Introduction to Cyber Attack

Dr. Barry Mullins
AFIT/ENG
Bldg 642
Room 209
255-3636 x7979

Don't Learn to Hack - Hack to LEARN.

History of Hacking

- Assignment:
  - Watch the following 50-minute video to learn more about the history of hacking
  - www.youtube.com/watch?v=Y47m1cOyKjA (Also on file server)

Kevin Mitnick (Blackhat 2016)

Information Warfare Threat

"The world isn't run by weapons anymore, or energy or money. It's run by ones and zeroes, little bits of data. It's all just electrons.

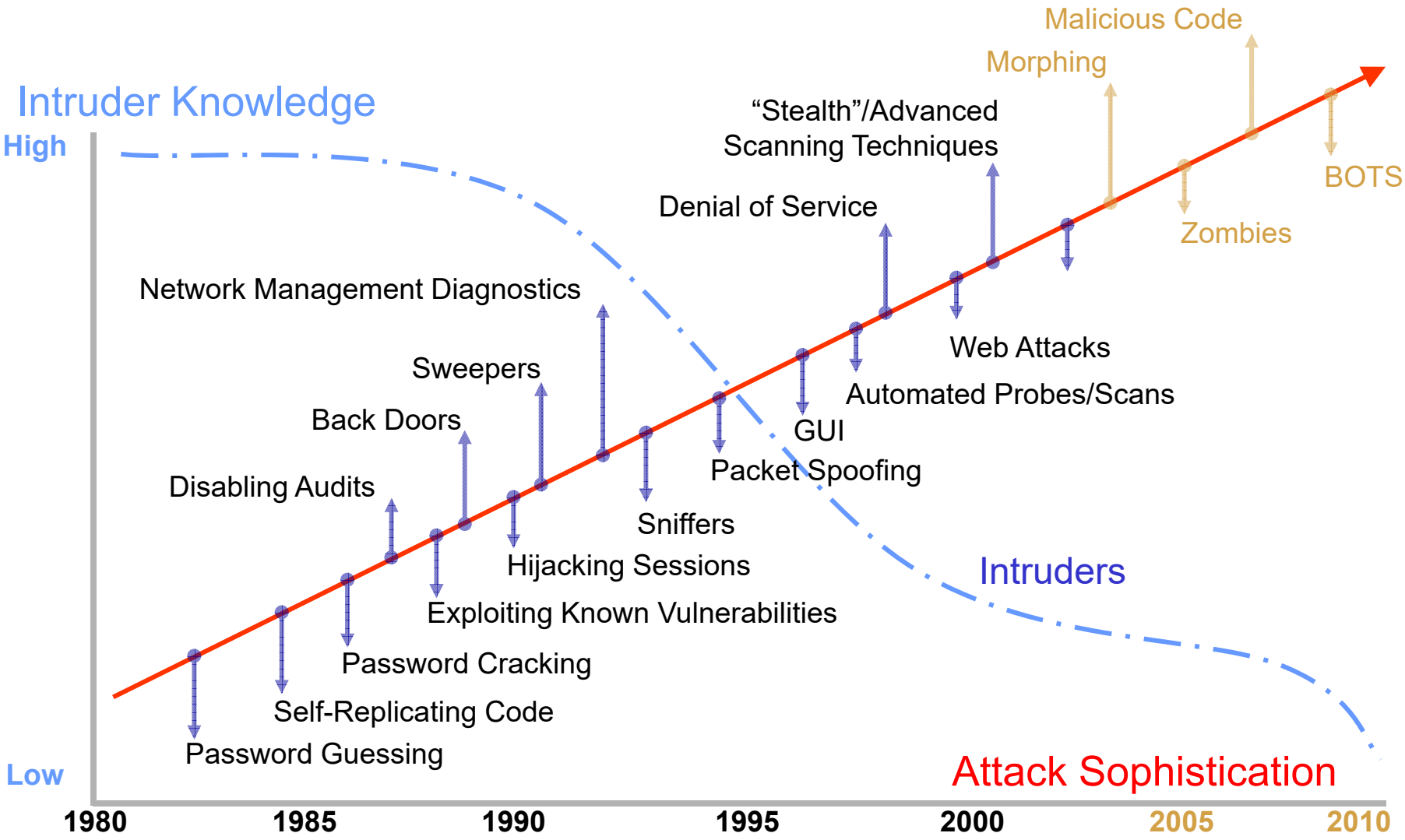
There's a war out there, old friend, a world war. And it's not about who's got the most bullets. It's about who controls the information: ...what we see and hear, how we work, what we think.

It's all about the information."

-- Sneakers Movie (1992)

- Technically advanced military… but also vulnerable
  - > 90% of military comms over commercial systems

Attack Sophistication vs. Intruder Knowledge



Sources: *Carnegie Mellon University, 2002 and Idaho National Laboratory, 2005*

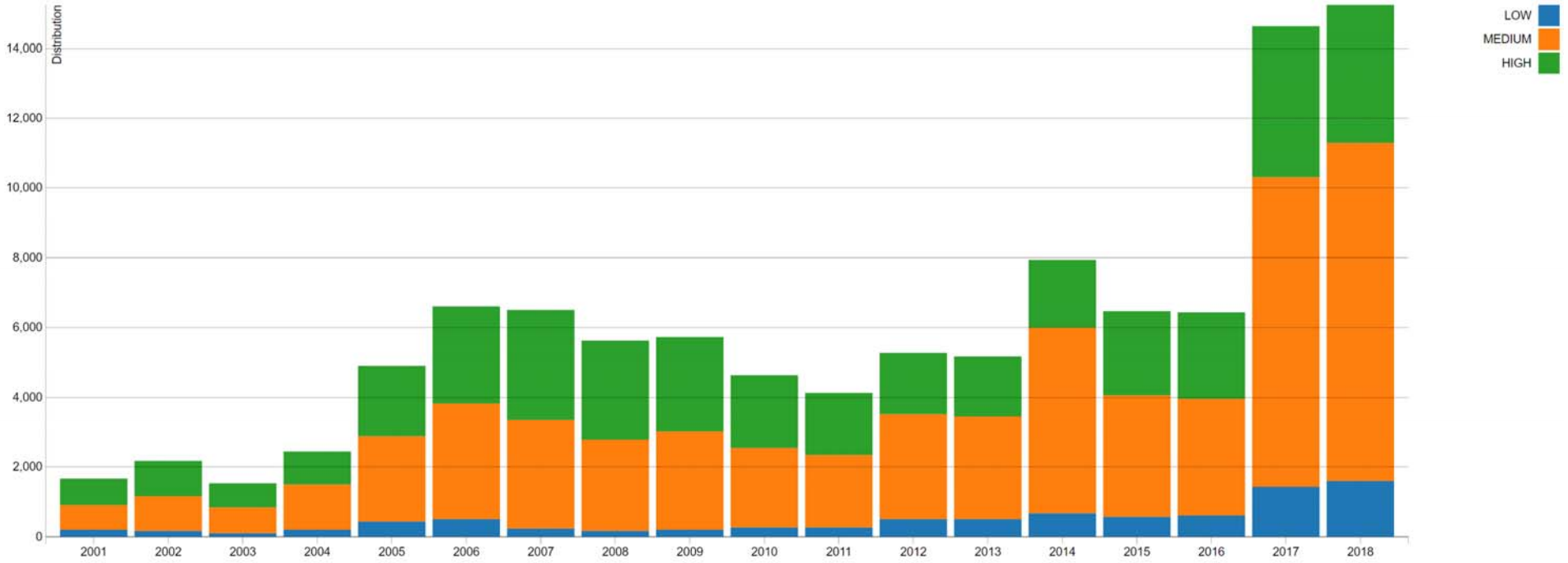
Who Are The Threats?

- External
- Insider
- Never underestimate your adversary

- Obligatory Sun Tzu quote (Art of War)
  - If you know the enemy and know yourself,
    you need not fear the result of a hundred battles.
  - If you know yourself but not the enemy,
    for every victory you gained you will also suffer a defeat.
  - If you know neither the enemy nor yourself,
    you will succumb in every battle.

Forces That Have Brought The World To It's Knees Over The Centuries

Got Vulnerabilities? One Data Point



https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time/

LOW, MEDIUM and HIGH is based upon the CVSS V2 Base score
CVSS - Common Vulnerability Scoring System

Got Vulnerabilities? How About No Power?!?!

- DHS experiment called "Aurora"
- Conducted in March 2007 at the Department of Energy's Idaho lab

Mike Assante

http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

Why Does This Happen?

- Security is often overlooked (not a primary concern)
- Systems complex in nature and rich in features can be riddled with security holes
- Attacking is becoming common and easy
  - Believe it or not, there are books clearly explaining how to attack! ☺
- People will click on anything
- Security and attacks are a perpetual cat-and-mouse game
  - Keeping up-to-date with latest trends helps

Why Does This Happen?

- Lots of buggy software & wrong configurations…
  - These are vulnerabilities
  - Awareness is the main issue
    - Train software designers, coders, and sys admins
- Some contributing factors
  - Programming texts do not emphasize security
  - Programmers are lazy
  - Consumers do not care about security… historically
  - Security is expensive and takes time
  - Security may make things harder to use

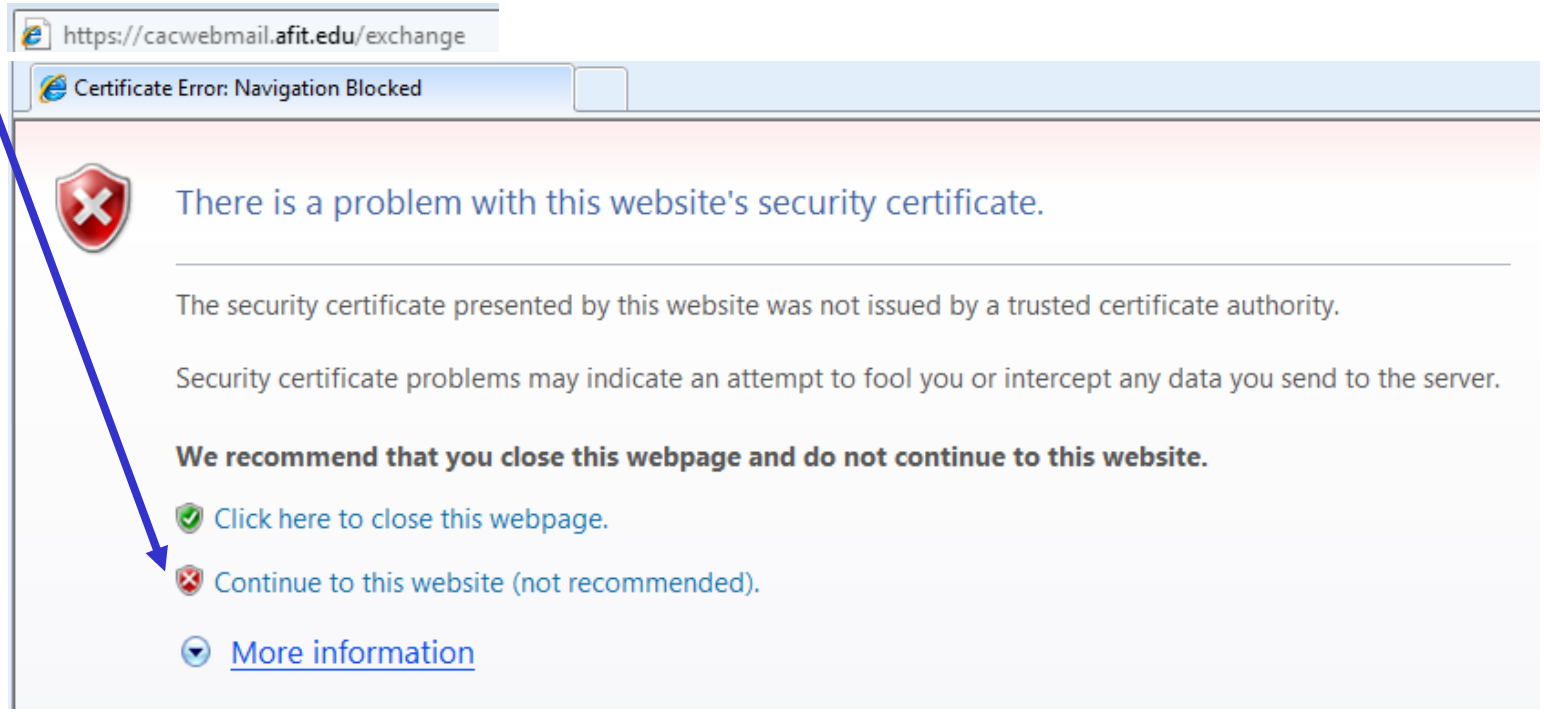
Who Would Win?

$10 million security program

Enable Content

Contributing Factors to Insecurity

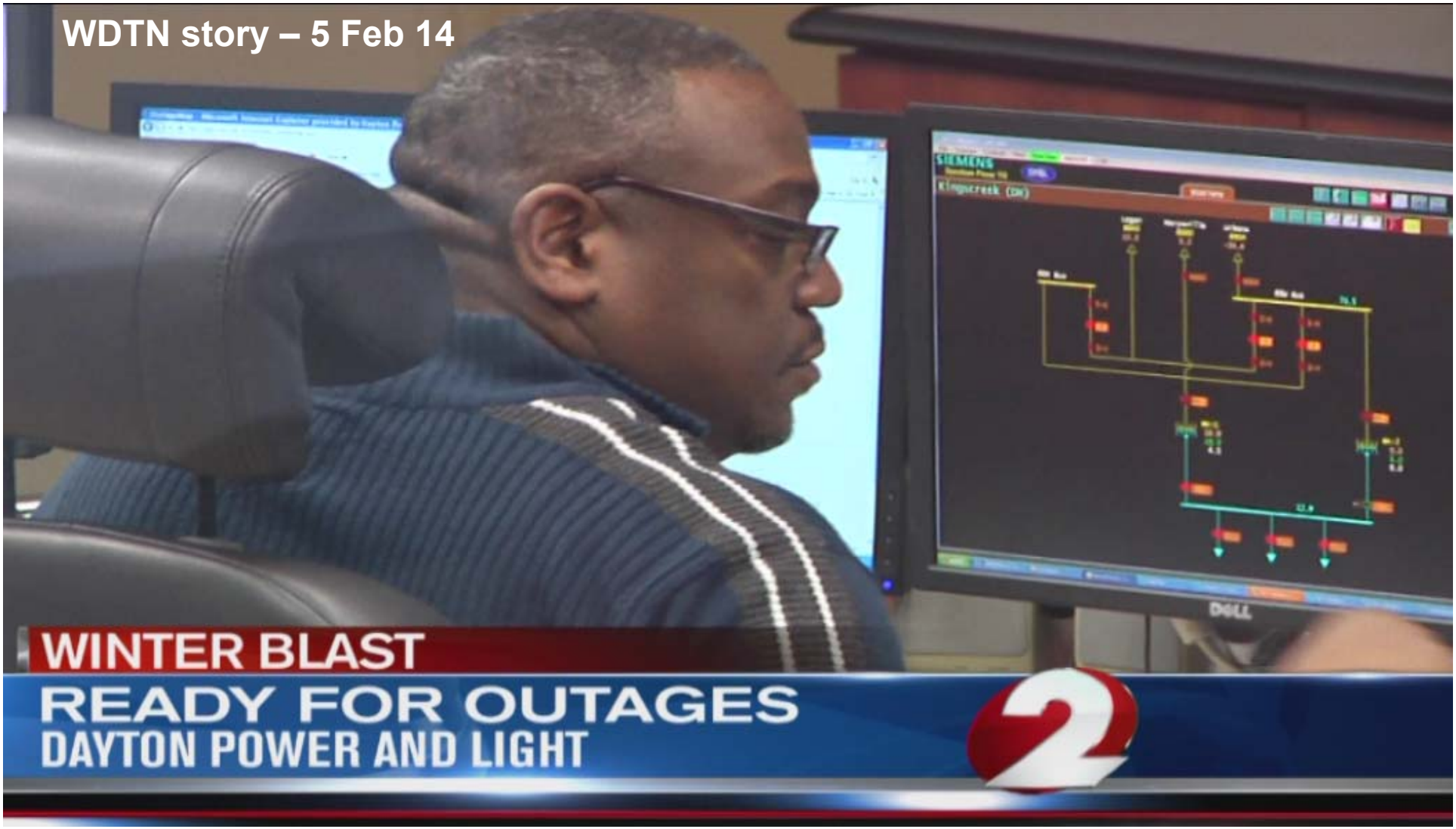
- Protocols and standards designed in the 60s and 70s
  - Not designed with security in mind
- Computer architectures will run any data given
- **Users** required to fix/patch bugs when found
- No default checking of user or external input
- **Users** control which certificates to accept (trust)



Contributing Factors to Insecurity

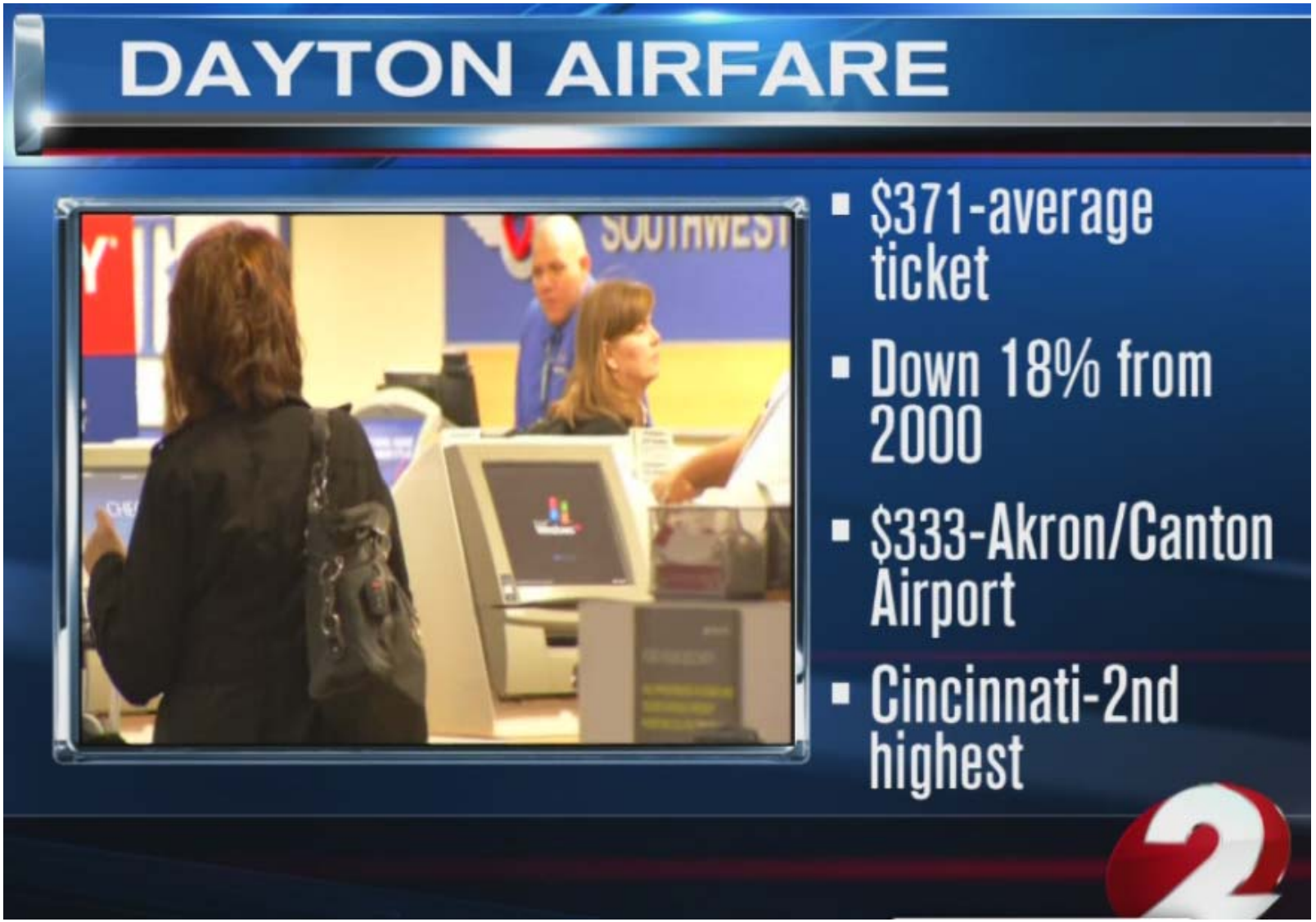
- Organizations or users don't (or CAN'T) upgrade obsolete OSs
- Support for Windows XP terminated on 8 April 2014
- Windows XP market share is 4.08% as of November 2017
  - ~100 million computers worldwide
  - http://www.netmarketshare.com/report.aspx?qprid=11&qpaf=&qpcustom=Windows+XP&qpcustomb=0

Contributing Factors to Insecurity



Contributing Factors to Insecurity

- Dayton airport kiosks use Windows XP (23 Apr 14)



20 3:30 AM - 18 Aug 2017

Troy Hunt @troyhunt · 7h

This hotel needs a serious upgrade...

18 Aug 17

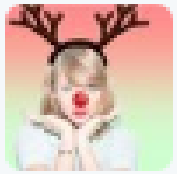
Contributing Factors to Insecurity

- Despite end of support, Windows XP / Windows Server 2003 patched in May and June 2017 due to WannaCry Ransomware

Contributing Factors to Insecurity

3:40 PM - 21 Dec 2016

In reply to Andy Scarface



SwiftOnSecurity @SwiftOnSecurity · 6m

.@dragontologist Last year, I removed a Win2000 server from our network. By spearheading the project to replace it.

Jack Daniel
@jack_daniel

Following

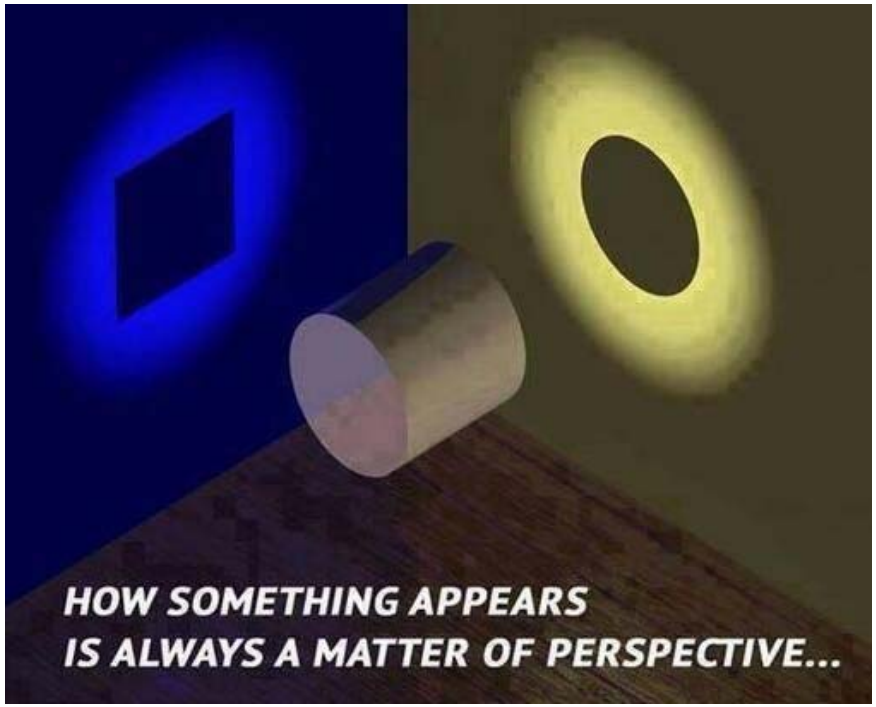
So many people (and companies) focused on zero days while ignoring 5,437 days.

(That's days since XP was launched)

1:26 PM - 13 Jul 2016

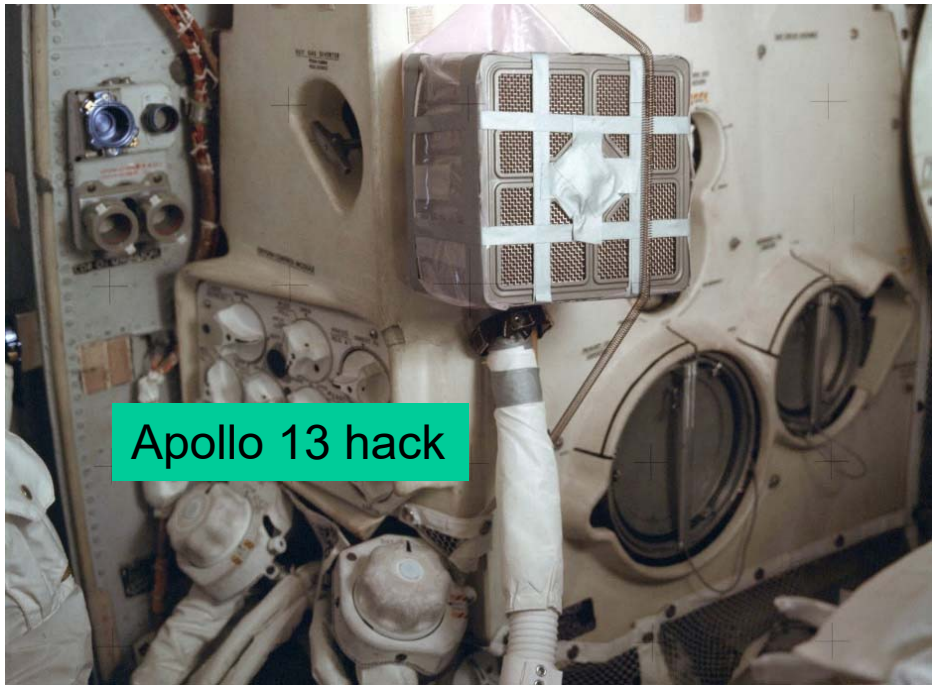
Defend/Attack Point of View

- When an Information Technology (IT) system is being designed and implemented
  - Developers concerned with *building* the system
  - Impractical/impossible to think of every abuse scenario
- What is the hacker/penetration tester mentality?
  - How to *break* the system
  - How to make system do something it shouldn't
- We need to develop an attacker mindset



"Hacker"

- First definition by Tech Model Railroad Club (MIT) in 1946:
  - "One who applies ingenuity to create a clever result called a hack"
- A person who enjoys modifying how the system functions
- Someone who tries to "figure out how things work"
- "A person interested in exploration, usually of a computer"
- Someone who could quickly create software code that worked
  - Hack out a routine



The Secret Lives of Hackers video:
https://www.youtube.com/watch?v=DKzi5CYNFAg

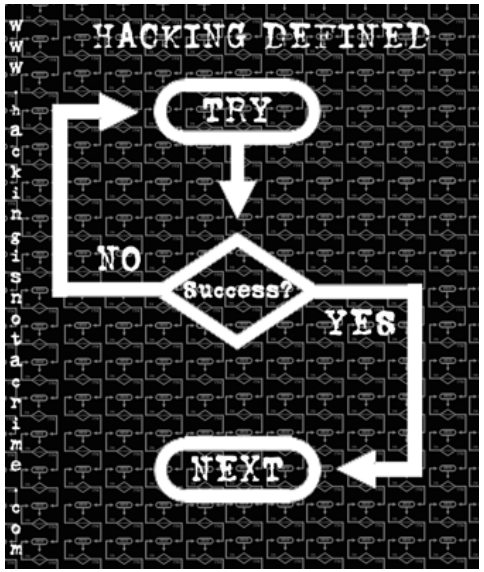
Hacker

- Hackers often have a different mindset…
- Most of us follow the "rules"…

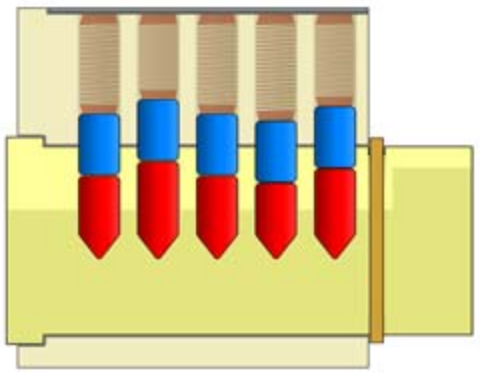
Some don't …

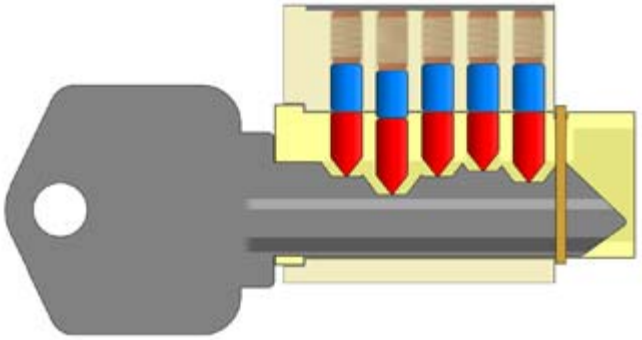
A Skilled Attacker

- The attacker
  - Knows each OS's special characteristics
  - Can recognize and exploit the "personality traits" of each OS, so exploitation will go much faster
  - Gathers information about the target
  - Scans the target, determining the number of computers, their OSs, their open ports
  - Scans more deeply, looking for specific vulnerabilities
  - Attempts to exploit each vulnerability found, eventually finding a way in and then accomplishing his goal
  - Stores programs and/or creates accounts that will allow him in more easily next time
  - Erases any evidence that he was ever there
  - Lives a life of research, trial & error, and **practice practice practice**



Hacking is much like lock picking…





- The attacker
  - Knows each lock's special characteristics
  - Can recognize and exploit the "personality traits" of each lock, so picking will go much faster
  - Never thinks that the picking tool opens the lock
  - Knows that the pick is just running over the pins to gain information about the lock
  - Knows it's the human who opens the lock
  - Remembers what works with each lock
  - Erases his fingerprints
  - Lives a life of research, trial & error, and practice

Is Physical Security Important To Cyber?

- Absolutely!!
- If I can touch your hardware, it no longer belongs to you
- What about non-cyber assets?
  - Files
  - Medical records
  - Drugs

Practice …

Deviant Ollam ツ @deviantollam · 21h

"That's right... test each button. Now, which one feels stiffer than the others? Which one is likely binding?" :-)

Breaking Into A Bank With Whiskey

This bank lobby/vestibule was locked (unless you had an ATM card, of course) but the doors were controlled by a Request-to-Exit (REX) sensor that operated via passive infrared.
Triggering that sensor (by, say, blowing a fine mist of whiskey through the tiny gap between the doors) was enough to cause the door controller to unlock.

https://www.youtube.com/watch?v=SDl4AO4ancI -- Published on Sep 3, 2016

Gathers Information About The Target

Dan Kaminsky retweeted

Rance @revrance · Sep 30 30 Sep 14

Let's play "spot the secure airport door code"...

SecuriTay Retweeted

Jonathon Colman @jcolman · Jun 29 29 Jun 16

I sense a weak password

Implementation Flaw?

Implementation Flaw?

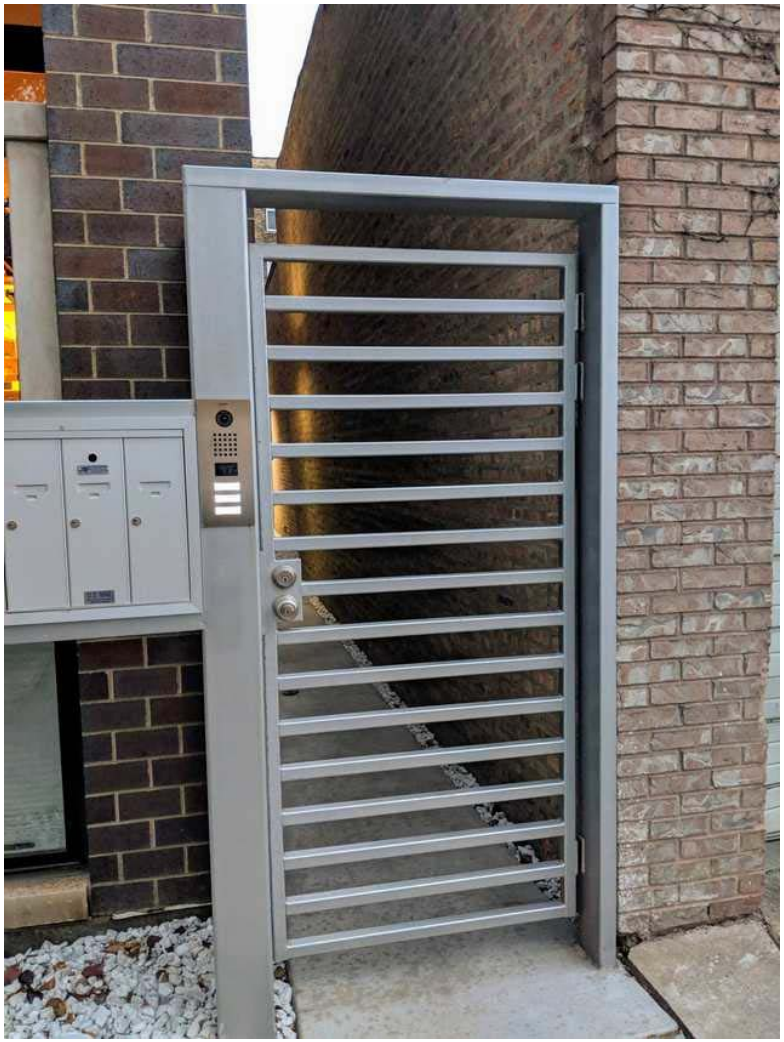
Implementation Flaw?

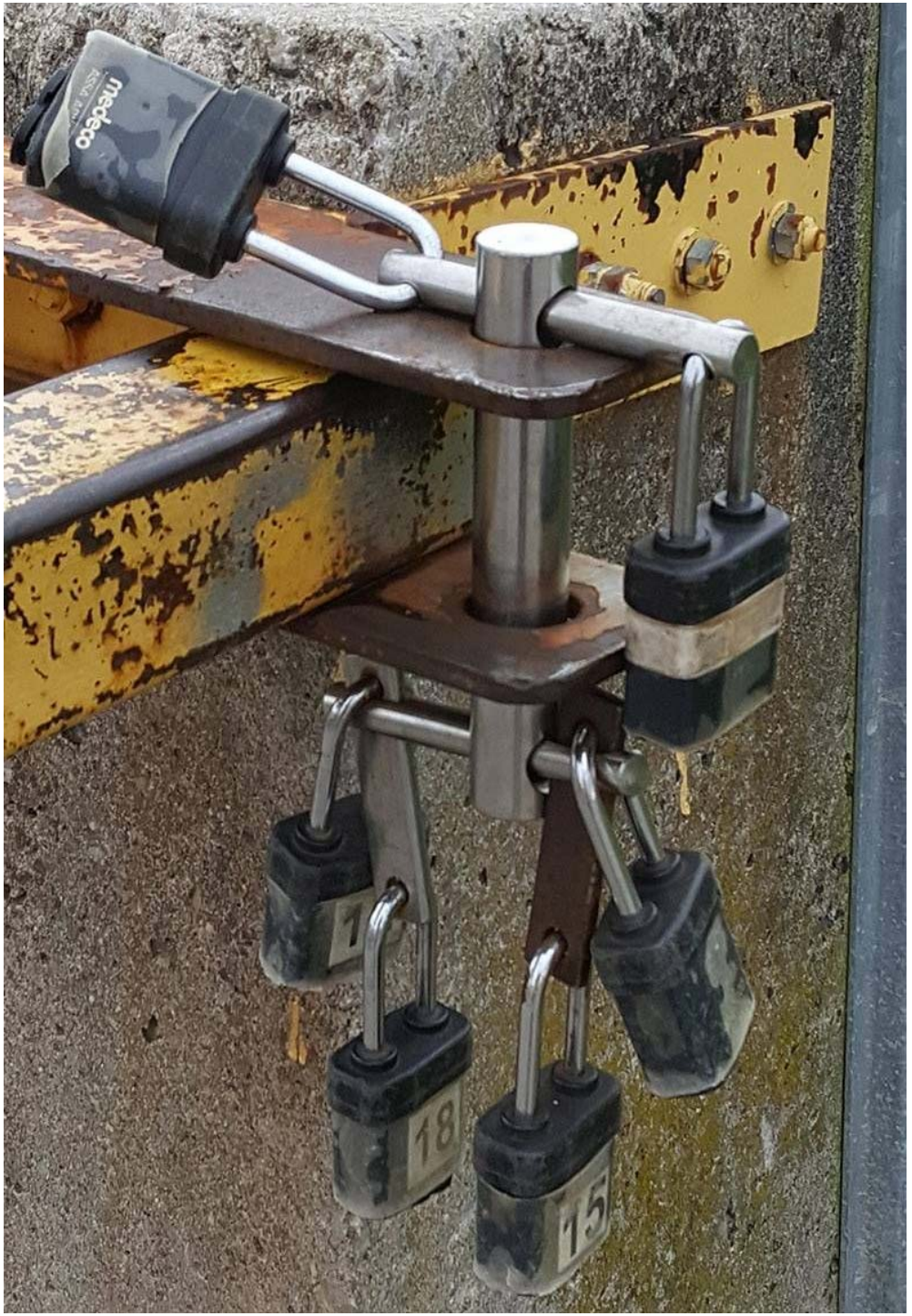
Implementation Flaw?

Implementation Flaw?

Implementation Flaw?

Implementation Flaw?





Implementation Flaw?

Implementation Flaw?

Implementation Flaw?

Implementation Flaw?

Hacker Mindset

- Doesn't accepts "This is how it works"
- Playing with the imagination and possibilities while interacting with ideas, people, and the environment, leading to new outcomes
- Gathers information from every possible source

Hacker Mindset Test

Hacker Mindset Test

Hacker Mindset Test

Hacker Mindset Test

"A Successful Hacker" by Raphael Mudge

The #1 Trait of a Successful Hacker

May 8, 2014

…

What's the difference between someone who will become a good hacker and someone who will stay a script kiddie, forever?

I know the answer. Here it is. The number one trait for a successful hacker is

the ability to reason about things one can't directly observe.

Since a hacker is in the business of circumventing controls or discovering the unknown, they're constantly in the blind. They have to reason about what they're trying to hack though. If they can't, they'll never figure out the system they're working on.

…

http://blog.cobaltstrike.com/2014/05/08/trait-1-for-a-successful-hacker/

Hacker Terminology

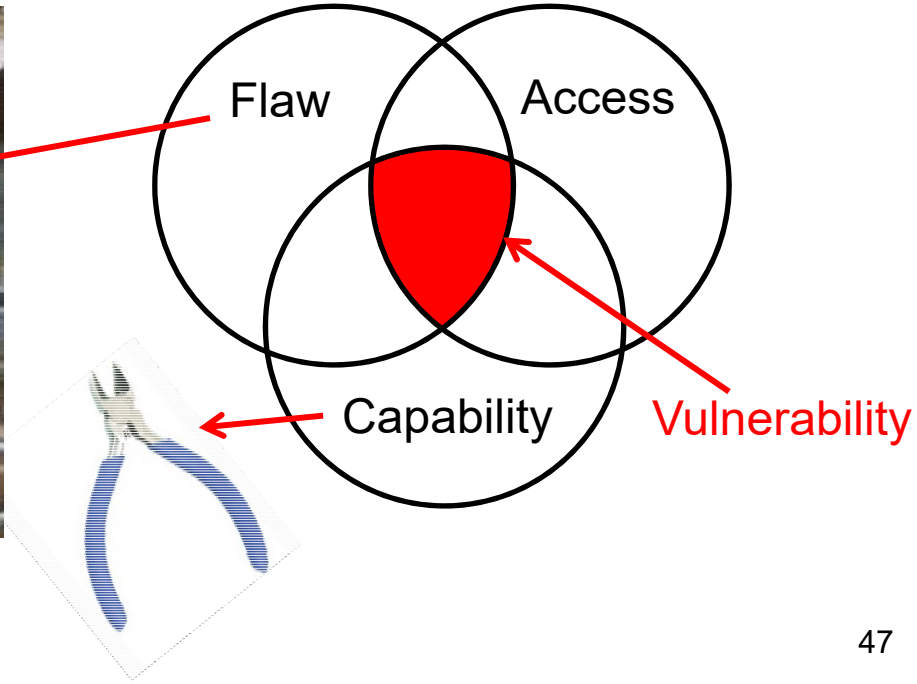
- Black Hat / Cracker / Malicious Hacker
  - A person who forces the system to perform in an unintended manner for unethical purposes
  - One who breaks security on a system without authorization
- White Hat / Ethical Hacker / Penetration Tester
  - A person who forces the system to perform in an unintended manner for ethical reasons
  - Explore your own company's systems searching for vulnerabilities with permission
- Gray Hat
  - Hacks into computers without permission (or compensation) to find vulnerabilities and reports these to the system owners

Hacker Terminology

- Script Kiddie
  - Unskilled hacker → typically an insult
- Exploit
  - Piece of software, sequence of commands or method that takes advantage of bug, glitch, or vulnerability to get unintended or unanticipated behavior out of computer software, hardware, or other electronic devices
- 0day
  - Exploit that is yet to be reported to the software vendor
  - Hackers look to earn 0day → a status symbol
    - Use it to trade for desired "booty": tools, credit card #s

Vulnerability

- Flaw that degrades the performance/security posture of a system
- Intersection of
  - System susceptibility (flaw)
  - Access to the flaw
  - Threat's capability, talent, resources for exploitation



What Are Security Assessments?

- Three common terms for security assessments
  1. Security Audit
  2. Risk Assessment
  3. Penetration Test

- They may sometimes be used synonymously but are not the same

1. Security Audits
2. Risk Assessments

1. Security Audit
   - More of a compliance check
   - Checklists and standards
   - Policies and procedures
   - Backups
   - Verification
   - Are you doing what you are supposed to be doing

2. Risk Assessment
   - Also more of a paper exercise
   - Weighs likelihood against impact
   - Weighs cost against benefit

3. Penetration Test / Hacking

- Looks for security vulnerabilities
  - Unpatched operating system or application
  - Known security holes
  - Accounts with weak or no passwords
- Examines impact of discovered vulnerabilities
- Targets digital, physical, and personnel (social engineering)
- Hands on test of network security
- More thorough and effective

Things to Consider in Ethical Hack / Pen Test

- Be careful and do it right!!
  Must have documented agreement to conduct the penetration test
  - Have a lawyer review it
  - Most ethical hackers carry substantial insurance coverage

- Develop/use a good methodology
  - Must be repeatable
  - Must be able to document the results

Things to Consider in Ethical Hack / Pen Test

- Never change permissions on files or folders
  - This includes sharing a drive/folder such that anyone can gain access

- Never start services on the target that provide access to the target such as FTP, SSH, HTTP, RDP, etc.
  - This includes creating a service that is password protected

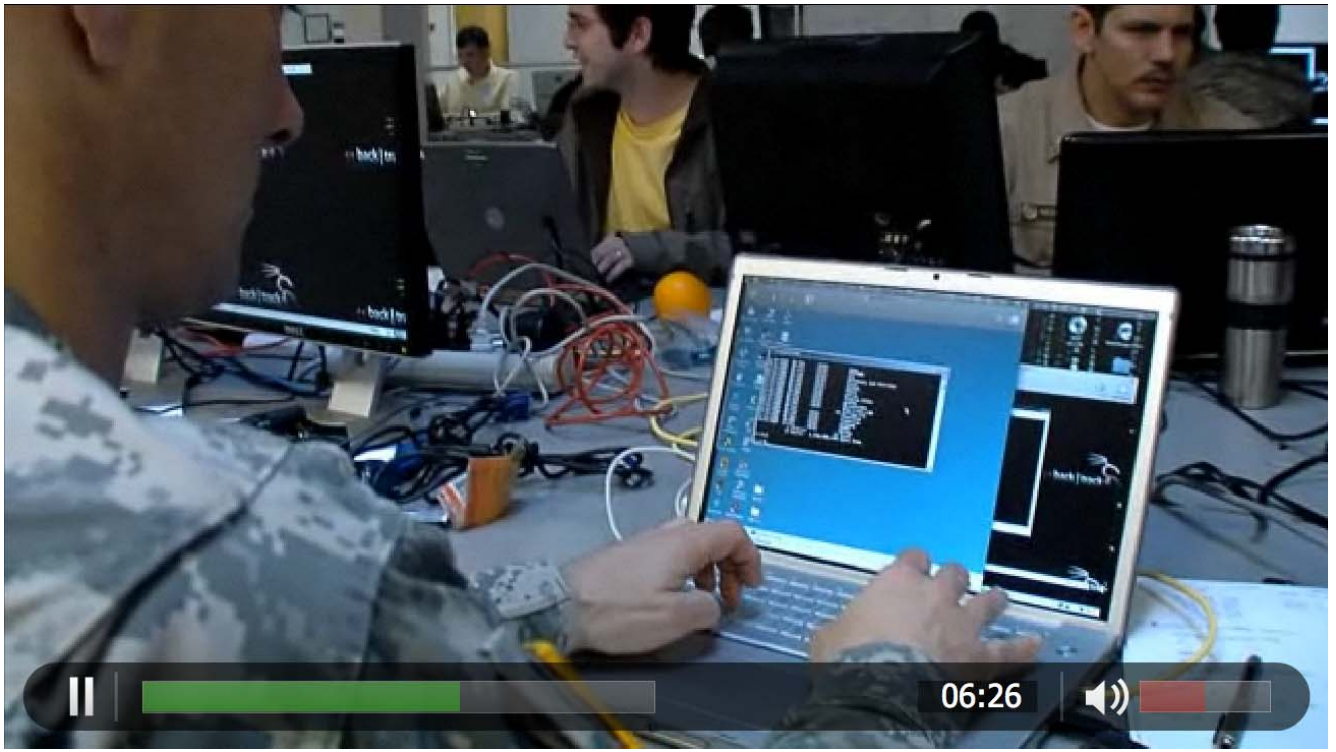
Why These Tools?

- Problem approach differs with tools and training
  - "If your only tool is a hammer, all problems look like a nail"
  - We'll use both Windows and Linux tools
    - Should use VMware Workstation!!
  - We'll exploit both Windows and Linux boxes

- Why are we studying these tools and techniques?
  - You need to see various genres of attack tools / techniques
  - These are the actual tools attackers use today
  - Inexpensive ☺
  - Provide *fundamental understanding* of techniques attackers use

Kali Linux

- Linux-based Penetration Testing Distribution
- Can (and should be) run within VMware Workstation
- Official docs: docs.kali.org
- Copy the VM off the file server to your machine before opening it



Always Get Permission!

- Many tools are automated and you'll want to leverage that…

- … but always get permission before running these tools, even on your organization's network

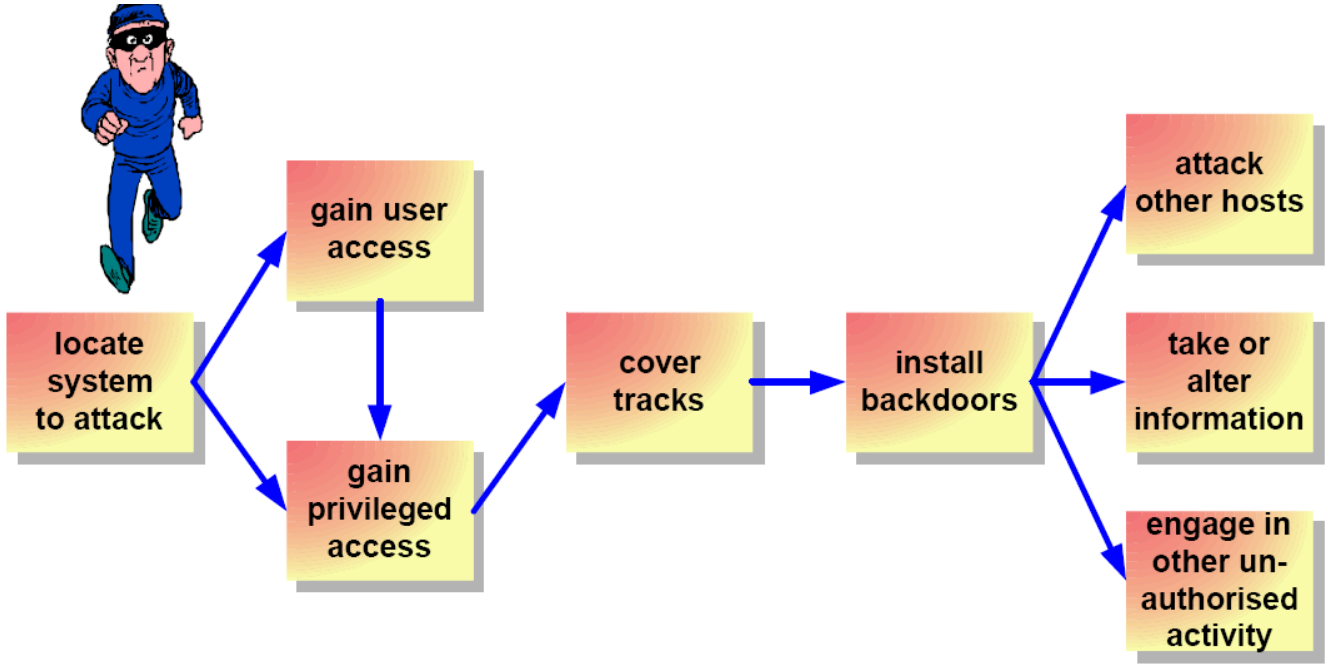
- Get written permission!
  - Sample form at: www.counterhack.net/permission_memo.html

Natalie Portman in Léon: The Professional

Be Polite to Your Targets

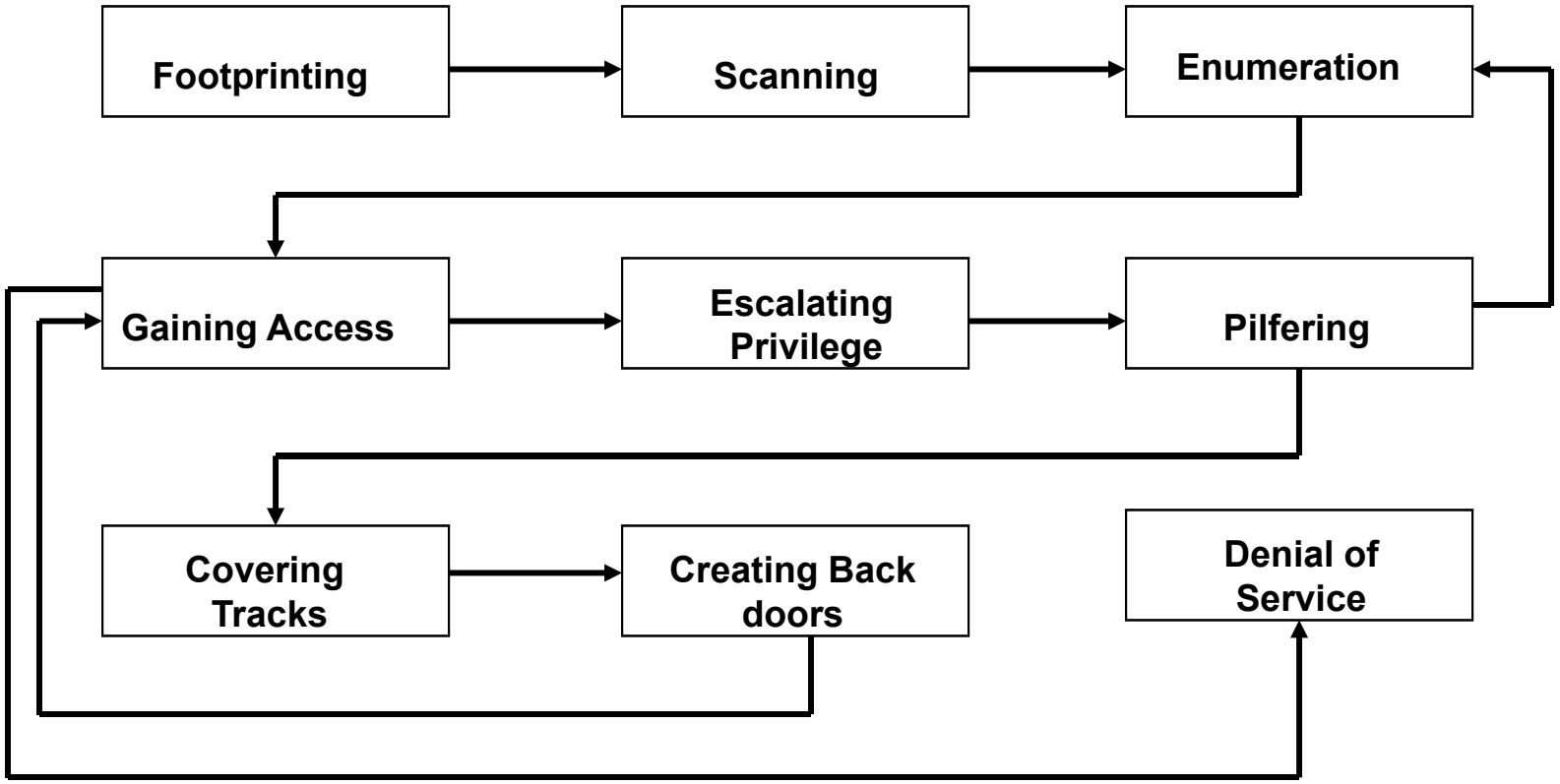
Anatomy of an Attack

- You will see several different methodologies to execute an attack



Anatomy of an Attack

- You will see several different methodologies to execute an attack



Anatomy of an Attack

They all have the same basic flow:

1.	Reconnaissance	Chapter 5
2.	Scanning	Chapter 6
3.	Gaining access	
	❖ Gaining access at the operating system & application level	Chapter 7
	❖ Gaining access at the network level	Chapter 8
	❖ Denial of service attacks	Chapter 9
4.	Maintaining Access	Chapter 10
5.	Covering Tracks and Hiding	Chapter 11

Sage Advice

- Learn the *trade, not the trick*
- Never give up!
- The more you know, the luckier you'll get
- Make sure you are solving the right problem/asking the right questions
- Never giving up doesn't mean there are not easier/cleaner/better alternatives!
- People are people… become your target
- Everything's easy in bite-sized chunks
- Time spent understanding your target is never wasted time!
  - *Give me six hours to chop down a tree and I will spend the first four sharpening the axe.* -- Abraham Lincoln

Finally…

- DerbyCon 3.0 (2013) slide