RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

Session ID: HUM-T09

Breaking In Is Easy—Breaking Bad Habits Is HARD!

Jayson Street
InfoSec Ranger
Pwnie Express
@jayson@pwnieexpress.com

#RSAC

Legal Disclaimer

(I’m the one who doesn’t knock)

#whoami

@jayonstreet V3rb0t3n.com dissectingthehack.com awkwardhugs.org

You keep using that word. I do not think it means what you think it means.

Everyone keeps repeating the term
Advance Persistent Threats like a broken record!

Why not throw some love to Basic Adorable Destruction?!?

We all know how easy it is to just be BAD!

The key indicators of a person doing BAD

1. RECON Mode is only about 2 hours of Google & Victim's own website. (Though I've never used the full 2 hours yet)

2. Social Engineering Mode is usually walking into victims location and winging it (note sometimes without doing #1)

3. Pwnage Mode is basically plugging in a device to the victims computer or network (sometimes with their help)

4. ????

5. Profit!?!

So let’s break down the 3 best approaches I’ve used to be BAD

1.Tech, Repair Guy, Delivery, Job Applicant, Customer, Wanderer

2.Auditor, Executive, Policy Enforcement

3.Crazy Off The Wall Personalities (Not recommended but totally fun and usually work)

Story Time

The Beirut Bank Job!

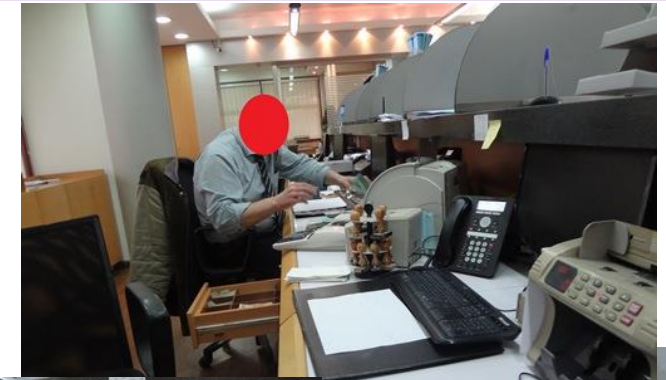
@hackerstrip

http://hackerstrip.com

The Beirut Bank Job!

Time from 1st walk into door to full access to bank.
= 2 minutes & 22 seconds

The Beirut Bank Job!



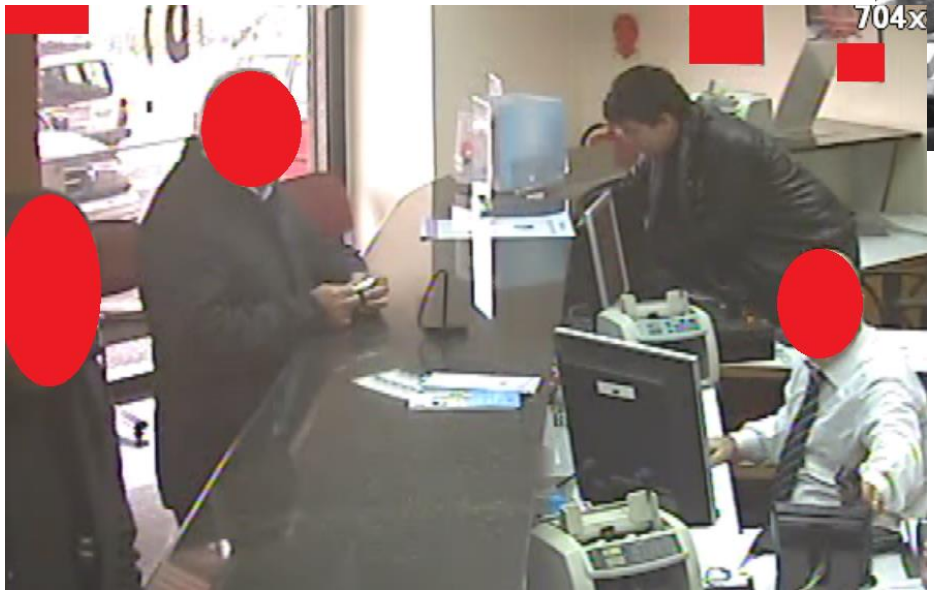
The Beirut Bank Job!

So I have the employee ID, password & smart card! Now I need their PC and Network access

I was there doing BAD things for over TWENTY MINUTES! WITHOUT BEING STOPPED!

The Beirut Bank Job!

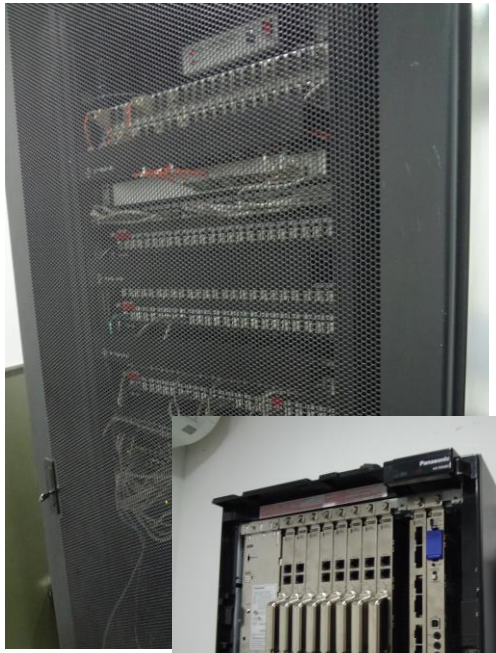
Well I needed a computer!



The Beirut Bank Job!

Well I got a computer!

The Beirut Bank Job!



Last I needed access to their internal network!..... OK DONE!

Sad State of Security at the State Treasury

Sad State of Security at the State Treasury

Rules of Engagement

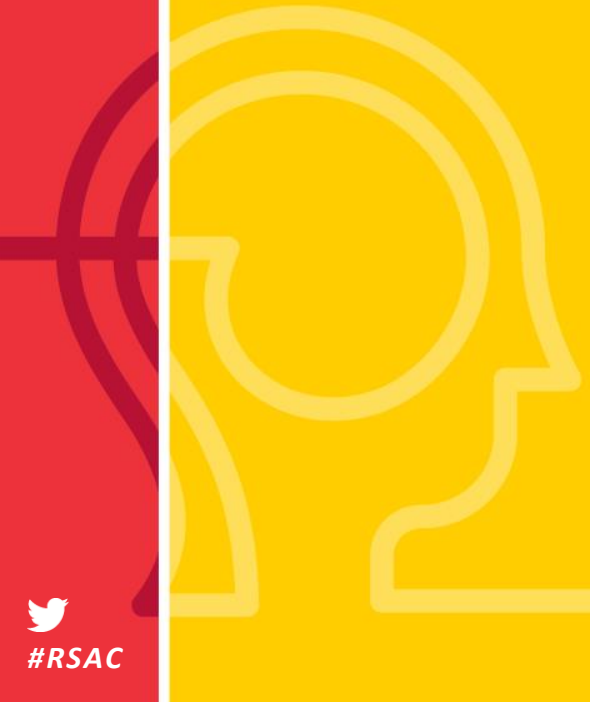
1.Talk to no one coming in or out of the building.

2. Only stay in the public areas if you do get in.

3. You can only talk to the cleaners but you are not allowed to lie to them!

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center



#RSAC

How did that work out for them?!?

Attacks that make you go…huh?!

Barefoot & Bad…. Also successful!

Barefoot & Bad…. Also successful!

Target – One of the most prestigious hotels in Southern France

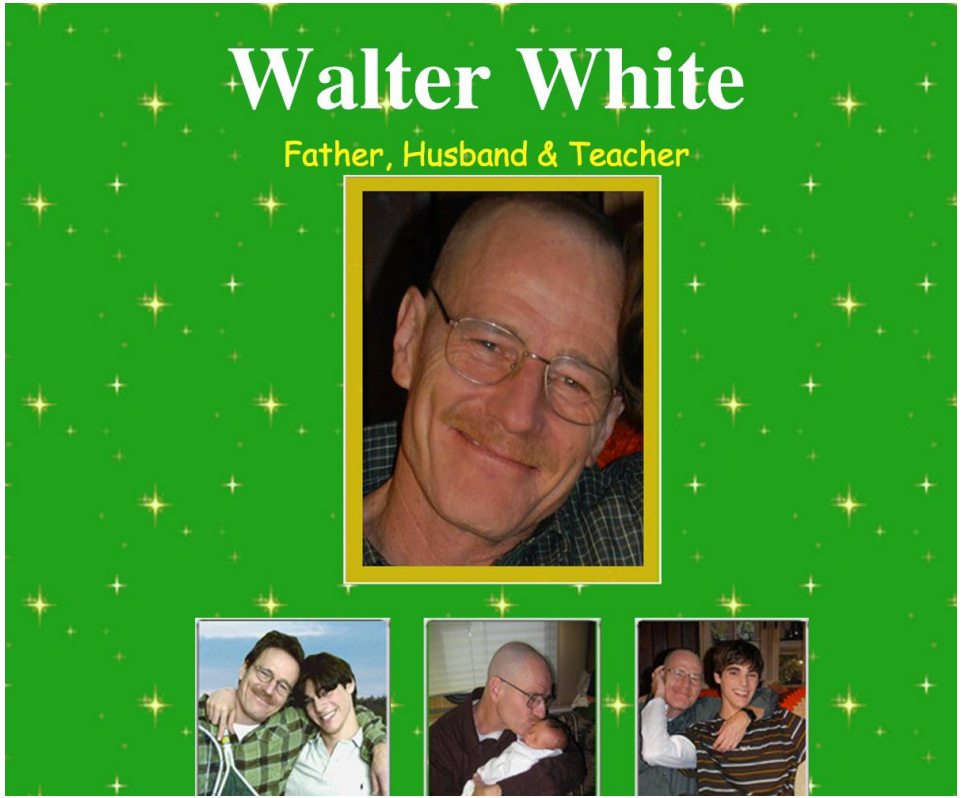
Pretext – Drunk hotel guest who was jetlagged.

Barefoot & Bad…. Also successful!

Outcome – Total compromise of the entire hotel!

Results – Client learned to treat guest with some suspicion not just respect!

Summary



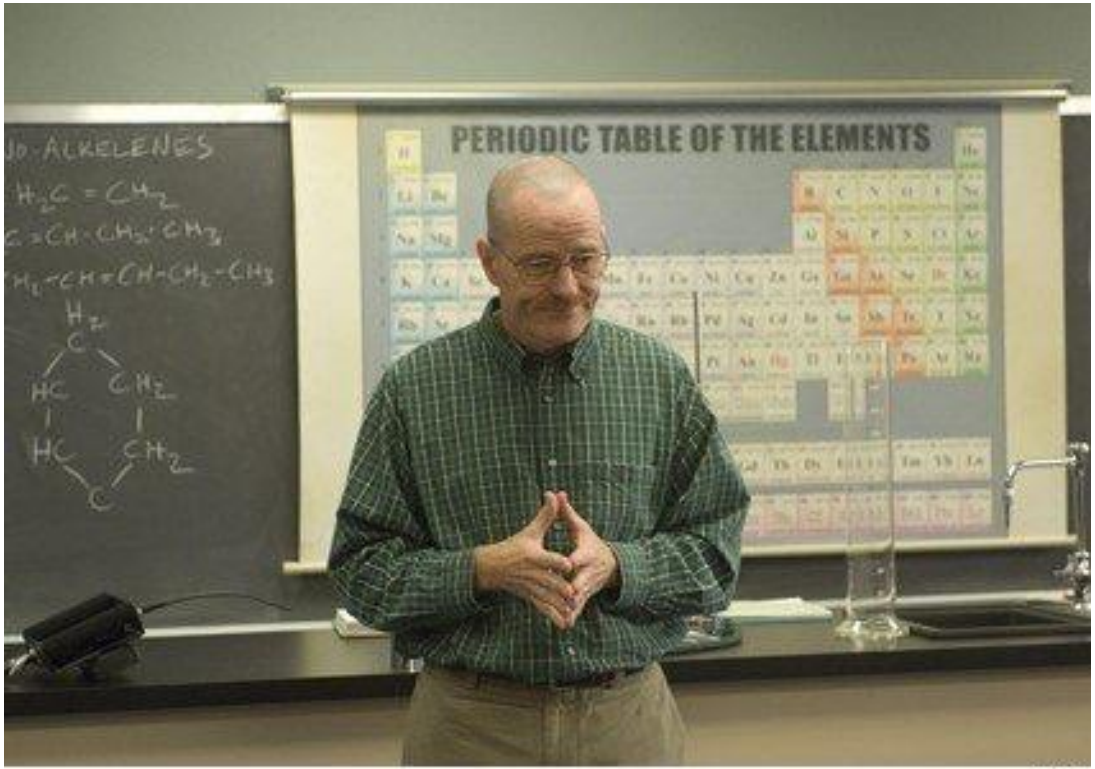
The Three E's

Educate

Empower

Enforce

Educate



AMC

Educate

We have learned to be afraid of people with these!

(Well maybe not scared of these guys) ;-)

Educate

But not people with THESE!

Educate

OR THESE!!!!

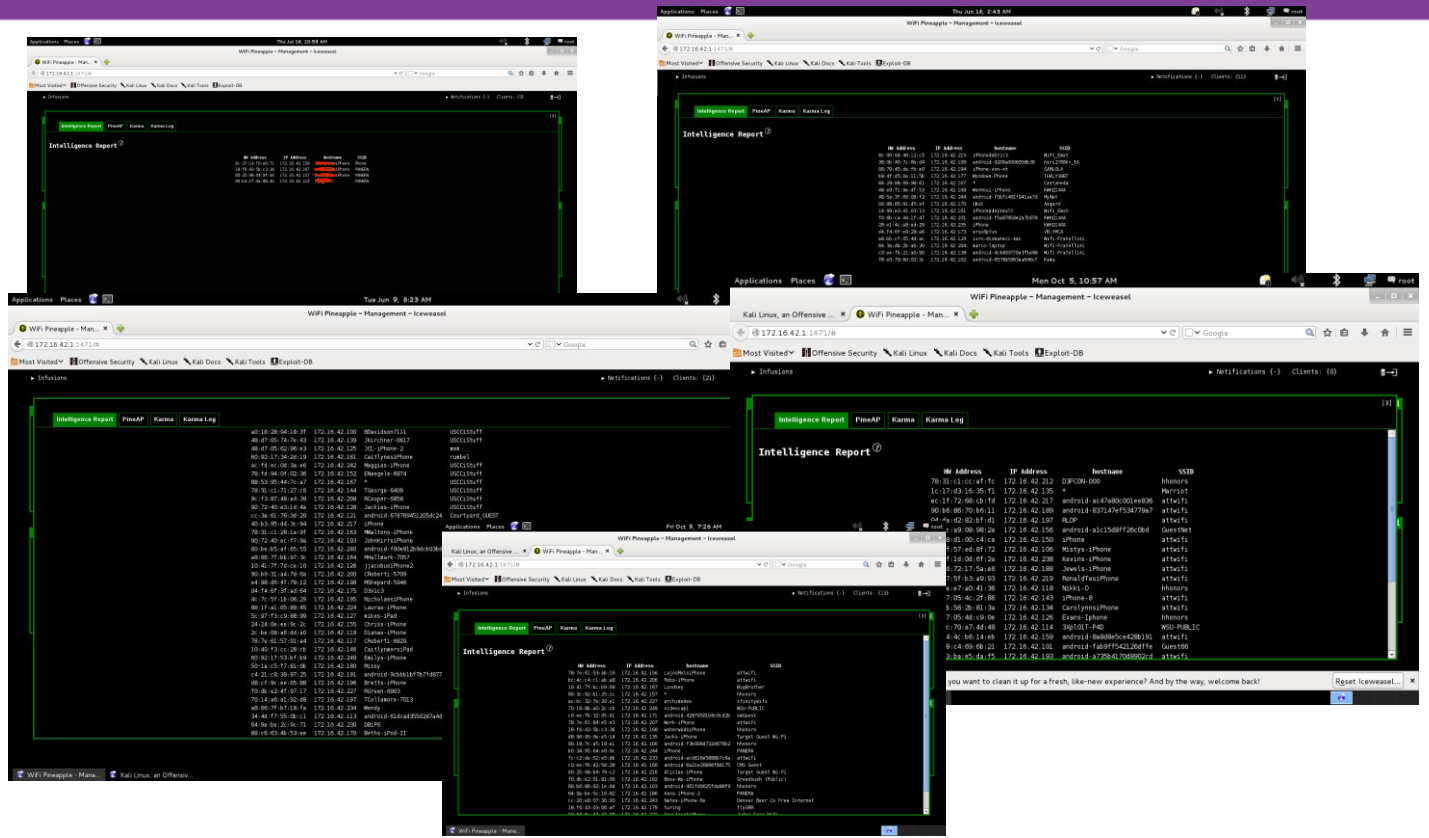
Educate

1. Teach employees common dangers they face not only at work but at home as well! Make them security conscious by default not by policy!

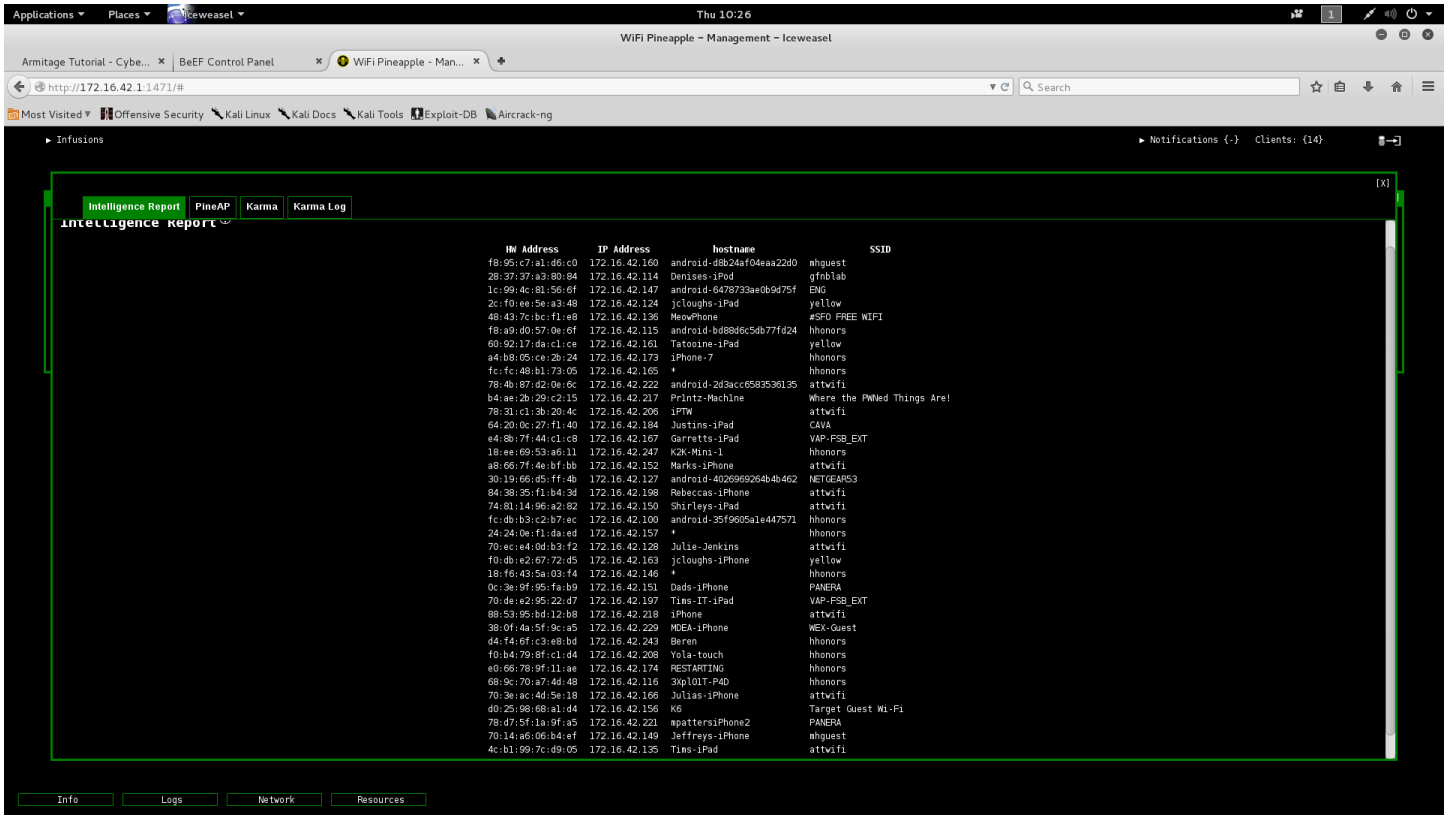
2. Drive home the fact that “Stranger Danger” is a good policy no matter how old you are!

3. Create teachable events year round not an annual exercise in futility!

Educate


Intelligence Report
Intelligence Report
Intelligence Report
Intelligence Report
Intelligence Report

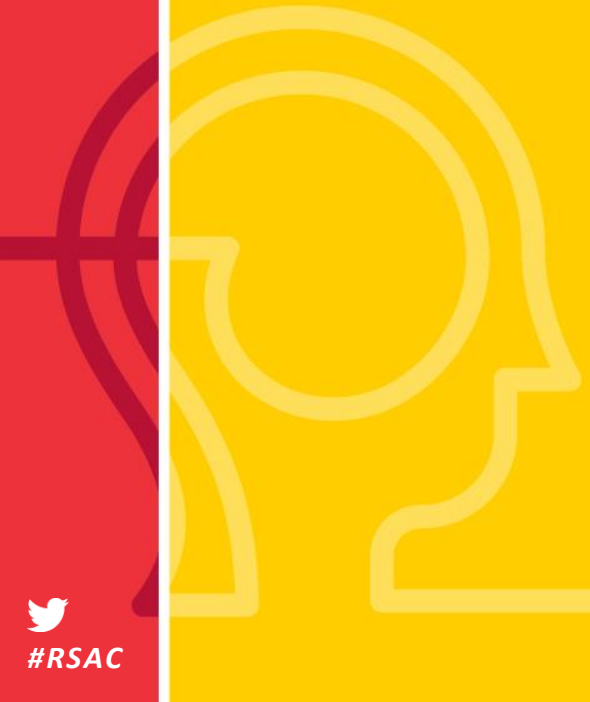
Educate


Applications
Places
Iceweasel
Thu 10:26
WiFi Pineapple – Management – Iceweasel
Armitage Tutorial - Cybe...
BeEF Control Panel
WiFi Pineapple - Man...
http://172.16.42.1:1471/#
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
▸ Infusions
▸ Notifications {-}
Clients: {14}
[X]
Intelligence Report
PineAP
Karma
Karma Log
Intelligence Report
MW Address
IP Address
hostname
SSID
f8:95:c7:a1:d6:c0 172.16.42.160 android-d8b24af04eaa22d0 mhguest
28:37:37:a3:80:84 172.16.42.114 Denises-iPod gfnblab
1c:99:4c:81:56:6f 172.16.42.147 android-6478733ae0b9d75f ENG
2c:f0:ee:5e:a3:48 172.16.42.124 jcloughs-iPad yellow
48:43:7c:bc:f1:e8 172.16.42.136 MeowPhone #SFO FREE WIFI
f8:a9:d0:57:0e:6f 172.16.42.115 android-bd88d6c5db77fd24 hhonors
60:92:17:da:c1:ce 172.16.42.161 Tatooine-iPad yellow
a4:b8:05:ce:2b:24 172.16.42.173 iPhone-7 hhonors
fc:fc:48:b1:73:05 172.16.42.165 * hhonors
78:4b:87:d2:0e:6c 172.16.42.222 android-2d3acc6583536135 attwifi
b4:ae:2b:29:c2:15 172.16.42.217 Prlntz-Machlne Where the PWNed Things Are!
78:31:c1:3b:20:4c 172.16.42.206 iPTW attwifi
64:20:0c:27:f1:40 172.16.42.184 Justins-iPad CAVA
e4:8b:7f:44:c1:c8 172.16.42.167 Garretts-iPad VAP-FSB_EXT
18:ee:69:53:a6:11 172.16.42.247 K2K-Mini-1 hhonors
a8:66:7f:4e:bf:bb 172.16.42.152 Marks-iPhone attwifi
30:19:66:d5:ff:4b 172.16.42.127 android-4026969264b4b462 NETGEAR53
84:38:35:f1:b4:3d 172.16.42.198 Rebeccas-iPhone attwifi
74:81:14:96:a2:82 172.16.42.150 Shirleys-iPad attwifi
fc:db:b3:c2:b7:ec 172.16.42.100 android-35f9605a1e447571 hhonors
24:24:0e:f1:da:ed 172.16.42.157 * hhonors
70:ec:e4:0d:b3:f2 172.16.42.128 Julie-Jenkins attwifi
f0:db:e2:67:72:d5 172.16.42.163 jcloughs-iPhone yellow
18:f6:43:5a:03:f4 172.16.42.146 * hhonors
0c:3e:9f:95:fa:b9 172.16.42.151 Dads-iPhone PANERA
70:de:e2:95:22:d7 172.16.42.197 Tims-IT-iPad VAP-FSB_EXT
88:53:95:bd:12:b8 172.16.42.218 iPhone attwifi
38:0f:4a:5f:9c:a5 172.16.42.229 MDEA-iPhone WEX-Guest
d4:f4:6f:c3:e8:bd 172.16.42.243 Beren hhonors
f0:b4:79:8f:c1:d4 172.16.42.208 Yola-touch hhonors
e0:66:78:9f:11:ae 172.16.42.174 RESTARTING hhonors
68:9c:70:a7:4d:48 172.16.42.116 3Xpl0lT-P4D hhonors
70:3e:ac:4d:5e:18 172.16.42.166 Julias-iPhone attwifi
d0:25:98:68:a1:d4 172.16.42.156 K6 Target Guest Wi-Fi
78:d7:5f:1a:9f:a5 172.16.42.221 mpattersiPhone2 PANERA
70:14:a6:06:b4:ef 172.16.42.149 Jeffreys-iPhone mhguest
4c:b1:99:7c:d9:05 172.16.42.135 Tims-iPad attwifi
Info
Logs
Network
Resources

Educate

RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center



#RSAC

Empower

In the end you realize that the only person who can protect you is…
YOU!

Empower

1. Users are not your problem they are part of your solution!

1. Give your employees a way to be effective then let them KNOW about it!

2. Give them opportunities to do the right thing & reward them when they succeed & teach when they fail.

Enforce

Employees must feel valued &
Management must take security seriously

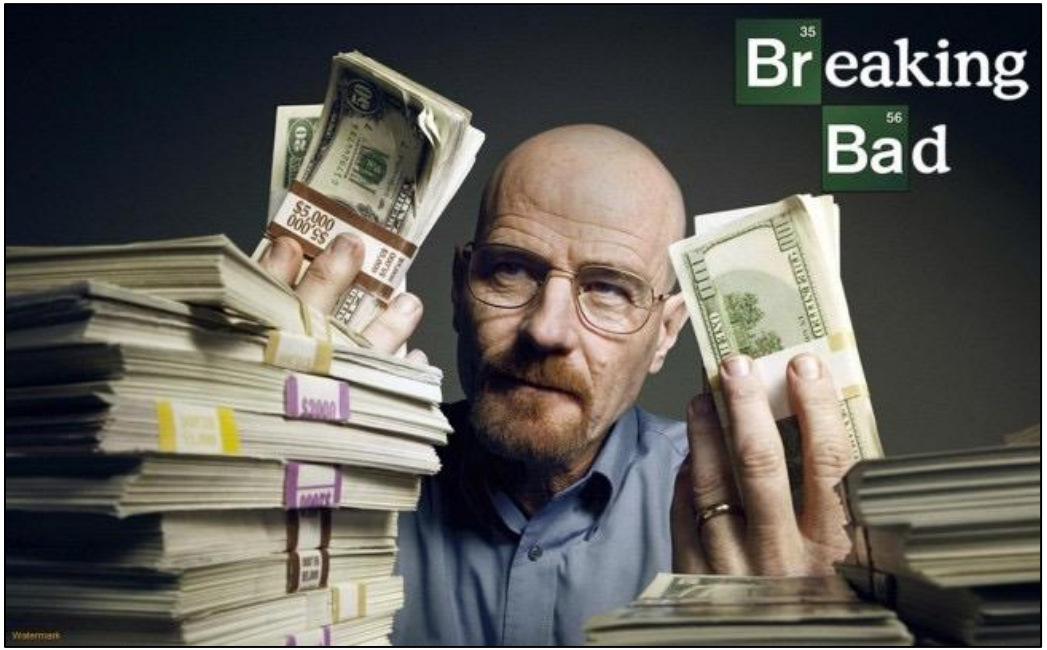
Enforce

1. Do employees see policy being enforced EVENLY throughout the enterprise?

2. Using positive reinforcement sometimes is more effective than the negative kind.

3. Visibility is sometimes all that is necessary!

Summary

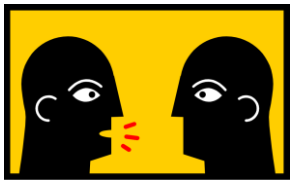


The only thing necessary for the triumph of evil is for good men to do nothing. ~Edmund Burke 1770 AD

Now let’s learn from others

Discussion and Questions????

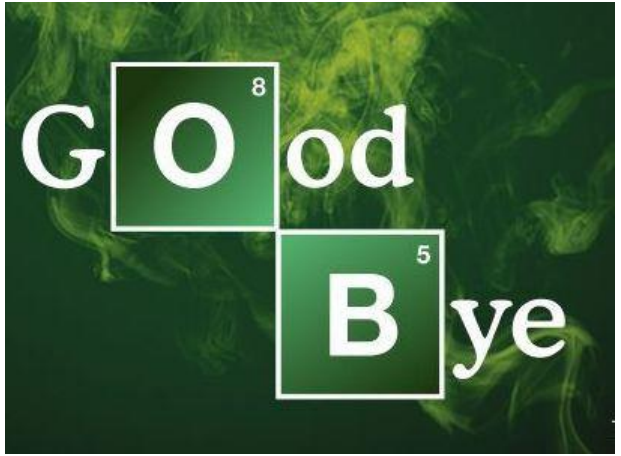
Or several minutes of uncomfortable silence it’s your choice.



This concludes my presentation Thank You

LINKS as you LEAVE

http://pwnieexpress.com/jaysonstreet



Twitter @jaysonstreet

Shout outs to @sehnaoui, Sara Kantor, @Hak5Darren, @Pwnieexpress, @GreyBrimstone, @KentNabors