Raj Mehta CNS
TE IT B 26

~~Experimental~~ Assignment No. 1

1) This is a joint alert from the US Department of Homeland security (DHS). Cybersecurity and infrastructure security Agency ((ISA) and the UK's National cyber security centre (NCSC).
This alert provides Information on exploitation by cybercriminal and advanced persistent thread (APT) groups of the current coronavirus disease 2019 ((OVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.
Both CISA and NCSC are seeing agrowing use of COVID-19 related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services such as VPNs amplifying the threat to individuals and organizations.
APT groups and cybercriminals are targeting individuals, Small and medium enterprises and large organizations with COVID-19 - related scams and phishing emails. This alert provides an overview of COVID-19 related malicious cyber activity and ~~offers~~ practical advice that individuals and organizations can follow the risk of being impacted.
The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC and industry.
Phishing using the subject of coronavirus or covid-19 as a lure,
Malware distribution using coronavirus or COVID-19 themed lures.

Registration of new domain names containing wording related to corona virus or COVID-19 and Attack against newly and often rapidly-deployed remote access.

2) Implement End-to-End encryption
Encrypt emails at rest and in transit: Ensure that email commonication between servers and clients is encrypted using TLS.

Step1: Obtain an S/MIME Digital certificate
Get a digital certificate.
visit a certificate authority like sectingo, Digicert, or SSL.com.
Apply for a free or trial S/MIME certificate for your email address.

Step2: configure the Email client for S/MIME
For microsoft outlook:
Install the certificate:
Open the windows certificate manager by typing certmgr.msc into Run dialog.

Step3: For Mozilla Thunder bird:
Install the certificate.
open Thonderbird and go-to tools > Acc settings > security.

Step4: Sending a digitally signed Email
compose a new mail
open your email client and click new Email to start composing email..
sign the email.
when yousend the email the reciepent will see that he have email digitally signed.

Step5: Sending an encrypted email
Exchange digital certificates with the receipient must have exchanged digital certificates.
Ask the recipient to send you a digitally signed email, their certificate will be automatically stored in your contacts

Step6: verifying the digital signature and encryption
check for the signature.
In outlook a "signed by [email address]" notice will appear and clicking on it will show details.

3) Packet sniffing with tcpdump
Eg of how tcpdump could be used be used on Linux device:

- First create a file for dumping all of info that will be produced by tcpdump:

```
touch tcpdumpfile
chmod tcpdump >tcpdumpfile
```

- sudo strings tcpdumpfile | more

If you wanted to see your password in tcpdump
strings tcpdumpfile | grep -i password.
Hit <ctrl-c> in the terminal window to stop.

4) Ports most frequently used to carry out an attack are 22, 80 and 443 which correspond to SSH, the HTTP and HTTPS
Port 80 and 443 are ports generally associated with the "the internet". Port 443/HTTPS is the HTTP protocol over TLS/SSL. Port 80/HTTP is the world wide web. A remote attackers could 'exploit this vulnerability to bypass security restrictions and gain unauthorized access to vulnerable application.
Hackers can exploit port 22 by using leaked SSH keys or brute forcing. SSH is one of the most common protocols in use in modern IT infrastructures.

5) The server looks into the packet and checks the port number. The port numbers in this case is TCP port 443 for SSL. HTTPS uses SSL for communication, so the packet would be allowed acess the firewall.