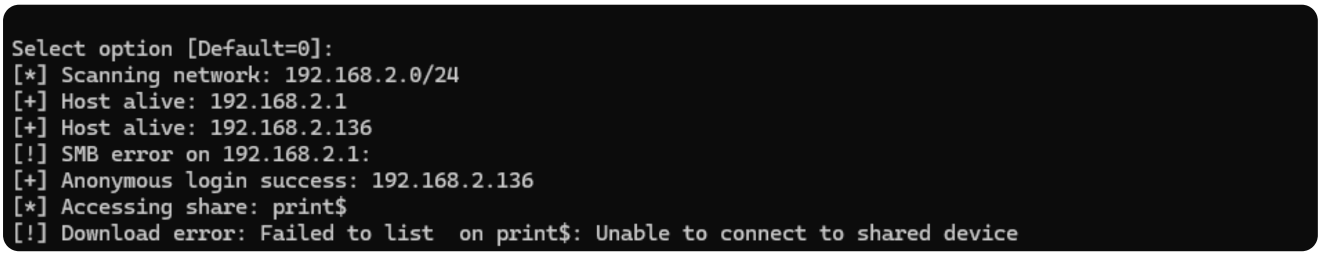
```
==========================================

Select option [Default=0]:
```



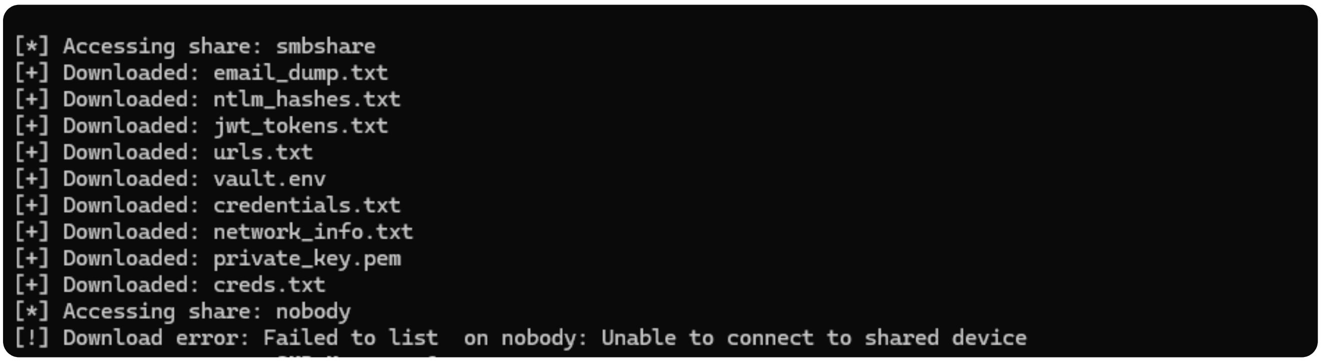
```
================== MENU ==================
0 - SMB Auto Enumeration
1 - Enter Custom Scope
2 - Extract Sensitive Information
3 - Generate a Report
4 - Show Summary
5 - Exit
==========================================

Select option [Default=0]:
```

0 - SMB Auto Enumeration

```
Select option [Default=0]:
[*] Scanning network: 192.168.2.0/24
[+] Host alive: 192.168.2.1
[+] Host alive: 192.168.2.136
[!] SMB error on 192.168.2.1:
[+] Anonymous login success: 192.168.2.136
[*] Accessing share: smbshare
[+] Downloaded: email_dump.txt
[+] Downloaded: ntlm_hashes.txt
[+] Downloaded: jwt_tokens.txt
[+] Downloaded: urls.txt
[+] Downloaded: vault.env
[+] Downloaded: credentials.txt
[+] Downloaded: network_info.txt
[+] Downloaded: private_key.pem
[+] Downloaded: creds.txt
```



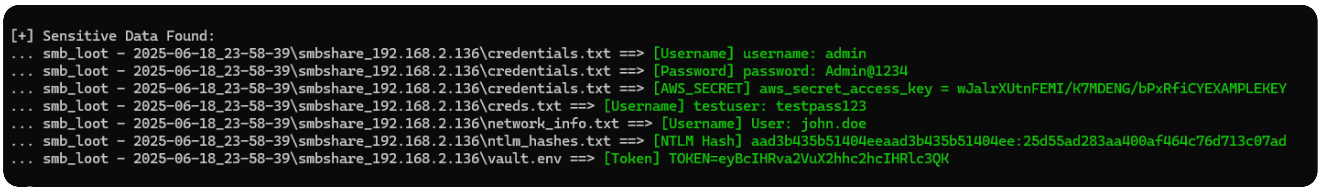
```
Select option [Default=0]:
[*] Scanning network: 192.168.2.0/24
[+] Host alive: 192.168.2.1
[+] Host alive: 192.168.2.136
[!] SMB error on 192.168.2.1:
[+] Anonymous login success: 192.168.2.136
[*] Accessing share: print$
[!] Download error: Failed to list  on print$: Unable to connect to shared device
```



```
[*] Accessing share: smbshare
[+] Downloaded: email_dump.txt
[+] Downloaded: ntlm_hashes.txt
[+] Downloaded: jwt_tokens.txt
[+] Downloaded: urls.txt
[+] Downloaded: vault.env
[+] Downloaded: credentials.txt
[+] Downloaded: network_info.txt
[+] Downloaded: private_key.pem
[+] Downloaded: creds.txt
[*] Accessing share: nobody
[!] Download error: Failed to list  on nobody: Unable to connect to shared device
```

2 - Sensitive Data Extraction

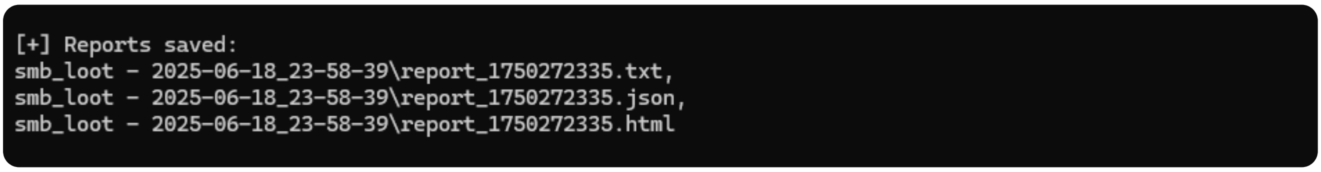
```
[+] Sensitive Data Found:
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt
==> [Username] username: admin
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt
==> [Password] password: Admin@1234
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt
==> [AWS_SECRET] aws_secret_access_key =
wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\creds.txt ==>
[Username] testuser: testpass123
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\network_info.txt
==> [Username] User: john.doe
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\ntlm_hashes.txt
==> [NTLM Hash]
aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\vault.env ==>
[Token] TOKEN=eyBcIHRva2VuX2hhc2hcIHRlc3QK
```



```
[+] Sensitive Data Found:
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt ==> [Username] username: admin
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt ==> [Password] password: Admin@1234
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt ==> [AWS_SECRET] aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\creds.txt ==> [Username] testuser: testpass123
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\network_info.txt ==> [Username] User: john.doe
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\ntlm_hashes.txt ==> [NTLM Hash] aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad
... smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\vault.env ==> [Token] TOKEN=eyBcIHRva2VuX2hhc2hcIHRlc3QK
```

3 - Report Generation

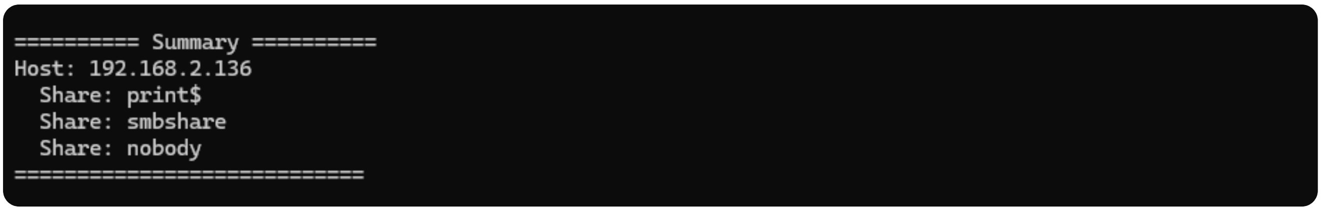
```
[+] Reports saved:
smb_loot - 2025-06-18_23-58-39\report_1750272335.txt,
smb_loot - 2025-06-18_23-58-39\report_1750272335.json,
smb_loot - 2025-06-18_23-58-39\report_1750272335.html
```



```
[+] Reports saved:
smb_loot - 2025-06-18_23-58-39\report_1750272335.txt,
smb_loot - 2025-06-18_23-58-39\report_1750272335.json,
smb_loot - 2025-06-18_23-58-39\report_1750272335.html
```

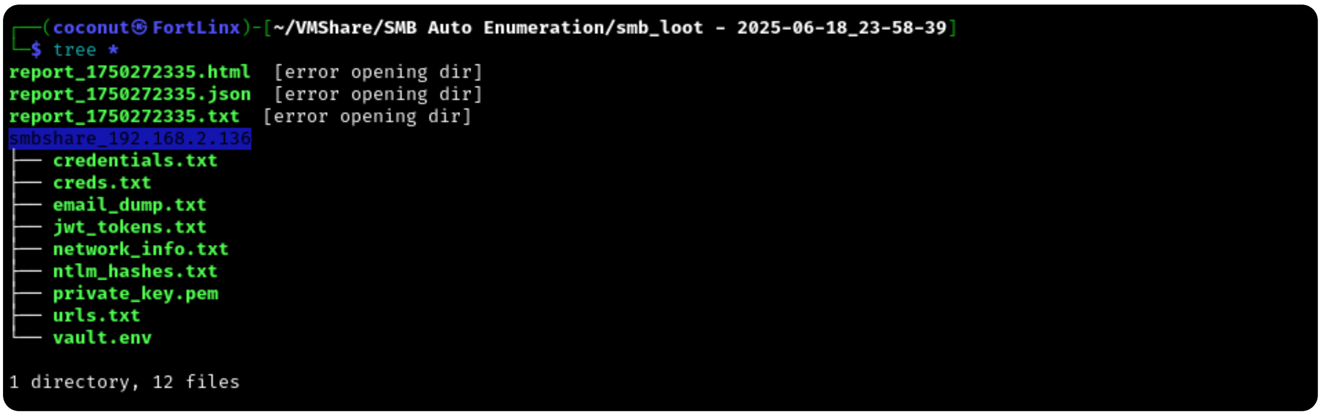
4 - Activity Summary

```
========== Summary ==========
Host: 192.168.2.136
  Share: print$
  Share: smbshare
  Share: nobody
============================
[*] Script finished. Exiting...
```



```
========== Summary ==========
Host: 192.168.2.136
  Share: print$
  Share: smbshare
  Share: nobody
============================
```

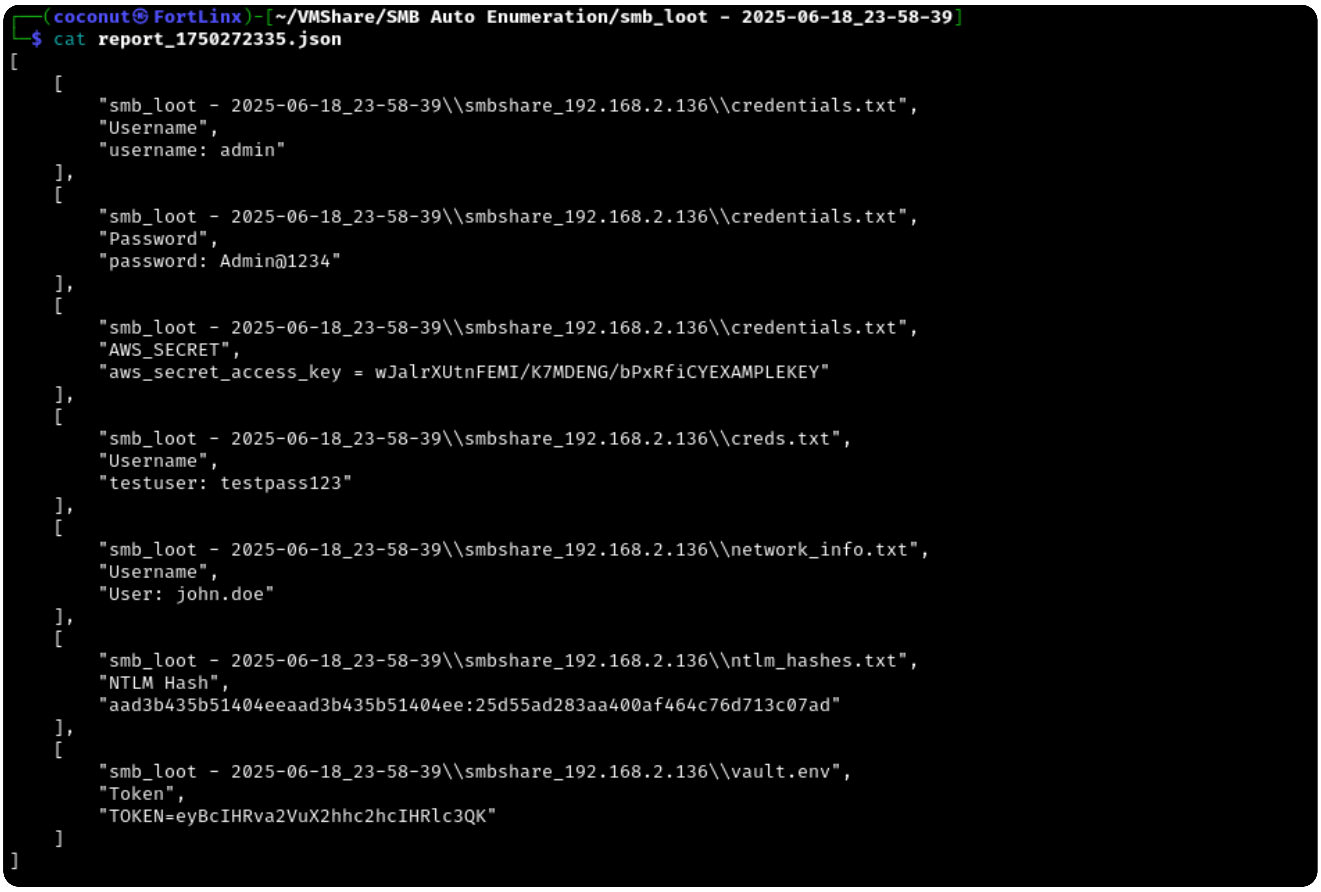
Contents in the Dump



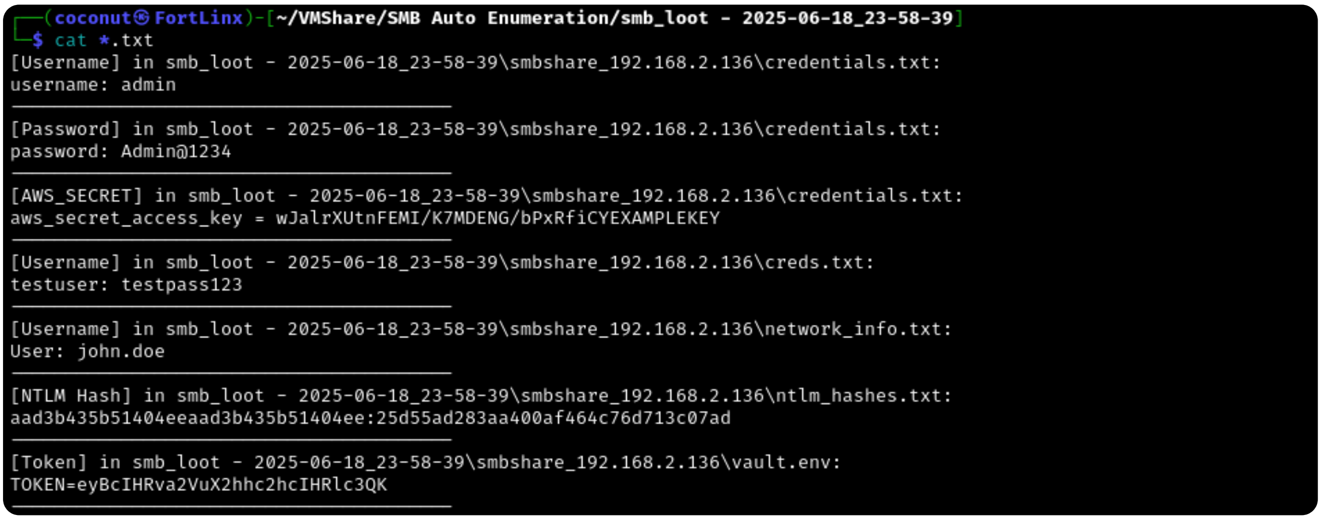
```
┌──(coconut㉿FortLinx)-[~/VMShare/SMB Auto Enumeration/smb_loot - 2025-06-18_23-58-39]
└─$ tree *
report_1750272335.html  [error opening dir]
report_1750272335.json  [error opening dir]
report_1750272335.txt  [error opening dir]
smbshare_192.168.2.136
├── credentials.txt
├── creds.txt
├── email_dump.txt
├── jwt_tokens.txt
├── network_info.txt
├── ntlm_hashes.txt
├── private_key.pem
├── urls.txt
└── vault.env

1 directory, 12 files
```

Reports Generated

```
[
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt", "Username", "username: admin"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt", "Password", "password: Admin@1234"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt", "AWS_SECRET", "aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\creds.txt", "Username", "testuser: testpass123"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\network_info.txt", "Username", "User: john.doe"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\ntlm_hashes.txt", "NTLM Hash", "aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad"],
    ["smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\vault.env",
  "Token", "TOKEN=eyBcIHRva2VuX2hhc2hcIHRlc3QK"]
  ]
```



```
┌──(coconut㉿FortLinx)-[~/VMShare/SMB Auto Enumeration/smb_loot - 2025-06-18_23-58-39]
└─$ cat report_1750272335.json
[
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt",
        "Username",
        "username: admin"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt",
        "Password",
        "password: Admin@1234"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\credentials.txt",
        "AWS_SECRET",
        "aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\creds.txt",
        "Username",
        "testuser: testpass123"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\network_info.txt",
        "Username",
        "User: john.doe"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\ntlm_hashes.txt",
        "NTLM Hash",
        "aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad"
    ],
    [
        "smb_loot - 2025-06-18_23-58-39\\smbshare_192.168.2.136\\vault.env",
        "Token",
        "TOKEN=eyBcIHRva2VuX2hhc2hcIHRlc3QK"
    ]
]
```



```
┌──(coconut㉿FortLinx)-[~/VMShare/SMB Auto Enumeration/smb_loot - 2025-06-18_23-58-39]
└─$ cat *.txt
[Username] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt:
username: admin
────────────────────────────────────────
[Password] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt:
password: Admin@1234
────────────────────────────────────────
[AWS_SECRET] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\credentials.txt:
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
────────────────────────────────────────
[Username] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\creds.txt:
testuser: testpass123
────────────────────────────────────────
[Username] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\network_info.txt:
User: john.doe
────────────────────────────────────────
[NTLM Hash] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\ntlm_hashes.txt:
aad3b435b51404eeaad3b435b51404ee:25d55ad283aa400af464c76d713c07ad
────────────────────────────────────────
[Token] in smb_loot - 2025-06-18_23-58-39\smbshare_192.168.2.136\vault.env:
TOKEN=eyBcIHRva2VuX2hhc2hcIHRlc3QK
────────────────────────────────────────
```