Exploitation in Meatspace

Matt Linton, Chaos Specialist
My background

● 18+ years in the tech industry
● 18+ years in rescue (volunteer)
● Pen-testing specialty is “Dirty tricks”
Exploitation in Meatspace

- Sometimes an org is just too well defended on the network and host layers
- You get stuck
- No worries, just walk in and cause trouble in person!
Why this talk?

- People see this stuff in movies and want to try it
- This stuff actually works
- This stuff has pitfalls, including ouchies™
- You need to know where to REALLY learn it
- Think of this not as a class, but a series of lessons learned
QUIZ 1

What separates penetration testing from criminal action?
PERMISSION

You’ve got it, right? Right??
Permission IS:

Written, Specific, Direct, and provided by someone *authorized to give it!*

Your get out of jail card
Some helpful hints on permission

- Get it in writing
- Keep a copy
- Be specific about your scope
- Be specific about the expected outcomes
- Have a ‘surrender plan’ in advance if caught by guards/MPs
- Include interrupts so others (eg, MPs) know permission is in place
- Oral permission is not permission
- Implied permission is NOT PERMISSION
Caveat:

● Sometimes even when you have permission in writing, it wasn’t permission
● This is more of a hazard if your test succeeds, and embarrasses someone
● Have a pre-existing relationship with legal counsel
“Get out of Jail” vs “Stay out of Jail”

Written permission is your “Get out of Jail” card

If possible, work with security/police/MPs to produce a “Don’t get in jail in the first place” card.
Still Interested?
Safety

When you physically breach, you are entering the unknown

Following are some important safety tips
TL;DR: Don’t be stupid.
Safety Warning #1

I am not responsible if you cripple yourself or others while attempting things without knowing what you’re doing.

This talk is an overview not a comprehensive course. Do not attempt things without competence.
Safety Warning #2 - Getting caught

- Police, MPs, Security guards, etc are not to be trifled with
- If caught, give up and follow the surrender plan
- Show them your SOOJ card, but if they’re not in the mood to listen, comply first and contact your POC later

1950: OK to Trifle

2014: Probably unwise to trifle
Helpful Safety Hints

- If it’s dangerous, unknown or unseen, breach in teams.
- Get your team some safety training, and assign roles accordingly.
## Example team roster:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities/Trainings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Test Onsite Lead</td>
<td>Senior member, responsible party</td>
</tr>
<tr>
<td>Penetration Tester #2</td>
<td>Train: First Aid</td>
</tr>
<tr>
<td>Penetration Tester #3</td>
<td>Train: First Aid</td>
</tr>
<tr>
<td>Safety Officer</td>
<td>Train: First Aid (Advanced), Haz-Mat Awareness Can veto any decision on the spot</td>
</tr>
</tbody>
</table>
Lesson Learned - Medical corridor
Lesson Learned - Medical corridor
Before You Breach

1. What’s your goal?
   a. Placing hidden Wifi/Zigbee access points?
   b. Placing wireless keyloggers?
   c. Stealing sensitive data?
   d. Obtaining persistent access?
   e. Other?
Hidden Devices

Placing a hidden device allows one to leverage attacks. Example:

1. Impersonate Hotspot (eg, ATTWifi)
2. Inject traffic into unencrypted HTML
3. Malicious JS drops exploit
4. Second-stage seals compromise
Hidden Devices

Wifi Injector & Cuddly Turtle Toy

Multipurpose Raspberry Pi

Network Printer Man In the Middle
Hidden Devices

Pro:
- Can provide persistent network access,
- Malware injection point

Con:
- Can be difficult to leverage,
- Require an upstream connection for MITM attacks
Keyloggers

A good keylogger is stealthy and remotely-accessible. Target the right user and get admin privs!
Keyloggers

Pro:
Steal credentials,
Can wirelessly report,
Persist post-IR *if lucky*
Unlikely to be discovered right away

Con:
Raises privacy concerns (see scope),
If discovered, dead giveaway
Sensitive data in hard form

Targeting data storage lockers/etc,
Stealing removable media that’s unattended
Grabbing backup tapes
How about a validated second-factor?
Stealing data in hard form

Pro: If targeted correctly (eg, backups), can be the entire shop all in one grab

Con: Very likely that it’ll be noticed missing.
Also hard to leave undetected with armload of DLTs.
Persistent Intelligence

How about placing wireless cameras?
With audio recording?
(Check your SCOPE!)
Breaching Layer Zero

Layer Zero is physical layer ownage

Also known as breaking and entering, trespassing, spying, espionage
The Layer Zero mindset

- There is a straight, logical line between you and what you want
- That line bypasses obstacles in your way
Casing the joint:

First step to successful penetration: Know the target.

Learn as much as you can about the building, facilities, etc.
Casing the Joint

- Find information ahead of time
  - Google Maps / Google Earth
  - Local city hall probably has floor layouts, full blueprints
  - Targeted Searches
    - “Your Target” inurl:ppt,doc,xls,pdf,docx
    - May reveal good information about org structure, building interiors, etc

(cont)
Casing the Joint

- Find information ahead of time
  - Get a tour! (This works sometimes)
  - Interns, Visits, etc
  - Just plain stake out and watch
Operation NinjaParty
The adversary

- Gates at each gap
- Guards at each gate
- Locked doors and windows
- No messin ‘around
Casing the Joint

- Grey-White square near second floor walkway is a stationary, noisy HVAC compressor
- Climb compressor,
- Throw Etrier over balcony rail
- Climb Etrier
- Second floor walkway achieved
- Pretend to be smoking, wait for door to open, and enter
Locks and Alarms

- Locks and Alarms work synchronously
- The lock delays your forward progress
- The alarm summons active security

```java
if ($difficulty_of_lock >= $response_time)
    youlose();
else
    break;
```
Locks and Alarms

- If there’s an alarm you need to disable it, or render it useless
  - Cut or overwhelm the detection source
  - Cut or overwhelm the communication path
  - DOS -- convince the adversary to ignore or disable it
Locks and Alarms

- Locks can be bypassed pretty easily, usually.
  - Look for installation failures
  - Double-door pins are frequently not set
  - Hinges sometimes reversed
  - Locks wear and fail to set right
  - There’s always picking and bumping
  - Double-doors? Give ‘em a good shove.
Locks and Alarms
Locks and Alarms

Spot the problem here.
Locks and Alarms
Door Blockers

Protip:

Sometimes you can use these little guys to stick to metal doorjambs when people open the door, and gum up the re-lock mechanism.
Locks and Alarms

- Where to learn more:
  - tooool.us -- The Open Organisation Of Lockpickers
  - Community College “Locksmithing” curriculum
Barrier Bypass

- Barriers are often poorly-considered
- Where’s your straight line?
Barrier Bypass

- A note about HVAC ducting paths
- Just don’t do it, seriously
- It’s a “Movies only” trick
- They’re tighter than you think
- They aren’t rated to hold you
- Also, ASBESTOS.
Barrier Bypass

- Maintenance corridors ARE often a good path
- May be between floors, behind wall spaces, above drop-ceilings
- Look for square metal plates w/ screws
Climbing and Descent

- Often a quick climb or descent can be the most straightforward path
- Up to a balcony, down through a skylight, etc
Climbing and Descent

- Descent easier than Ascent (duh)
- Both can be dangerous
- Best done in teams
A note on falling

- You need to practice this stuff first
- With others who know how to do it
- “Distance fallen is a poor predictor of major injury in falls, in adults” -- nih.gov
- That’s both good news, and BAD news
A note on falling

- TL;DR: Falling is BAD, m’kay?
Ascent: Know your limits.

Yes

Yes

Yes

No.
Climbing

- For many climbing-based skills you need a lightweight harness
- You can make one out of webbing
- I’m not going to show you how because doing it wrong will cripple you
Ascent

● Pros:
  ○ Bypass obstacles
  ○ Can be done out of sight
  ○ Is generally unexpected

● Cons:
  ○ It’s really hard
  ○ You have to practice
  ○ You can get stuck
  ○ You can get hurt

*If you fail you might look really stupid*
Ascent

- Best used to quickly overcome “small” obstacles
- Use an Etrier / Aid Ladder to ascend short distances quickly
- For longer distances, use of two and/or gibbs ascender can help
Climbing and Descent

Pictured: Straight ascent w/ no walls.

Use of foot webbing w/ gibbs, and hand ascenders.
Descent
Descent

● Pros:
  ○ Only “need” one rope
  ○ Can be more stealthy
  ○ Easier than Ascent

● Cons:
  ○ Need another exit, or
  ○ Must ascend again

If you fail you can get seriously hurt
Operation: Get into Caesar’s Challenge
Descent - Rope recovery

- Self-recovery is same as a static line, but looped
Ropes

- Ropes vary greatly from “Solid” to “Death wish”
- Ensure your load rating is adequate, including shock rating
Ropes

- Paracord (550lb) doubled can be OK in a pinch
- 8mm+ static kernmantle is much better and still pretty lightweight
- Thicker ropes are safer but more clunky
Climbing and Descent

- Where to learn more:
  - Rock-climbing / Mountaineering organizations
  - WSAR/USAR Classes (Find a volunteer org)
Poor Opsec

- People practice poor opsec
- Check your assumptions
Poor Opsec

- File cabinets - Often left unlocked
- Safes - Often people forget to re-dial, jiggle those handles!
- Keys in drawers, in flimsy “Key cabinets”
- Passwords on white boards
Poor Opsec

Source: CNN interview of LAPD’s “RACR” tech division
Poor Opsec

- When you see one of these near a comb-lock....
Social Engineering Onsite

People are the weakest link in the chain
Get them to do what you want!
Social Engineering Onsite
Social Engineering Onsite

Nobody expects…. you to just show up and walk right in.

This is your chance to play adult dress-up!
Social Engineering Onsite

Things to keep in mind:
● This is totally natural and normal.
● You are not nervous.
● Your story is consistent and flows
● You are baffled as to why someone would question your presence
● PRACTICE, PRACTICE, PRACTICE
Social Engineering Onsite

Learn Human Behavior

- Ask for small favors, build trust
- Make yourself sympathetic
- Empathize with your target
Social Engineering Pitfalls

Check your scope!

- It may be illegal to impersonate X in your state
- X may not take kindly to being impersonated, regardless of legality
Social Engineering

- Where to learn more:
  - Industry groups (SANS, etc)
  - social-engineer.org (and podcast)
  - Improv School (yes!)