Global Information Security Society for Professionals of Pakistan

Topic : Email Security Simplified – Lesson 2

Speaker’s Name : Shahzad Subhani

Agenda

- Email Attacks Types
  - Email Relaying
  - Email Spam
  - Email Malware/Ransomware
  - Email Spoofing/Phishing/Spear Phishing
  - Email Impersonation
  - Email Dos/DDos Attacks

Assumptions OR Pre Requisites

- Basic Knowledge about How SMTP Protocol
- Basic Knowledge on How Email Works
- Basic Knowledge about SMTP Error Codes
- Basic Knowledge about SMTP DNS Records
- Basic Knowledge about Email Troubleshooting

Email Attack Types

- Email Relaying
- Spam/Unwanted Emails/Marketing Emails/Newsletters
- Malware (Viruses/Worms/Trojans/Spyware/Ransomware)
- Spoofing (People Sending you email from Spoofed Domains)
- Phishing/Spear phishing
- Impersonation (Other People sending email on your behalf)
- Dos/DDOs (DoS stands for Denial of Service)

Email Relaying

- Email Relay means Sending Emails though an SMTP Server
- Email Relay becomes an attack if attacker uses your SMTP Server to relay emails to another Domain ,without your knowledge
- A Very common attack in early days of SMTP
- Worms OR Trojans using misconfigured Company Servers to send emails
- Most Servers are Configured and Well Protected by default

Email Relaying Example

- Go to Mxtoolbox.com and do Mx lookup for any domain e.g. gmail.com
- Click on SMTP Test. Mxtoolbox Servers will try to test the Servers and give this kind of report .

	Test	Result
!	SMTP Banner Check	Reverse DNS does not match SMTP Banner
✓	SMTP Reverse DNS Mismatch	OK - 172.217.222.27 resolves to qi-in-f27.1e100.net
✓	SMTP Valid Hostname	OK - Reverse DNS is a valid Hostname
✓	SMTP TLS	OK - Supports TLS.
✓	SMTP Connection Time	0.163 seconds - Good on Connection time
✓	SMTP Open Relay	OK - Not an open relay.
✓	SMTP Transaction Time	0.538 seconds - Good on Transaction Time

Email Relaying Example

- Connecting to 172.217.222.27

220 mx.google.com ESMTP e1si6017776qki.686 - gsmtp [112 ms]
EHLO keeper-us-east-1c.mxtoolbox.com
250-mx.google.com at your service, [18.205.72.90]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8 [122 ms]
MAIL FROM:<supertool@mxtoolboxsmtpdiag.com>
250 2.1.0 OK e1si6017776qki.686 - gsmtp [121 ms]
RCPT TO:<test@mxtoolboxsmtpdiag.com>
550-5.1.1 The email account that you tried to reach does not exist. Please try
550-5.1.1 double-checking the recipient's email address for typos or
550-5.1.1 unnecessary spaces. Learn more at
550 5.1.1 https://support.google.com/mail/?p=NoSuchUser e1si6017776qki.686 - gsmtp [123 ms]

Email Relaying Prevention Tips

- Configure your Email Server/Gateway to receive Incoming Emails only for your Domains
- For outbound Emails , only allow authorized IP Addresses to relay emails
- Port 25 Access to Email Gateway OR Email Server should be given to selected IP Addresses only

Email Spam

- Any Kind of Promotional , Unwanted Email, Marketing Email is considered as Spam . Most common example is drug related spam
- Every Organization receives and blocked hundreds of Spam emails every day
- People use corporate account on different sites , Their Email addresses gets stolen and then used by spammers /Newsletters Spam
- Emails with too much graphics or Short URLs are also classified as Spam by many Email Gateways

Tips

- Always keep looking for False Positives as some good emails are marked a spam as well . Such domains or senders can be whitelisted
- Block all emails from Google Groups or other Mailing lists as people should not use corporate accounts for mailing lists

Email Malware/Ransomware

- Very Common Attack
- Executable files are sent over email OR
- links are sent in email bodies and user is enticed by subject OR key words to click on it
- Executables extensions are changed to doc or xls or anything benign
- Excel OR word documents are sent with hidden malicious macros in it
- Think twice before clicking on a Link especially if you are not expecting such email

Email Malware/Ransomware Prevention

- Always block Executables however some time executables extensions are changed to doc or xls or anything benign
- If your Email Gateway Supports , remove macros OR any codes from incoming PDF, Word and Excel Files . In Symantec Messaging Gateway , they provide such Option as DISARM .
- Email Gateways that identify True File Type can detect and Block Such Emails however emails with URLs can skip through if email gateway is not able to check URL so you need to add another layer of sandboxing
- User Awareness is very Important and they need to think twice before clicking on a Link especially if they are not expecting such email

Email Spoofing/Phishing

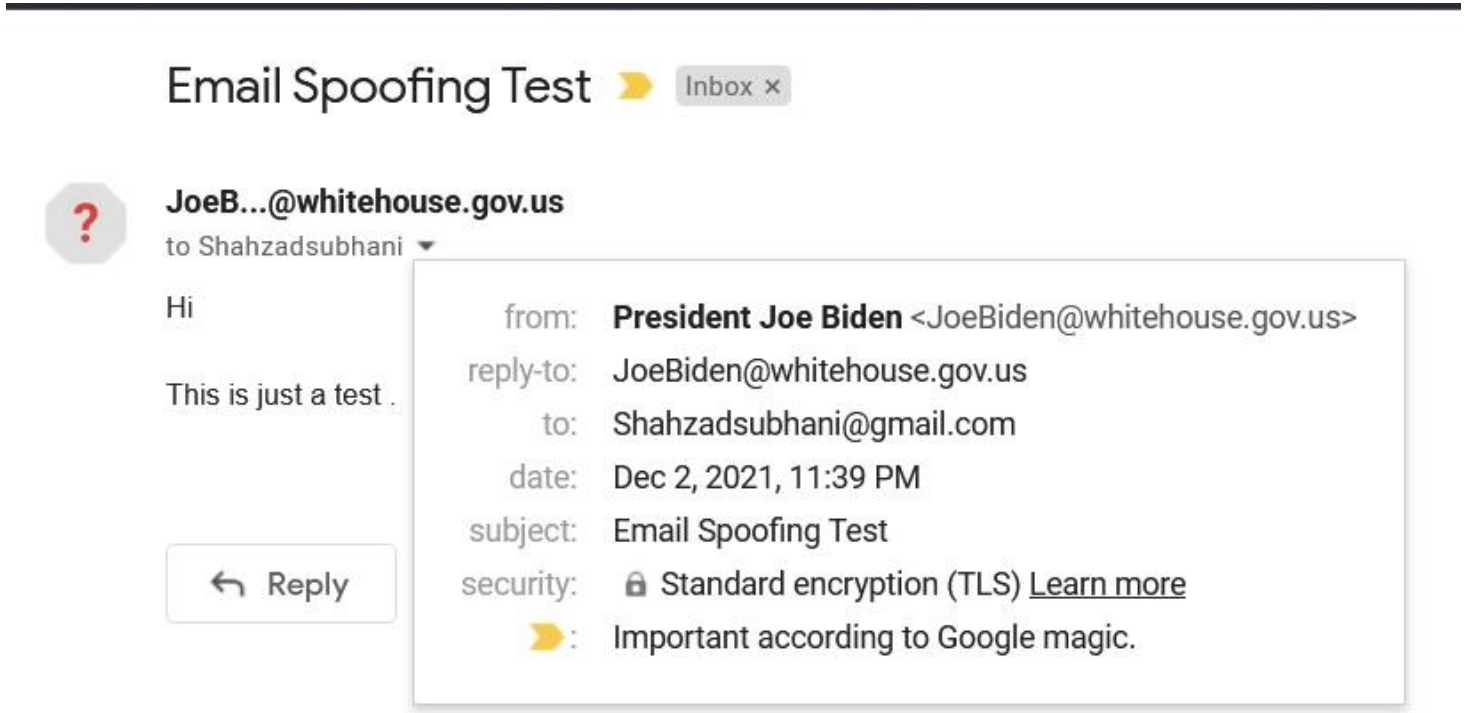
- Spammer/Attacker sends an email that has been manipulated to seem as if it originated from a Trusted Source .
- To put it simply , People are sending your email from baddomain.com but it appears to you as gooddomain.com
- Spoofed email can be used to get the user click on a link OR an email from CEO to a CFO asking for an Urgent Wire Transfer (Google Business Email Compromise Attack)
- Spoofing is done to hide the real identity of attacker and is mostly used as part of a Phishing attack
- Phishing occurs when attacker sends a fraudulent email disguised as an authorized and trusted source.
- Intent of email is to get personal or financial information OR trick the recipient into installing malware on his/her device
- EHLO name is different however FROM , REPLY-TO and RETURN-PATH are spoofed and User Email Client shows Spoofed FROM

Spear Phishing

- Spear phishing is a highly targeted phishing attack.
- Phishing and Spear phishing both use emails to reach the victims .
- However Spear-phishing sends customized emails to specific person/organization and criminal researches the target's interests before sending the email
- In some real world scenarios , some organizations OR their employees are hacked and then emails are sent from those organizations to their Partner Organizations .
- Due to email coming from a trusted organization , Chances of clicking on a link OR opening an attachment is very high .

Email Spoofing Example

- Sent via https://emkei.cz (Just do a google search on Online Email Spoofing)



Email Spoofing/Phishing Prevention Tips

- For Inbound Traffic , Configure your Email Gateway to check for the following
  - Use Local/Global IP Reputation Lists to block or defer at connection level
  - Use DNS Validation and Reject connections for IP Address which do not have Reverse DNS Record
  - You can also Reject connections where the reverse DNS record exists for the connecting IP address, but the 'A' or 'AAAA' record of the resulting domain does not match the connecting IP address
  - Check if EHLO/HELO Name is real OR fake by checking if the domain provided at HELO and EHLO has neither an 'A', nor an 'AAAA', nor an 'MX' record in DNS
  - Reject messages where the domain provided in the MAIL FROM address has neither an 'A', nor an 'AAAA', nor an 'MX' record in DNS
  - Configure Spoofing checks if there is a mismatch between Envelope Sender (MAIL FROM) and FROM Address . Envelope Sender is the address used at Email Handshake Level (MAIL FROM)
- Most Mailing Lists used different Envelope Sender and FROM . You need to start making exceptions else they will be blocked as Spoofed emails .
- Caution : DNS Checks at handshake level can impact System Performance so you need to find a good balance

Email Impersonation

- Email Impersonation means abc.com sending emails to someone.com as xyz.com .
- This is happening out of your Network so you don’t have much control however there is a way .

TIPS

- Impersonated emails can be prevented by adding Trust to your Outgoing emails
- Trust can be added to the Organization's outgoing emails by using a combination of SPF, DKIM and DMARC .
- Incoming Emails should be checked for SPF and DMARC Failures

Email DoS/DDoS Attacks

- An Email DoS Attack means that attackers send you so much emails that your Email Servers are not able to handle the load and crash. As a result , you should not be able to receive any legitimate business emails .
- Such Attack can be used to cause business/reputation Loss especially if the organization business is conducted via emails
- These attacks are not very common however there is still a possibility
- Such Attacks can be easily prevented by following
  - Limit number of maximum connections to be handled by your MTA
  - Limit number of connection per IP Address
  - Limit number of recipients for each email
  - Limit number of messages/emails sent in one session
  - Define a queue size and defer connections when your inbound queue is full
  - Use Local/Global IP Reputation Lists to block or defer connections at connection level