2. Phishing Analysis

I. Introduction to Phishing

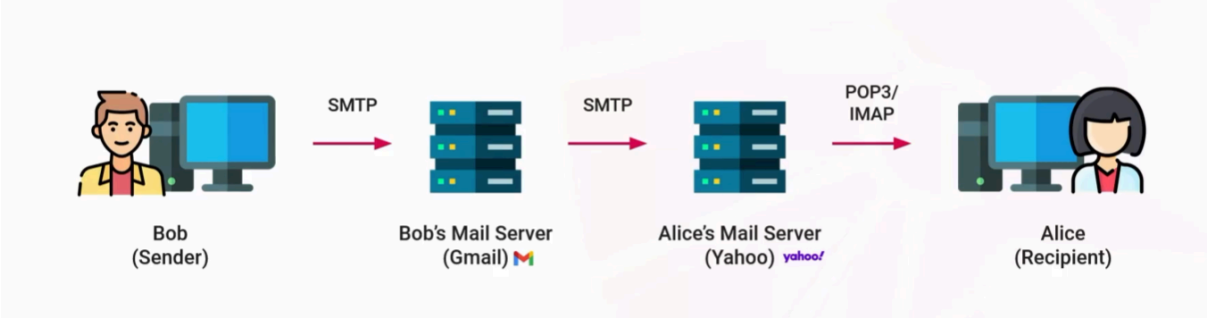
Phishing

- Impersonation
- Stealing sensitive info
- Deliver and install malware
- Exploiting humans

How Does Phishing Work?

- Authority
- Trust
- Intimidation
- Social Proof
- Urgency
- Scarcity
- Familiarity

II . Email Fundamentals



Sender -> Sender's Mail Server -> Receiver's Mail Server -> Receiver

Email Headers

- Lines of metadata
- Can be spoofed by attackers

Email Body

- Main content
- Visible to recipient

Email Address

Local Part (Mailbox) + Domain Part

Email Protocols

- SMTP
  - Simple Mail Transfer Protocol
  - Used to send outgoing mail
  - Port 25 (or 465, 587)
- POP3
  - Post Office Protocol (version 3)
  - Downloads emails, then deletes them
  - Port 110 (or 995)
- IMAP
  - Internet Message Access Protocol
  - Advanced email sync
  - Port 143 (or 993)

Mail Agents

- Mail Transfer Agent (MTA)
  - Route and transfer email messages across mail servers
  - Determine appropriate route and relays
- Mail User Agent (MUA)
  - Compose, send, receive, manage emails
  - Gmail, Outlook, Yahoo, Thunderbird
- Mail Delivery Agent (MDA)
  - Accepts incoming emails from MTAs
  - Places emails in recipients inbox
- Mail Submission Agent (MSA)
- Mail Retrieval Agent (MRA)

III. Phishing Attack Types

- Information Gathering
  - Collect data thru recon
  - Verify existing accounts
  - Craft credible phishes
- Credential Harvesting
  - Obtain login creds from victims
  - Fake login pages, deceptive URLs
- Malware Delivery
  - Malicious attachments or links
- Spear Phishing
  - Targeting and customized phishing
  - Research specific individuals or organizations
- Whaling
  - Targeting high-profile individuals
- Vishing, Smishing, Quishing
- Business Email Compromise (BEC)
  - Compromising legit email accounts
  - Unauthorized wire transfers, invoice scams
- Spam

IV. Phishing Attack Techniques

- Pretexting
  - Fabricate backstory
  - Manipulate under false pretense
- Spoofing and Impersonation
  - Email Address Spoofing
  - Domain Spoofing
- URL Manipulation
  - URL Shortening
  - Subdomain Spoofing
  - Homograph Attacks
  - Typosquatting
- Encoding
  - Obfuscating and evade detection
  - Dbase64, URL encoding, HTML encoding
  - Obscure JavaScript
- Attachments
  - Download and execute
- Abuse of Legit Services
  - Google Drive, Dropbox etc
  - Using trusted reputations to send malware
- Pharming
  - Two-step technique
  - Malware-based Pharming
  - DNS Server Poisoning

V. Phishing Analysis Methodology

1. Initial Triage
   a. Quickly assess and prioritize
2. Header and Sender Examination
   a. Investigate MTAs, addresses, IPs, etc
   b. Identify true origin and check authenticity
3. Content Examination
   a. Analyze email content for language, formatting, etc
   b. Look for social engineering red flags

4. Web and URL Examination
    a. Collect web artifacts
    b. Utilize tools to inspect URLs and domains
5. Attachment Examination
    a. Securely extract and analyze attachments
    b. Checking file reputation and sandboxing
6. Contextual Examination
    a. Consider broader context, recent or current incidents
    b. Look for patterns and assess scope
7. Defense Measures
    a. Take reactive defense actions (if needed)
    b. Take proactive defense actions
    c. Communicate with users and stakeholders
8. Documentation and Reporting
    a. Maintain records of findings, verdicts, and actions taken through detailed reports
    b. Close out alerts and tickets

VI. Email Header and Sender Analysis

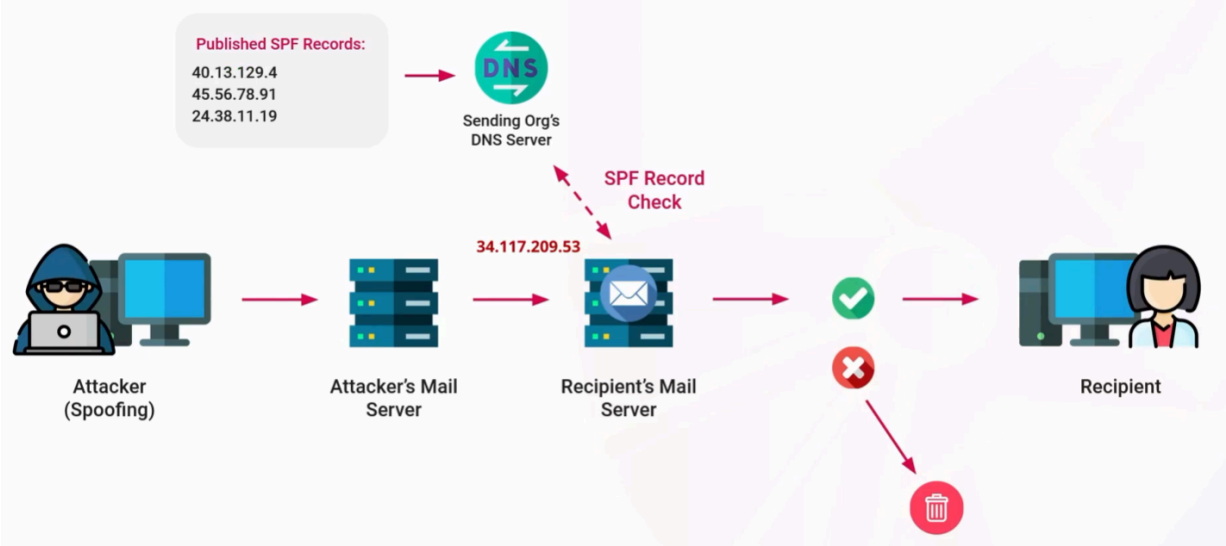
- `Date`
    - Date the email was sent
- `From`
    - Supposed sender
    - Easily spoofed
- `Subject`
    - Can be used to fingerprint an email
- `Message-ID`
- `To`
- `Reply-To`
    - Email that replies go to
- `Return-Path`
    - Email address for bounce-backs
- `X-Sender-IP`
    - Origin IP address
- `Received`
    - There are often multiple Received headers
    - Each email server adds another Received message

- Cant be spoofed
- "passport" for email message
- Reverse chronological order
- Find origin IP address
- Can whois the IP

Use Email Header Tools to parse email header

VII. Email Authentication Methods

SPF - Sender Policy Framework



Allows domain owners to authorize which mail servers are allowed to send emails on behalf of their domain.

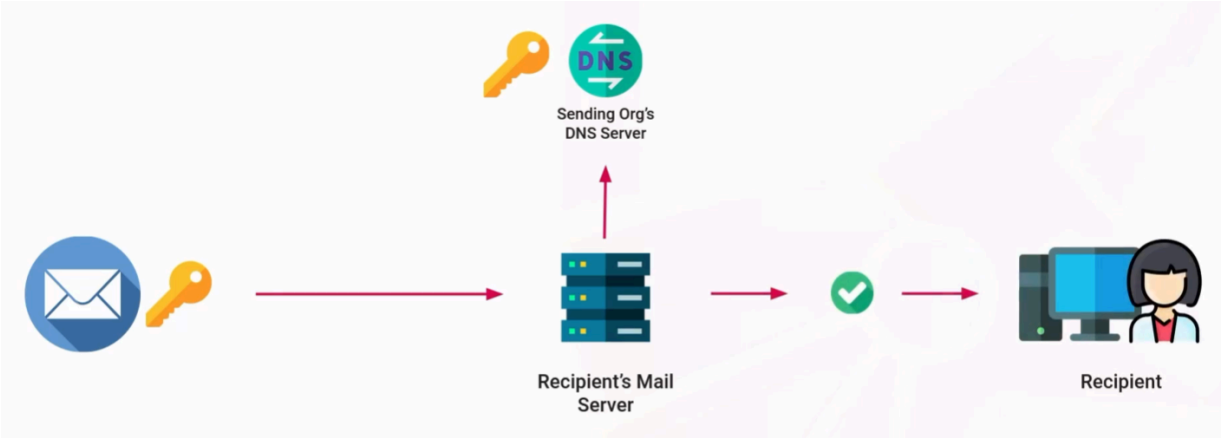
```
nslookup -type=txt shodan.io | grep -i spf
```

```
dig TXT shodan.io | grep -i spf
```

`-all` means it only allows the server IPs listed.
`~all` means allow other servers but treat with suspicion.

SPF by itself is not secure and can be spoofed by attackers.

DKIM - Domain Key Identified Mail



Method to authenticate the origin of an email. Allow receiver to verify email comes from where it claims to come from. Includes a digital signature based on PKI.

DMARC - Domain-based Message Authentication, Reporting, and Conformance

Used to specify policies for how to handle an email message if SPF or DKIM checks fail.

- none
- quarantine
- reject

VIII. Email Content Analysis

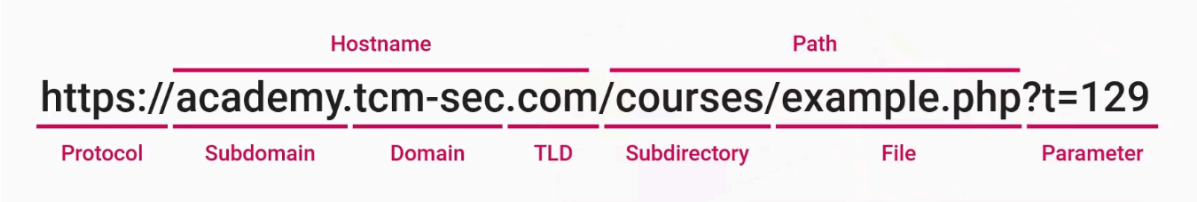
Email can use boundary strings to separate different parts of the email body.
Emails can designate separate views for text-only vs HTML email formats.

Red Flags:

- Induced Sense of Urgency
- Typo in Company Name
- Uses generic language instead specific information (Dear Customer instead of Dear [Name])

- AI can generate convincing text with no errors. Don't trust a lack of grammar mistakes
- Base64 and HTML Entity Encoding is sometimes used

IX. Anatomy of a URL



X. Email URL Analysis

Methodology

1. Collect URL artifacts
2. Check reputation with tools
3. Determine how to handle URL

Finding URLs in Emails

1. Open in Sublime Text Editor
    a. Open the `.eml` file in Sublime to view the header information easily. Can also use the built-in search feature to find specific elements in the page.
2. Open in CyberChef
    a. Useful Recipes:
        i. `From Quoted Printable`
        ii. `Extract URLs`
        iii. `Defang URL`

URL Analysis Tools

1. URL2PNG
    a. https://www.url2png.com/
    b. Take a screenshot of a website without visiting it:
2. urlscan
    a. https://urlscan.io/
    b. Use this to analyze web pages
3. Virustotal
    a. https://virustotal.com/gui/home/url
    b. URL Scanner

4. urlvoid
    a. https://urlvoid.com
    b. Website Reputation Checker
5. Wannabrowser
    a. https://www.wannabrowser.net
    b. Browser simulator
6. URLhaus
    a. https://urlhaus.abuse.ch
    b. Collection of malicious URLs

Additional Analysis

Scan the base URL as well as the subdomain URL.
Scrutinize subdirectories in the URL

XI. Static Attachment Analysis

Collect the Attachments

1. Manual
    a. Right Click > Save As
2. Automated
    a. Use `emldump.py` to collect attachments in an email file via command line

Generate Hashes

File Hashes can be used to search for previously discovered malicious files.

```
sha256sum <attachment.ext>
sha1sum <attachment.ext>
md5sum <attachment.ext>
```

```
get-filehash .\<attachment.ext>
get-filehash .\<attachment.ext> -algorithm md5
get-filehash .\<attachment.ext> -algorithm sha1
```

Check File Hash Reputation

XII. Dynamic Attachment Analysis and Sandboxing

Sandboxing is opening the attachment in a safe VM. Can be used to document the behavior of the file

1. Process Activity
2. Registry Activity
3. Network Activity
4. File Activity (Disk Activity)

Upload to https://www.hybrid-analysis.com
joesandbox.com

Virustotal - only upload hashes, not actual files (Confidentiality)

Basically: Just run in a sandbox and see what happens

XIII. Static MalDoc Analysis

```
oledump.py
```

```
oledump.py sample1.xlsm -s 4 --vbadecompresscorrupt
```

XIV. Static PDF Analysis

XV. Automated Email Analysis with PhishTool

https://www.phishtool.com

Drag and drop `.eml` files to begin analysis

Integrate with VirusTotal via API key

XVI. Reactive Phishing Defense

- Containment
  - Determine scope
  - Quarantine
  - Block sender artifacts
  - Block web artifacts
  - Block file artifacts
- Eradication
  - Remove malicious emails
    - Content search and discovery
  - Remove malicious files
  - Abuse form submissions
  - Credential changes
  - Reimaging
- Recovery
  - Restore systems
- Communication
  - Notify affected users
  - Update stakeholders
- User Education
  - End-user training

XVII. Proactive Phishing Defense

- Email Filtering
  - Email security appliances
  - Marking external emails
- URL Scanning and Blocking
  - Real-time URL inspection
  - Block recently registered domains
- Attachment Filtering
  - File extension blocks
  - Attachment sandboxing
- Email Authentication Methods
  - SPF
  - DKIM

    - DMARC
- User Training
    - Security Awareness Training
    - Phishing simulation exercises
    - Reporting functionality

XVIII. Documentation and Reporting

Template:

```
Phishing Analysis Report Template

Headers
====================================
Date:
Subject:

To:
From:

Reply-To:
Return-Path:

Sender IP:
Resolve Host:

Message-ID:


URLs
=====================================



Attachments
====================================
Attachment Name:
MD5:
SHA1:
SHA256:
```

Description

Artifact Analysis

Sender Analysis:

URL Analysis:

Attachment Analysis:

Verdict

Defense Actions