POP Enumeration

The Post Office Protocol (POP) is a widely used protocol for retrieving email messages from a remote server. POP servers often contain sensitive information about users, such as email addresses, usernames, and potentially even email contents.

Banner Grabbing

Lets start with banner grabbing with netcat

```
nc 10.10.177.29 110
```

Openssl

If the target is using the secure version of POP that is POPS. Then we can use the openssl utility to gather information from it.

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

Nmap Enumeration

Lets now perform enumeration of POP service using nmap.

```
sudo nmap -p 110,995 -sV 10.10.177.29

sudo nmap -p 143 -sV --script pop3-ntlm-info,pop3-capabilities
10.10.177.29
```

POP Version Enumeration with Metasploit

We can also use metasploit for POP version enumeration, Let us see how.

```
use auxiliary/scanner/pop3/pop3_version
set RHOSTS <TARGET>
run
```

Now let see what we can do if we have a little access on the POP server and how it can be abused to get a full control over the target.

Suppose, after enumerating the other services, we found a username and password combo. The username is seina and her password is scoobydoo2.

Now will be first log into the pop server.

```
$ telnet 10.10.102.132 110
Trying 10.10.102.132...
Connected to 10.10.102.132.
Escape character is '^]'.
+OK Welcome to the Fowsniff Corporate Mail Server!
USER seina
+OK
PASS scoobydoo2
+OK Logged in.
```

Once we are logged in, we will use the LIST command to list the number of messages. Here we can see there are 2.

```
LIST
+OK 2 messages:
1 1622
2 1280
.
```

Lets retrieve and read the first one, For that we will use the RETR command.

```
RETR 1
+OK 1622 octets
Return-Path: <stone@fowsniff>
X-Original-To: seina@fowsniff
Delivered-To: seina@fowsniff
Received: by fowsniff (Postfix, from userid 1000)
        id 0FA3916A; Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
To: baksteen@fowsniff, mauer@fowsniff, mursten@fowsniff,
    mustikka@fowsniff, parede@fowsniff, sciana@fowsniff, seina@fowsniff,
```

```
    tegel@fowsniff
Subject: URGENT! Security EVENT!
Message-Id: <20180313185107.0FA3916A@fowsniff>
Date: Tue, 13 Mar 2018 14:51:07 -0400 (EDT)
From: stone@fowsniff (stone)

Dear All,

A few days ago, a malicious actor was able to gain entry to
our internal email systems. The attacker was able to exploit
incorrectly filtered escape characters within our SQL database
to access our login credentials. Both the SQL and authentication
system used legacy methods that had not been updated in some time.

We have been instructed to perform a complete internal system
overhaul. While the main systems are "in the shop," we have
moved to this isolated, temporary server that has minimal
functionality.

This server is capable of sending and receiving emails, but only
locally. That means you can only send emails to other users, not
to the world wide web. You can, however, access this system via
the SSH protocol.

The temporary password for SSH is "S1ck3nBluff+secureshell"

You MUST change this password as soon as possible, and you will do so
under my
guidance. I saw the leak the attacker posted online, and I must say that
your
passwords were not very secure.

Come see me in my office at your earliest convenience and we'll set it up.

Thanks,
A.J Stone
```

See we got this email and in the email, we got the temporary password of the SSH server. Using this we can gain full control over the server.
