IMAP Enumeration

The Internet Message Access Protocol (IMAP) is a widely used protocol for accessing and managing email messages on a remote server. IMAP servers often contain sensitive information about users, such as email addresses, usernames, and potentially even email contents.

Banner Grabbing

Lets start with the banner grabbing with telnet and netcat

```
telnet 192.168.29.141 143

nc 192.168.29.141 143
```

OpenSSL

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

```
openssl s_client -connect 10.0.0.3:993
```

NTLM Disclosure

On Windows, with NTLM authentication enabled, sending a IMAP NTLM authentication request with null credentials will cause the remote service to respond with a NTLMSSP message disclosing information to include NetBIOS, DNS, and OS build version.

```
nmap -p 587 --script smtp-ntlm-info --script-args smtp-ntlm-
info.domain=example.com 10.0.0.3
```
