Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Sep 22 17:11:48 2025

[34m =========================================( [0m [32mTarget Information [0m [34m )=========================================

[0mTarget ........... 10.201.125.47

RID Range ........ 500-550,1000-1050

Username ......... ''

Password ......... ''

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[34m ===========================( [0m [32mEnumerating Workgroup/Domain on 10.201.125.47 [0m [34m )===========================

[0m [33m

[+] [0m [32mGot domain/workgroup name: WORKGROUP

[0m

[34m ===============================( [0m [32mNbtstat Information for 10.201.125.47 [0m [34m )===============================

[0mLooking up status of 10.201.125.47

BASIC2 <00> - B <ACTIVE> Workstation Service

BASIC2 <03> - B <ACTIVE> Messenger Service

BASIC2 <20> - B <ACTIVE> File Server Service

..\_\_MSBROWSE\_\_. <01> - <GROUP> B <ACTIVE> Master Browser

WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name

WORKGROUP <1d> - B <ACTIVE> Master Browser

WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

[34m ===================================( [0m [32mSession Check on 10.201.125.47 [0m [34m )===================================

[0m [33m

[+] [0m [32mServer 10.201.125.47 allows sessions using username '', password ''

[0m

[34m ================================( [0m [32mGetting domain SID for 10.201.125.47 [0m [34m )================================

[0mDomain Name: WORKGROUP

Domain Sid: (NULL SID)

[33m

[+] [0m [32mCan't determine if host is part of domain or part of a workgroup

[0m

[34m ==================================( [0m [32mOS information on 10.201.125.47 [0m [34m )==================================

[0m [33m

[E] [0m [31mCan't get OS info with smbclient

[0m [33m

[+] [0m [32mGot OS info for 10.201.125.47 from srvinfo:

[0m BASIC2 Wk Sv PrQ Unx NT SNT Samba Server 4.15.13-Ubuntu

platform\_id : 500

os version : 6.1

server type : 0x809a03

[34m =======================================( [0m [32mUsers on 10.201.125.47 [0m [34m )=======================================

[0m

[34m =================================( [0m [32mShare Enumeration on 10.201.125.47 [0m [34m )=================================

[0msmbXcli\_negprot\_smb1\_done: No compatible protocol selected by server.

Sharename Type Comment

--------- ---- -------

Anonymous Disk

IPC$ IPC IPC Service (Samba Server 4.15.13-Ubuntu)

Reconnecting with SMB1 for workgroup listing.

Protocol negotiation to server 10.201.125.47 (for a protocol between LANMAN1 and NT1) failed: NT\_STATUS\_INVALID\_NETWORK\_RESPONSE

Unable to connect with SMB1 -- no workgroup available

[33m

[+] [0m [32mAttempting to map shares on 10.201.125.47

[0m//10.201.125.47/Anonymous [35mMapping: [0mOK [35m Listing: [0mOK [35m Writing: [0mN/A

[33m

[E] [0m [31mCan't understand response:

[0mNT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND listing \\*

//10.201.125.47/IPC$ [35mMapping: [0mN/A [35m Listing: [0mN/A [35m Writing: [0mN/A

[34m ===========================( [0m [32mPassword Policy Information for 10.201.125.47 [0m [34m )===========================

[0m

[+] Attaching to 10.201.125.47 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

[+] BASIC2

[+] Builtin

[+] Password Info for Domain: BASIC2

[+] Minimum password length: 5

[+] Password history length: None

[+] Maximum password age: 37 days 6 hours 21 minutes

[+] Password Complexity Flags: 000000

[+] Domain Refuse Password Change: 0

[+] Domain Password Store Cleartext: 0

[+] Domain Password Lockout Admins: 0

[+] Domain Password No Clear Change: 0

[+] Domain Password No Anon Change: 0

[+] Domain Password Complex: 0

[+] Minimum password age: None

[+] Reset Account Lockout Counter: 30 minutes

[+] Locked Account Duration: 30 minutes

[+] Account Lockout Threshold: None

[+] Forced Log off Time: 37 days 6 hours 21 minutes

[33m

[+] [0m [32mRetieved partial password policy with rpcclient:

[0mPassword Complexity: Disabled

Minimum Password Length: 5

[34m ======================================( [0m [32mGroups on 10.201.125.47 [0m [34m )======================================

[0m [33m

[+] [0m [32mGetting builtin groups:

[0m [33m

[+] [0m [32m Getting builtin group memberships:

[0m [33m

[+] [0m [32m Getting local groups:

[0m [33m

[+] [0m [32m Getting local group memberships:

[0m [33m

[+] [0m [32m Getting domain groups:

[0m [33m

[+] [0m [32m Getting domain group memberships:

[0m

[34m ==================( [0m [32mUsers on 10.201.125.47 via RID cycling (RIDS: 500-550,1000-1050) [0m [34m )==================

[0m [33m

[I] [0m [36mFound new SID:

[0mS-1-22-1

[33m

[I] [0m [36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m [36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m [36mFound new SID:

[0mS-1-5-32

[33m

[I] [0m [36mFound new SID:

[0mS-1-5-32

[33m

[+] [0m [32mEnumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username '', password ''

[0mS-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)

S-1-5-21-2853212168-2008227510-3551253869-513 BASIC2\None (Domain Group)

[33m

[+] [0m [32mEnumerating users using SID S-1-22-1 and logon username '', password ''

[0mS-1-22-1-1000 Unix User\kay (Local User)

S-1-22-1-1001 Unix User\jan (Local User)

S-1-22-1-1002 Unix User\ubuntu (Local User)

[33m

[+] [0m [32mEnumerating users using SID S-1-5-32 and logon username '', password ''

[0mS-1-5-32-544 BUILTIN\Administrators (Local Group)

S-1-5-32-545 BUILTIN\Users (Local Group)

S-1-5-32-546 BUILTIN\Guests (Local Group)

S-1-5-32-547 BUILTIN\Power Users (Local Group)

S-1-5-32-548 BUILTIN\Account Operators (Local Group)

S-1-5-32-549 BUILTIN\Server Operators (Local Group)

S-1-5-32-550 BUILTIN\Print Operators (Local Group)

[34m ===============================( [0m [32mGetting printer info for 10.201.125.47 [0m [34m )===============================

[0mNo printers returned.

enum4linux complete on Mon Sep 22 17:18:12 2025