Phishing Emails 4

* Introduction
  + What is the MITRE ID for Software Configuration?
    - M1054
* Sender Policy Framework (SPF)
  + What is the SPF rule to use if you wish to ensure an operator rejects emails without potentially discarding a legitimate email?
    - v=spf1 ~all
  + What is the meaning of the -all tag?
    - Fail
* DomainKeys Identified Mail (DKIM)
  + Which email header shows the status of whether DKIM passed or failed?
    - Authentication-Results
    - Text

      Description automatically generated
* Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
  + Which DMARC policy would you use not to accept an email if the message fails the DMARC check?
    - p=reject
* Secure/Multipurpose Internet Mail Extensions (S/MIME)
  + What is nonrepudiation?
    - The uniqueness of a signature prevents the owner of the signature from disowning the signature.
* SMTP Status Codes
  + What wireshark filter can you use to narrow down the packet output using SMTP status codes?
    - Smtp.response.code
  + Per the network traffic, what was the message for status code 220?
    - <domain> Service ready
  + One packet shows a response that an email was blocked using spamhaus.org. What were the packet number and status code?
    - 156,553
  + Based on the packet from the previous question what was the message regarding the mailbox?
    - Mailbox name not allowed
  + What is the status code that will typically precede a SMTP DATA command?
    - 354
* SMTP Traffic Analysis
  + What port is the SMPT traffic using?
    - 25
  + How many packets are specifically SMTP?
    - 512
  + What is the source IP address for all the SMTP traffic?
    - 10.12.19.101
  + What is the filename of the third file attachment?
    - Attachment.scr
  + How about the last file attachment?
    - .zip
* SMTP and C&C Communication
  + Per MITRE ATT&CK, which software is associated with using SMTP and POP3 for C2 communications?
* Conclusion
  + Per the playbook, what framework was used for the IR process?
    - NIST