110,995 - Pentesting POP

Basic Information

Post Office Protocol (**POP**) is a type of computer networking and Internet standard **protocol** that extracts and retrieves email from a remote mail server for access by the host machine. **POP** is an application layer **protocol** in the OSI model that provides end users the ability to fetch and receive email (from here).

The POP clients generally connect, retrieve all messages, store them on the client system, and delete them from the server. There are 3 versions of POP, but POP3 is the most used one.

Default ports: 110, 995(ssl)

```
PORT    STATE SERVICE
110/tcp open  pop3
```

Enumeration

Banner Grabbing

```
nc -nv <IP> 110
openssl s_client -connect <IP>:995 -crlf -quiet
```

Manual

You can use the command `CAPA` to obtain the capabilities of the POP3 server.

Automated

```
nmap --script "pop3-capabilities or pop3-ntlm-info" -sV -port <PORT> <IP> #All are
```

The `pop3-ntlm-info` plugin will return some "**sensitive**" data (Windows versions).

POP3 bruteforce

POP syntax

```
POP commands:
  USER uid            Log in as "uid"
  PASS password       Substitue "password" for your actual password
  STAT                List number of messages, total mailbox size
  LIST                List messages and sizes
  RETR n              Show message n
  DELE n              Mark message n for deletion
  RSET                Undo any changes
  QUIT                Logout (expunges messages if no RSET)
  TOP msg n           Show first n lines of message number msg
  CAPA                Get capabilities
```

From here

Example:

```
root@kali:~# telnet $ip 110
 +OK beta POP3 server (JAMES POP3 Server 2.3.2) ready
 USER billydean
 +OK
 PASS password
 +OK Welcome billydean

 list

 +OK 2 1807
 1 786
 2 1021

 retr 1

 +OK Message follows
 From: jamesbrown@motown.com
 Dear Billy Dean,

 Here is your login for remote desktop ... try not to forget it this time!
```

```
username: billydean
password: PA$$W0RD!Z
```

Dangerous Settings

From https://academy.hackthebox.com/module/112/section/1073

Setting	Description
auth_debug	Enables all authentication debug logging.
auth_debug_passwords	This setting adjusts log verbosity, the submitted passwords and the scheme gets logged.
auth_verbose	Logs unsuccessful authentication attempts and their reasons.
auth_verbose_passwords	Passwords used for authentication are logged and can also be truncated.
auth_anonymous_username	This specifies the username to be used when logging in with the ANONYMOUS SASL mechanism.

HackTricks Automatic Commands

```
Protocol_Name:  POP   #Protocol Abbreviation if there is one.
Port_Number:  110     #Comma separated if there is more than one.
Protocol_Description: Post Office Protocol         #Protocol Abbreviation Spelled c

Entry_1:
  Name: Notes
  Description: Notes for POP
  Note: |
    Post Office Protocol (POP) is a type of computer networking and Internet standa
    The POP clients generally connect, retrieve all messages, store them on the cli

    https://book.hacktricks.xyz/pentesting/pentesting-whois

Entry_2:
  Name: Banner Grab
```

```
    Description: Banner Grab 110
    Command: nc -nv {IP} 110

  Entry_3:
    Name: Banner Grab 995
    Description: Grab Banner Secure
    Command: openssl s_client -connect {IP}:995 -crlf -quiet

  Entry_4:
    Name: Nmap
    Description: Scan for POP info
    Command: nmap --script "pop3-capabilities or pop3-ntlm-info" -sV -p 110 {IP}

  Entry_5:
    Name: Hydra Brute Force
    Description: Need User
    Command: hydra -l {Username} -P {Big_Passwordlist} -f {IP} pop3 -V

  Entry_6:
    Name: consolesless mfs enumeration
    Description: POP3 enumeration without the need to run msfconsole
    Note: sourced from https://github.com/carlospolop/legion
    Command: msfconsole -q -x 'use auxiliary/scanner/pop3/pop3_version; set RHOSTS {I
```


Previous
Harvesting tickets from Linux

Next - Network Services Pentesting
111/TCP/UDP - Pentesting Portmapper

Last modified 1mo ago