Are You Vulnerable?
The Tiger Team Approach

Purpose and Scope

- To present a best practice approach to securing your company
- To present real life examples of vulnerability assessment successes


Legal Disclaimer

- Don’t try this at home
- Get written permission before trying any of these techniques
  - The main difference between a tiger team and a burglar is permission

Juggling Tasks

Physical

Cyber

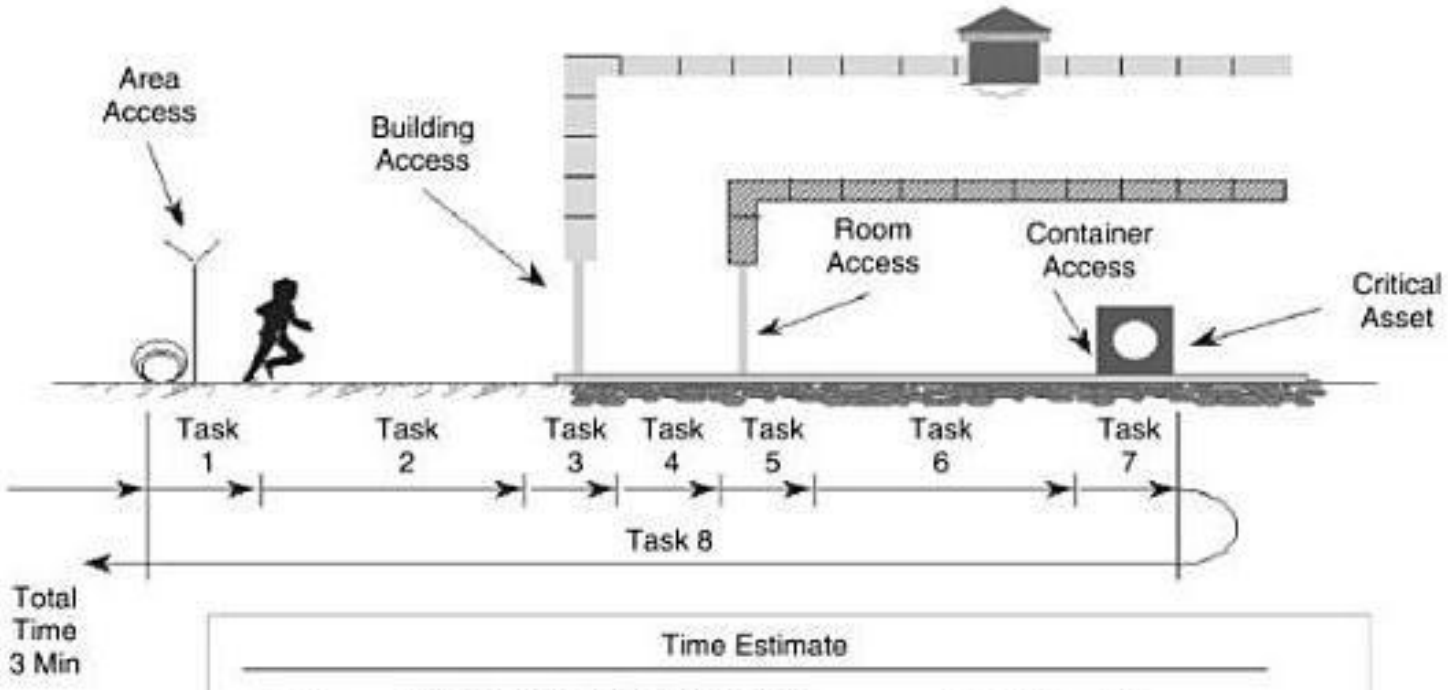
Regular Work

Privacy

Not Secure

Too Secure

Adversary Theft Path



Time Estimate

Task	Mean Time (min)	Cumulative Time (min)	Task Description
1	0.1		Climb over fence
2	0.3	0.4	Run 80 ft
3	0.8	1.2	Force door
4	0.4	1.6	Walk 50 ft
5	0.2	1.8	Cut lock
6	0.1	1.9	Walk to container
7	0.2	2.1	Open container and gather material
8	0.9	3.0	Escape
	3.0		Total (3 min)

Design and Evaluation of Physical Security Systems – Published by Butterworth-Heinemann

Deter – Detect - Delay

- Lock, Light & Limit Access
- View from bad guy's perspective

What needs to be protected?

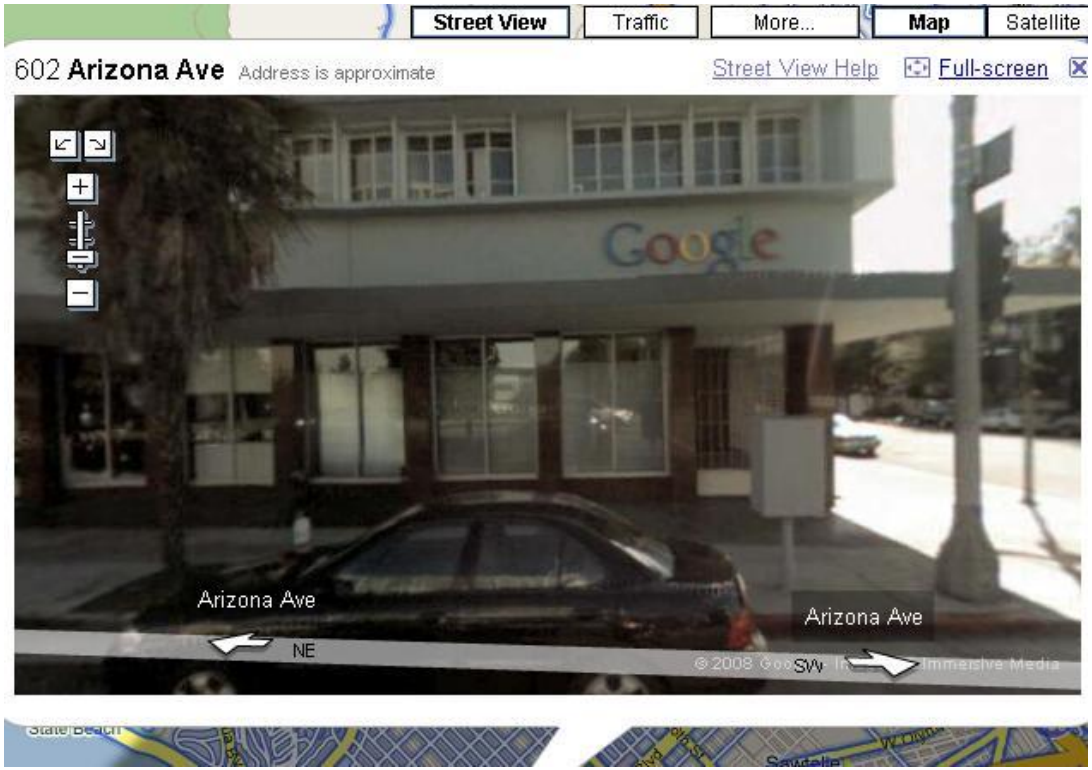
- Laptop = $1000
- SSN numbers - $2 each
- Breach notification - $18 - $209 per identity
- Bot herders can make $50k per month
- Copper - $3.20 /lb


Who are the bad guys?

- Insiders
  - Former or disgruntled employees
  - Click happy employees
- Outsiders
  - Thieves
  - Extremists / Terrorists
  - Hackers
  - Meth Heads

Discovery – Google hacking

- Password site:yoursite.com
- Filetype:doc site:yoursite.com classified
- Google Street View

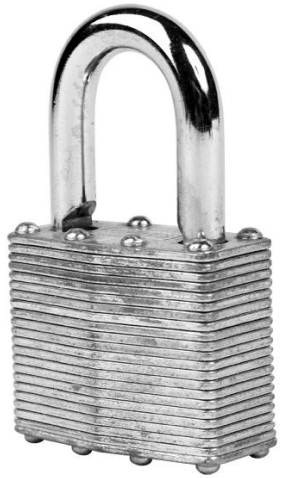


Insider Threat

- 60 percent of ex-employees leave with insider information
  - Enforce termination procedures
  - Limit access to those who need it
- View your network from an insider's perspective
  - Video: Lock your PC
- How many of your employees will click on an email I send them?

http://www.thetechherald.com/article.php/200909/3019/Almost-sixty-percent-of-ex-employees-leave-jobs-with-insider-information

- Locks keep honest people honest



Lock videos on the Internet

Video

http://www.youtube.com/whitehat1969

Tools of the Trade

Dumpster Diving


Techniques

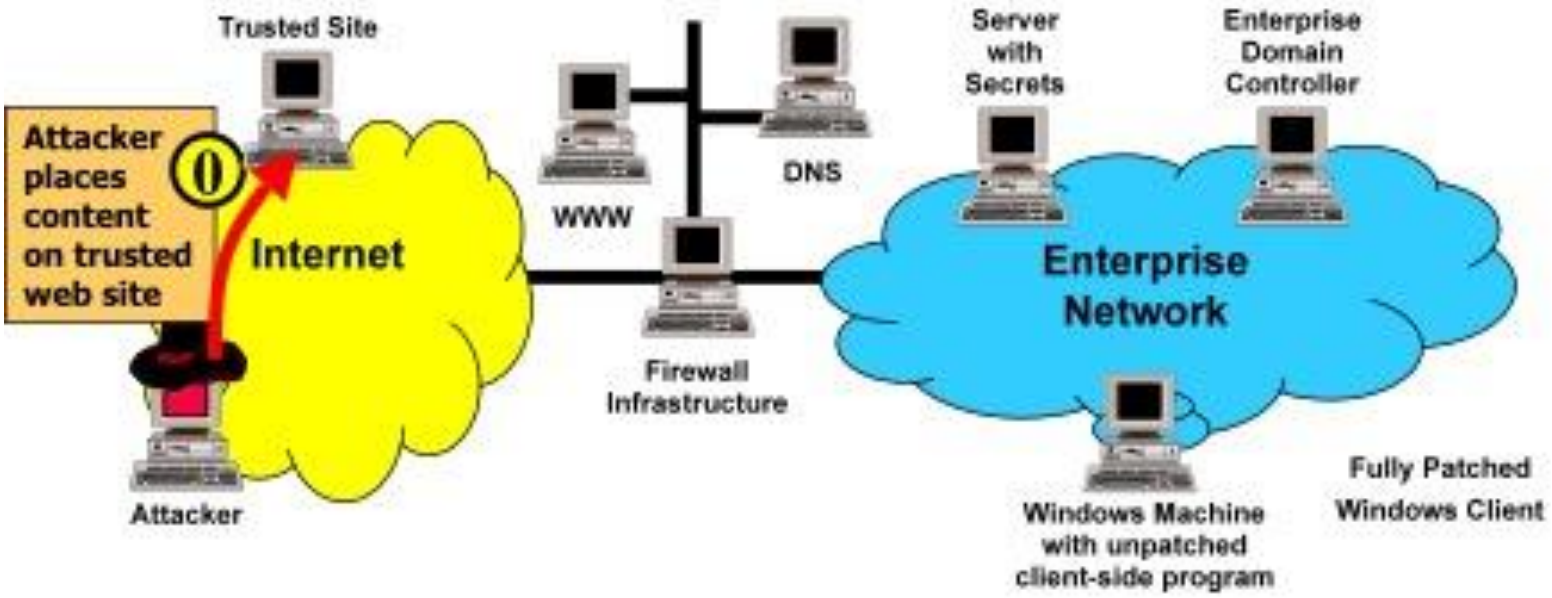
- Social engineering
- Social networking
- Lock by-passing
- Thumb drive sprinkle
- Dumpster diving
- Tailgating
- Out of office message
- Black box

Once I'm In

- Unlocked PC's & cabinets
- Unused network jacks
- Keyloggers

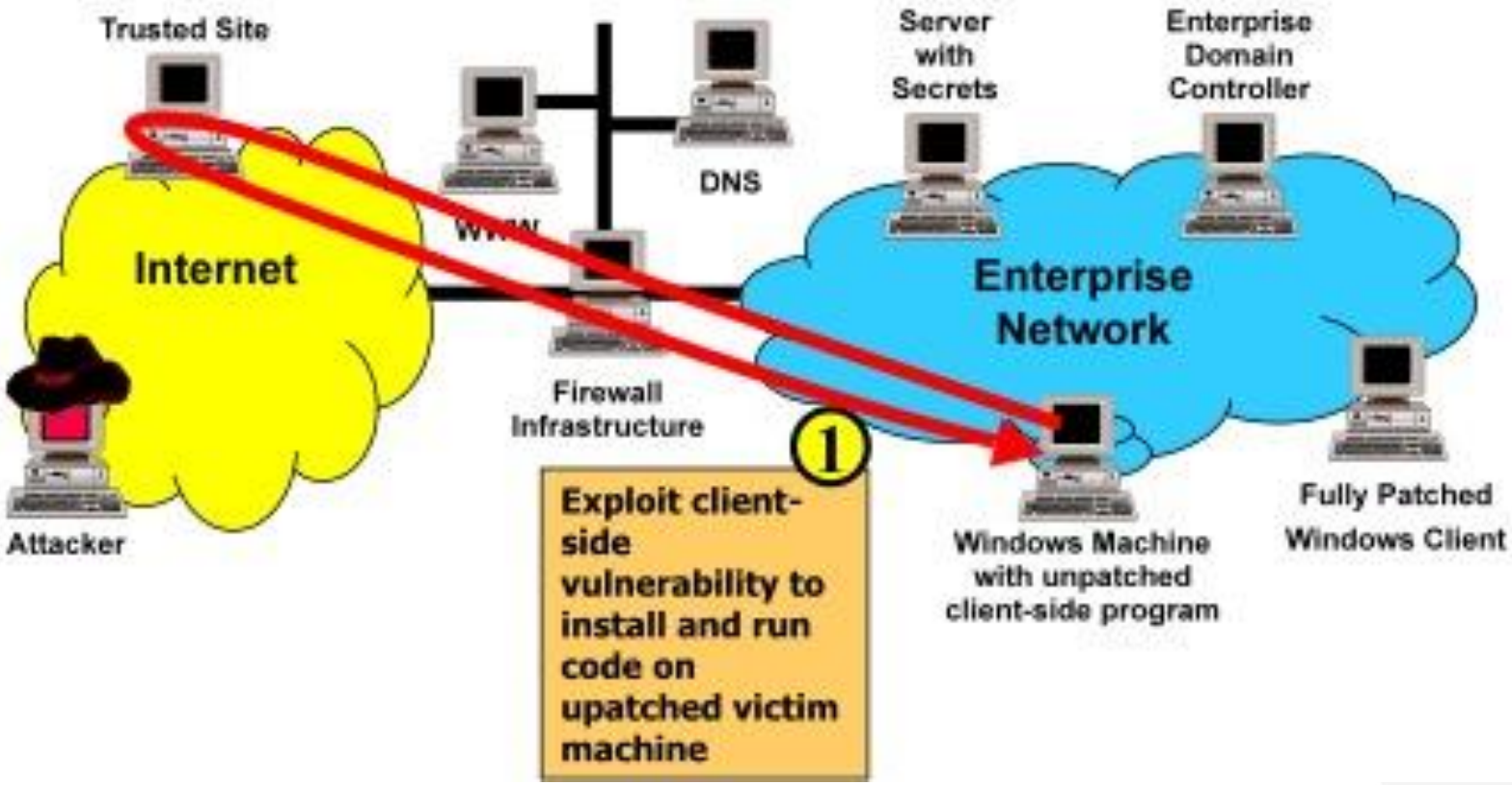
Client-Side Exploitation Example

- Step 0: Attacker Places Content on Trusted Site



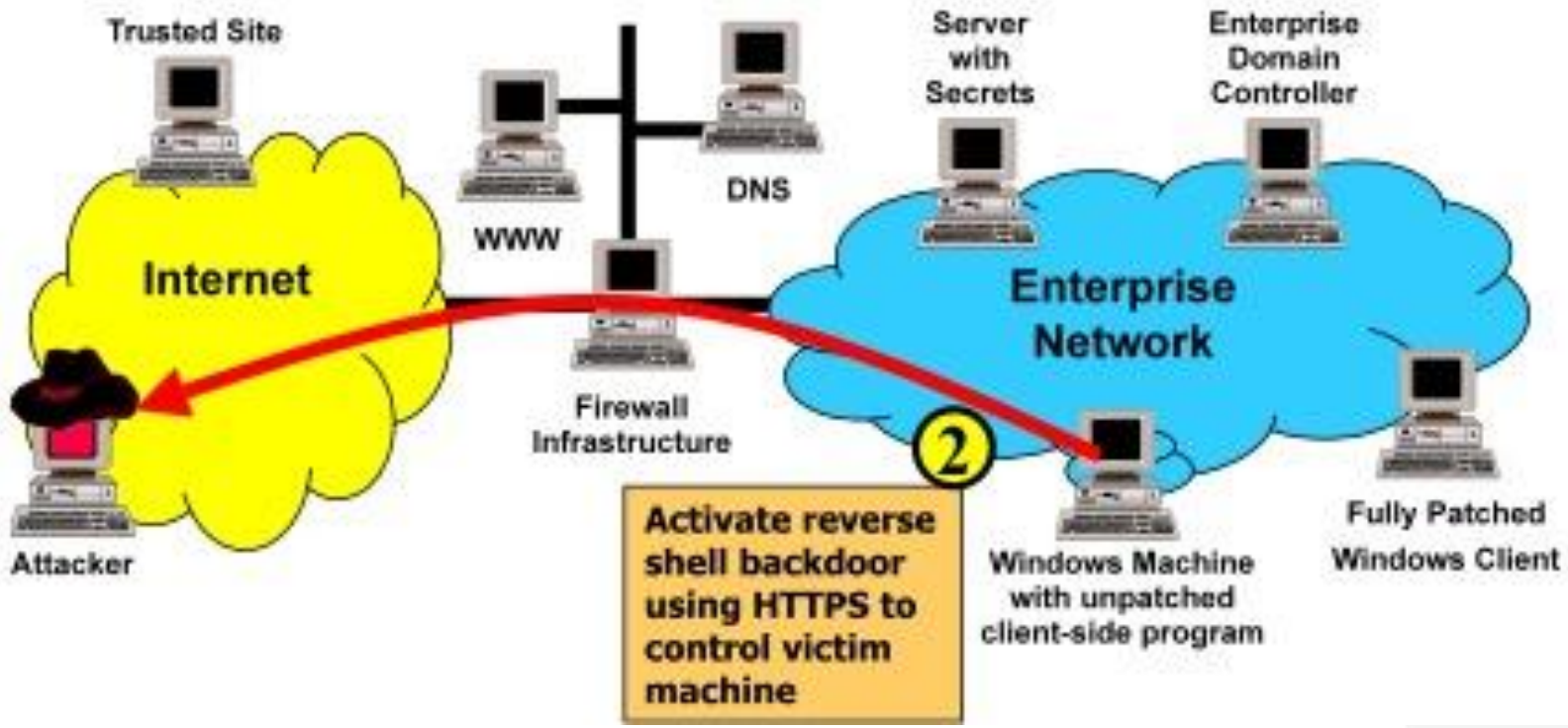

Client-Side Exploitation Example

- Step 1: Client-Side Exploitation



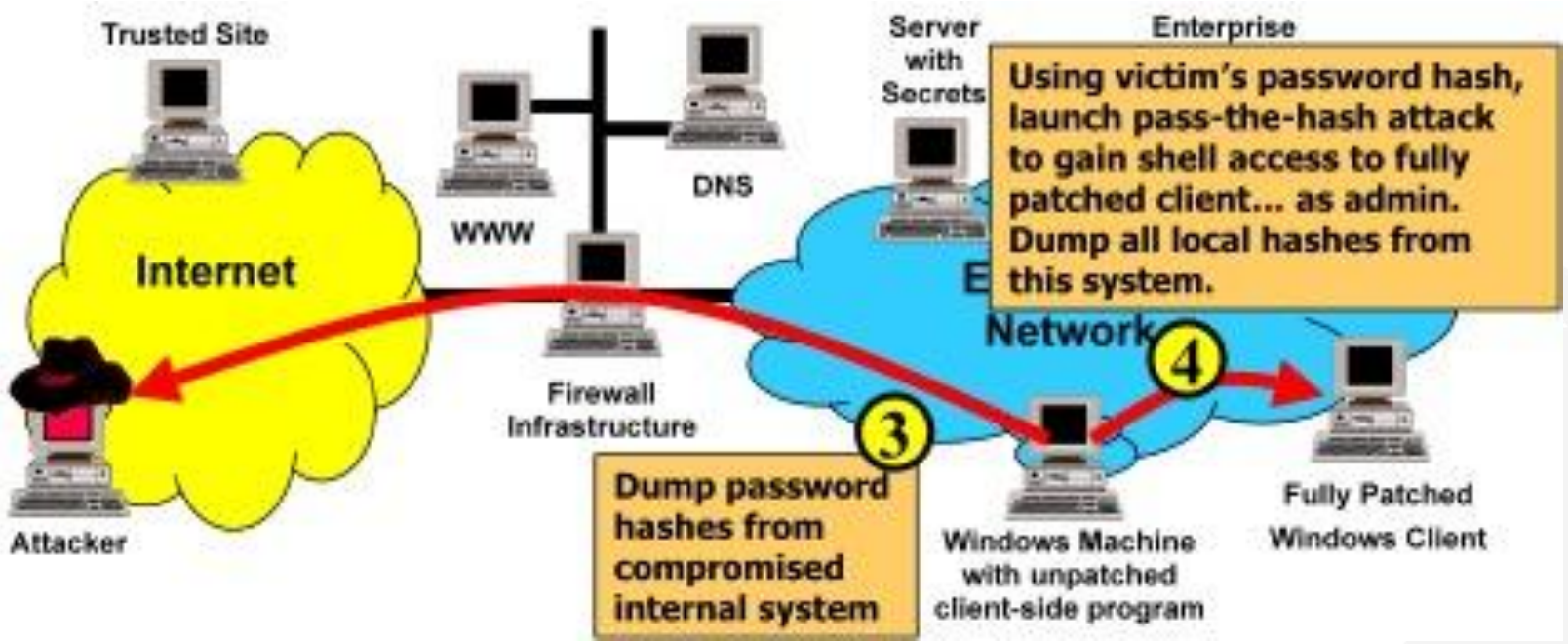
Client-Side Exploitation Example

- Step 2: Establish Reverse Shell Backdoor Using HTTPS



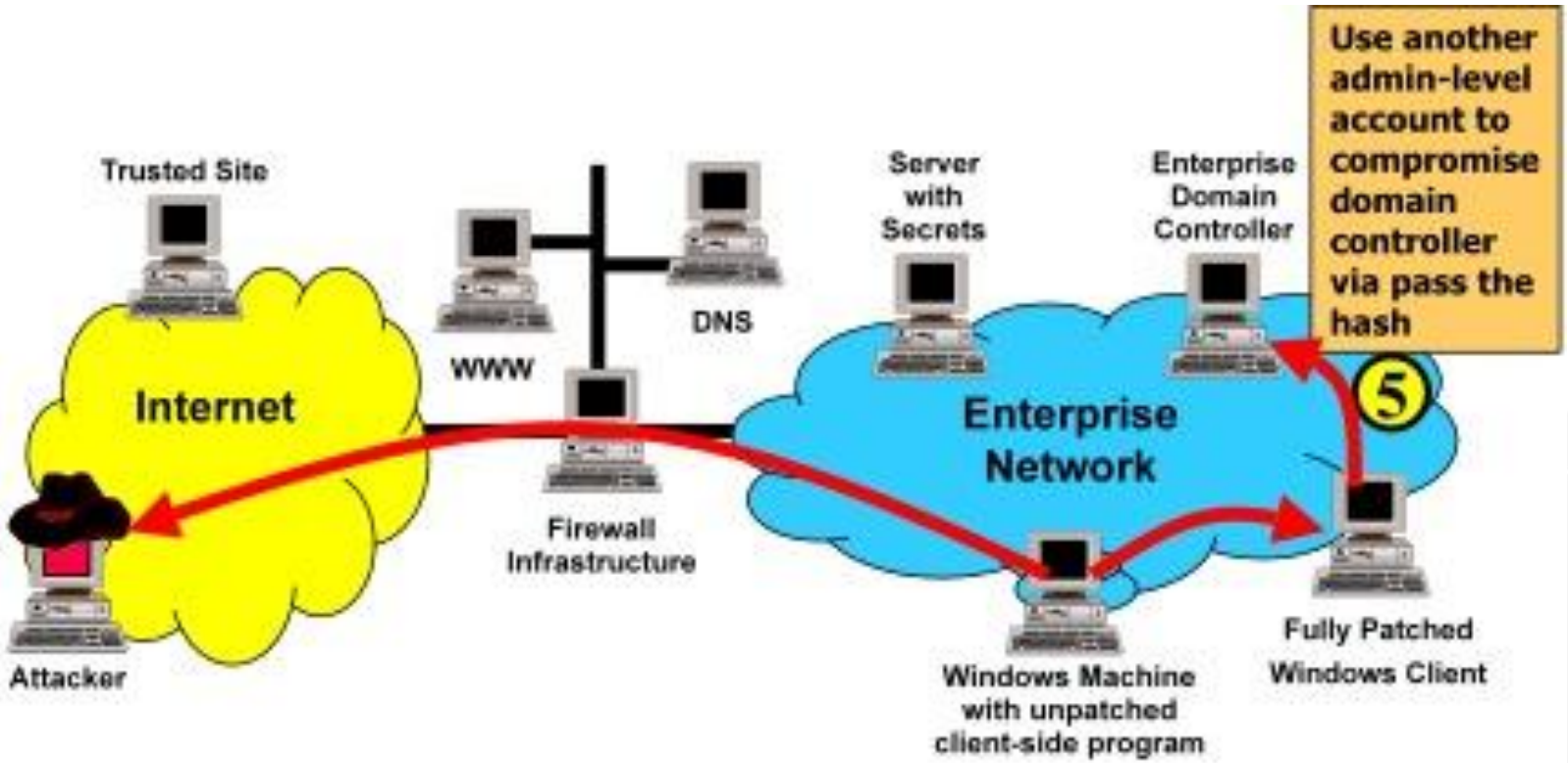
Client-Side Exploitation Example

- Step 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot



Client-Side Exploitation Example

- Step 5: Pass the Hash to Compromise Domain Controller

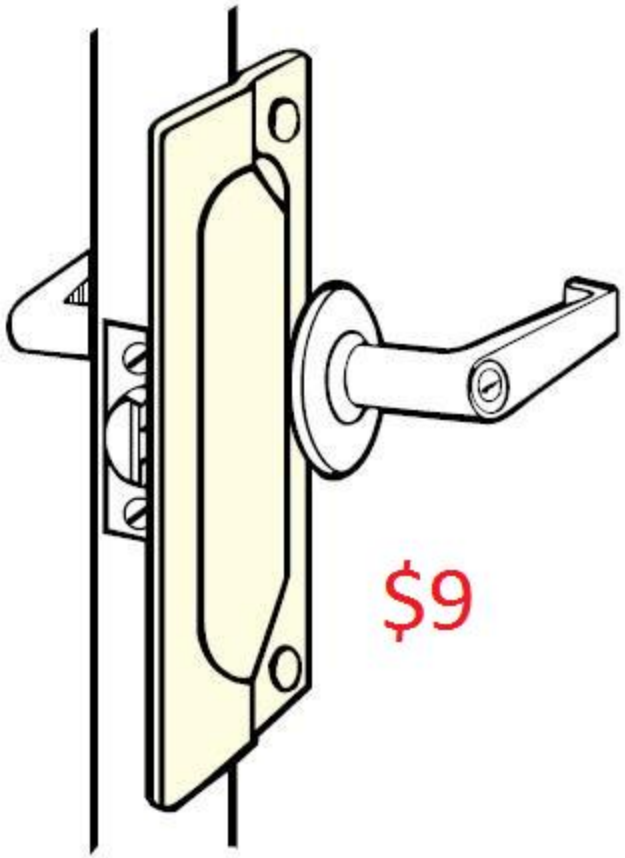


Tiger Team

Video

www.youtube.com/
whitehat1969

An Ounce of Prevention




Passwords

- Password Cracking
  - Identify weak or default passwords
  - Verify the use of complex passwords

Characters (complex)	Estimated time to crack
7	6 minutes
8	2.34 hours
14	9 hours
15	209 days


Pick The Best Password

password

Summer13

P@swordCompl3x

juggle13 google