Physical Penetration Testing

(a *QUICK* intro with some show and tell)

- **Who**
  - Adam Compton
    - adam.compton@gmail.com
    - @tatanus
  - In InfoSec for ~20 years; 15+ years as a penetration tester
- **What**
  - Intro to Physical Penetration Testing
- **When**
  - Now...
- **Where**
  - Here...
- **Why**
  - There was interest
- **How**
  - Slides and some Show & Tell

What is Physical Penetration Testing

Physical Tests are designed to find and exploit the vulnerabilities within a company's physical controls.

These vulnerabilities could be identified by:

- lock picking doors
- hopping fences
- piggy backing/tailgating
- bypassing physical access controls
- social engineering
- etc...

Is it easy?

Sometimes…

Some places are far more security conscious than others.

Some have 100% ID checks while others will walk you directly into their server room without asking for ID.

Well, what are some pitfalls?

In general, not being prepared.

- Not dressing the part.
  - Try not to stand out.
- Not being confident.
  - Act like you belong there.
- Not thinking fast on your feet.
  - When questioned/confronted be prepared to lie!
- Not having the tools you need.
  - No need to take everything, but make sure you have the basics.

How can I/we avoid those issues?

- Perform OSINT
  - Names of Executives, where are the remote offices, job listings, etc…
- Physical Scoping
  - Do they have fences?
  - Do they have guards?
  - What kind of badges do they use?
  - Is there a receptionist?
  - Is it in a shared building?
  - Are there external cameras?
  - Is there a smoking area?
  - Is there an internal Wifi network you can join/crack?
  - What do employees wear?

What is REQUIRED?

Most IMPORTANT: Signed legal agreement

Close Second: "Get out of Jail Free Card"

What other tools are useful?

While any tool can be useful in the proper situation, here are a few that I have found particularly useful.

- Lock Picks
- RFID Cloner
- Flash Light
- Binoculars
- Camera
- Multitool
- DropBox (Pwn Plug)
- Wifi Pineapple
- USB Rubber Ducky
- USB with Ophcrack LIVE on it
- USB Battery Pack
- Ethernet Cable
- Retractable-Flexible Claw
- Laptop

Physical Tools

Tools can generally be broken into 3 groups: Physical, Electronic, and the catchall .. Other

Physical tools are those that you would use to get physical access to secure or sensitive rooms/data.

These are also the ones that police and TSA might get suspicious about.

Examples are:

- Lock Picks
- Flash Light
- Binoculars
- Camera
- Multitool
- Retractable-Flexible Claw
- RFID Cloner

Electronic Tools

Electronic tools are those that you would use access computer systems, network traffic, and bypass access to secure or sensitive electronic data.

These are also the ones that most people will not question. They look like typical computers and computer accessories.

Examples are:

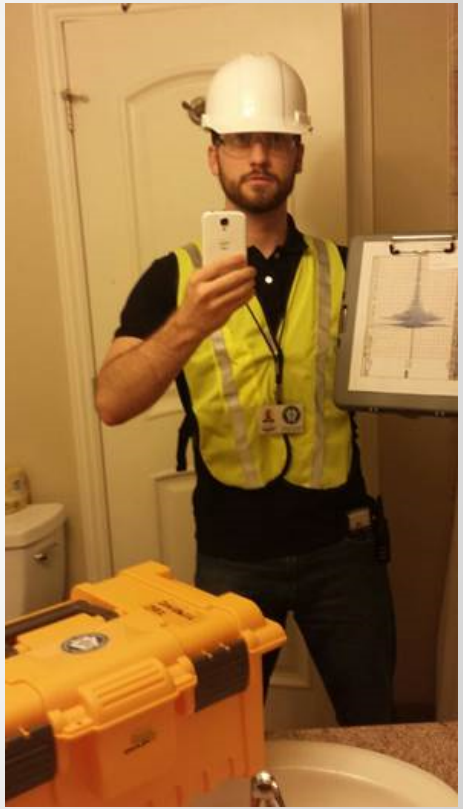
- RFID Cloner
- DropBox (Pwn Plug)
- Wifi Pineapple
- USB Rubber Ducky
- USB with Ophcrack LIVE on it
- USB Battery Pack
- Ethernet Cable
- Laptop

Other Tools

Basically anything else.

This includes:

- Proper attire (business suit, work overalls, themed jackets, etc…)
- Proper badges (just laminated cardstock, ProxCard, etc…)
- Drones…



The end.

Questions?

Comments?

Donations?