Everything I Need To Know About Security I Learned From Watching Kung Fu Movies

Paul Asadoorian

Security Weekly, Founder & CEO

Offensive Countermeasures, CEO

Kung Fu Movie Enthusiast

The Tale Of The Best Hacker and Social Engineer In The World

About Me

- I run the Security Weekly podcast network
- I am the CEO at Offensive Countermeasures
- I've worked building security infrastructure, penetration testing and as a product specialist for Tenable Network Security
- I studied Kung Fu for about 10 years (Long Fist AKA Changquan and Tai Chi)
- I've watched A LOT of Kung Fu movies (500+)

DISCLAIMER

“The opinions, words, phrases, sentences, so-called facts, images, and/or videos expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of the conference, sponsors, affiliates, security vendors, or anyone else. Only Paul could guarantee the accuracy or reliability of the information provided herein (but does not anyhow).

If you are easily offended by imagery, puns, jokes, funny phrases, adult language and humor, or anything even close to the above, please excuse yourself from this presentation.”

Talk Outline

- **How did I come up with this talk?**
- **Episode 1**: The Student & Teacher Dynamic
- **Episode 2**: Security/Kung Fu Tactics
- **Episode 3**: Political & Social
- **Episode 4**: Other interesting facts
- **Bonus**: Paul's Top Ten List of Kung Fu Movies to Watch Before You Die

Episode 1: The Teacher & Student Dynamic

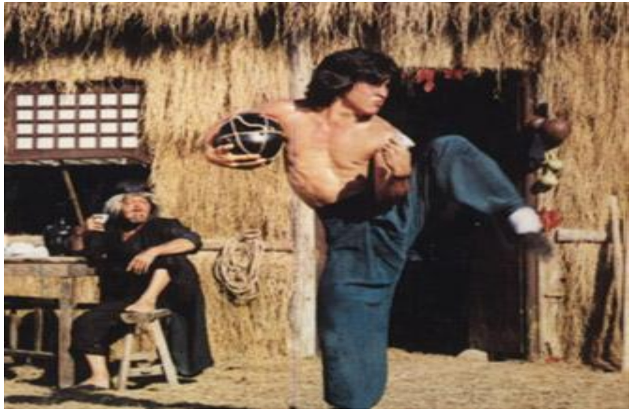
"He who is taught only by himself has a fool for a master."

- Ben Jonson

#1 Your master will be a hermit living in the woods, and reluctant to train you

Facts about Kung Fu masters in the movies:

1. They live on their own in the woods
2. They hide their skills
3. They are reluctant to train you



Your Hacker Mentor May Be Reluctant To Teach You

- Teaching people how to break things comes with moral responsibility (e.g. breaking the Internet)

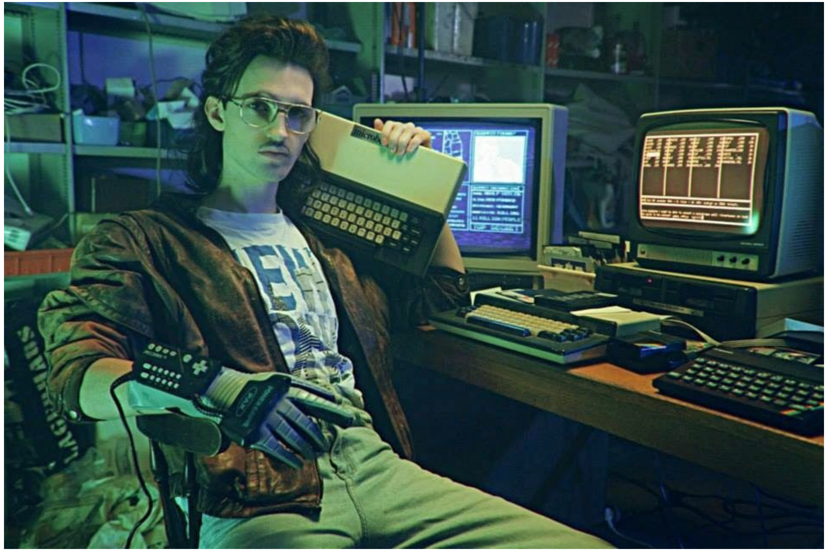
- Learning security is hard, the foundation is quite large, and people quit as a result

- Fortunately mentors are a few milliseconds away:
  - http://infosecmentors.net (Episode #504: https://www.youtube.com/watch?v=0N7CaznzrEk)
  - https://www.sans.org/mentor

You Hacker Mentor May Be Antisocial and not leave the house

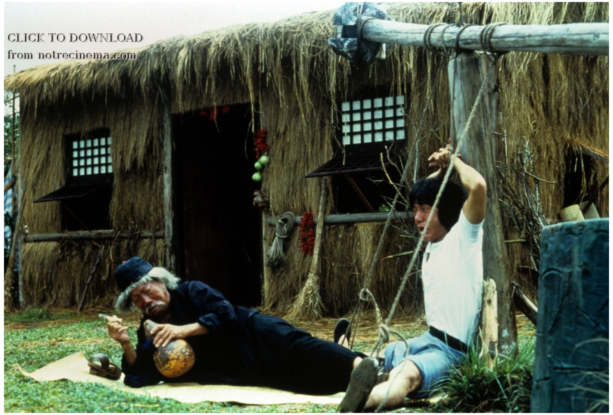
Many use the “cover” of the computer to communicate, and the Internet allows them to be “social”

IRC, Slack, Email, mailing lists, forums,Twitter, etc… are great ways to communicate to find mentors



“Hackerman” from Kung Fury (2015)

#2 Your master will be drunk and punish you for taking shortcuts



Your Security Mentor may be drunk and punish you for taking shortcuts

Shortcuts lead to:

Vulnerabilities in software/systems/networks

Pen test/vulnerability assessments that give people false hope

People who use the arrow keys in vi, never compile anything by hand, or just use Kali and call themselves a hacker

Too Many Shortcuts

Many do not do these three things and jump to solutions:

1. Know where your sensitive data lives and define different levels of sensitivity
2. Know where all your your systems and applications live
3. Know who is responsible for every system and application

Leave Drinking To The Masters

#3 You can learn Kung Fu by getting your ass kicked

If the master won’t teach you, just fight with them enough times so that you learn his style.

Note: This is **very** painful.

You can also bribe your master with a chicken….

"Master, let me be your student, and I'll give you a chicken."

You Can Learn Security By Getting Hacked

How did you get your start in Infosec? - “I was hacked”

Learn offense by playing defense: CCDC competitions

Getting hacked shows you how not to play defense and what a successful offense looks like.

Read About Others Who Got Hacked

http://pastebin.com/raw/0SNSvyjJ

Photo credit:
http://www.csoonline.com/article/2943968/data-breach/hacking-team-hacked-attackers-claim-400gb-in-dumped-data.html

Learning Kung Fu vs. Hacking

#4 Kung Fu masters have friendly battles where they fight to test each other's skills

Ip Man (Played by Donnie Yen) fights differently when challenged by a fellow master vs. when he is fighting for a bag of rice to feed his family...

← Lots of broken bones and dislocated limbs...

Realistic Training!

“Board don’t hit back.”

- Bruce Lee, Enter the Dragon (1979)

Challenge Yourself

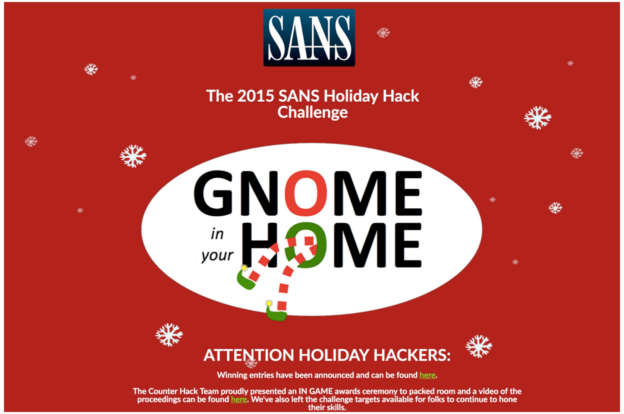
Enter a hacking competition, even if you believe your skills are not developed enough to win

Challenging yourself is more important than challenging your opponents

Take courses that you believe may be above your skill level

https://www.sans.org/course/advanced-exploit-development-penetration-testers
https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/

Hacking Challenges



SANS

The 2015 SANS Holiday Hack Challenge

GNOME in your HOME

ATTENTION HOLIDAY HACKERS:

Winning entries have been announced and can be found here.

The Counter Hack Team proudly presented an IN GAME awards ceremony to packed room and a video of the proceedings can be found here. We've also left the challenge targets available for folks to continue to hone their skills.

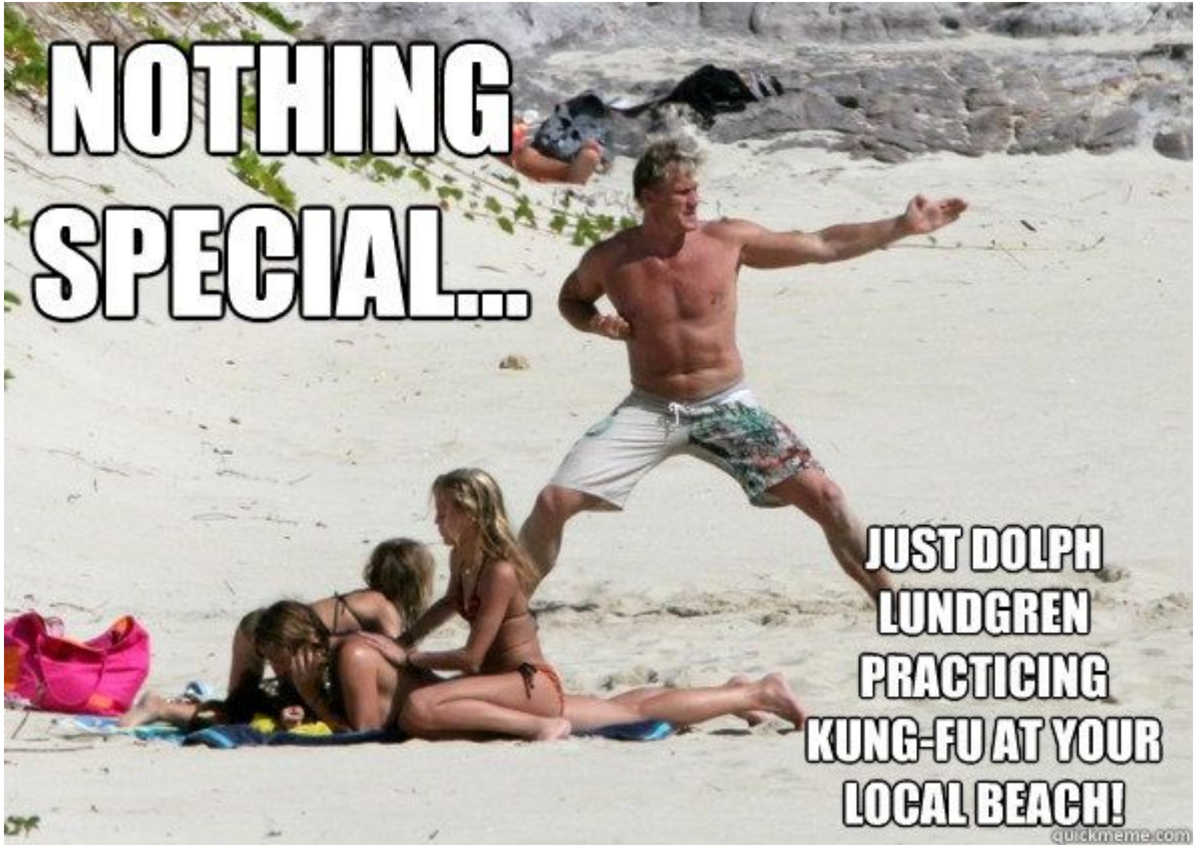
COUNTER HACK CHALLENGES

http://holidayhackchallenge.com

http://counterhack.net/Counter_Hack/Challenges.html

https://www.counterhackchallenges.com/

Episode 2: Security/Kung Fu Tactics



#5 If you are in a restaurant, there is a 100% chance you will have to fight

Seriously, when does everyone eat?

If you’re on the Internet, You Will be hacked

You are in a Kung Fu movie, in a restaurant every day as an information security professional.

This means you are always engaged with attackers

Threat Hunting is a growing technique, rather than look for vulnerabilities or malware, look for the after effects.

“Everyone has a plan until they’ve been hit.”

~ Joe Lewis

Open Source Threat Hunting

Bro IDS (https://www.bro.org/) - Deploy sensors and analyze network traffic

RITA: https://github.com/ocmdev/rita

Hunting Tactics: https://github.com/ThreatHuntingProject/ThreatHunting

Threat Intelligence: https://github.com/hslatman/awesome-threat-intelligence

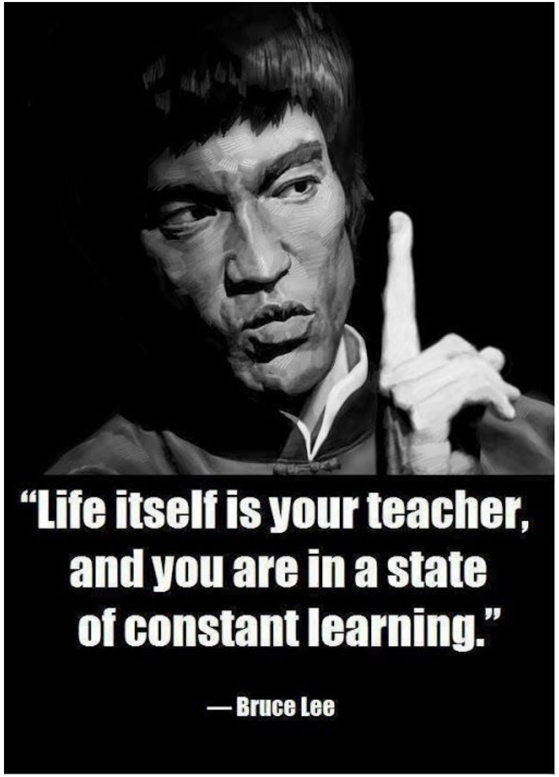
#6 If you rush your training, you will get your ass kicked 100% of the time

Gordon Liu fights Pai Mei like 3 times until he finally wins

He rushed his training, and paid the price...

Clan of the White Lotus (1980)

Don’t Rush: Learn By Doing



- The best security professionals spent time on the help desk, systems/network administrators and/or developers
- Learn how to properly build software/systems before attacking or defending it
- Learning how networking, operating systems and software works goes a long way, anything else is a shortcut
- There are exceptions, such as researchers

Proper Training

1. Have a plan (What are your goals?)
2. Build a lab
3. Signup for free / low cost training (cybrary.com and/or itpro.tv)
4. Practice every day or at least on a regular schedule
5. Get a mentor

#7 There is always someone more skilled than you

Wing Chun, played by Michelle Yeoh, is dressed as a man, many underestimate his/her skill.

Spoiler: She kicks everyone’s ass.

There is always someone more skilled than you

Attackers may be more skilled than you, learn from it

Others in the security community may be more skilled than you, learn from them

Don’t poke fun at those who may be less skilled than you

Be nice when people ask questions (Don’t be a D***)

#8 The weapon you choose matters little, it takes skill to win

Unless you’re Lau Kar Leung, he’s awesome with no weapons and with every other weapon you can think of.

He was also one of the primary lineage masters of Hung Gar Kung Fu.

This is a big deal.

He was TEACHING kung fu at 5 years old….

Just because you have a sword…

© 1997 TriStar Pictures, Inc. All Rights Reserved.

Build Your Own Tools

For fun I’ve written:

- A portscanner in C
- A honeyport script in Python
- A DNS blacklist in Bash

Tools Never Beat Experience and Training, However:

"I used [Gary] Kasparov as an example, although he is famous for playing chess, he is also famous for getting beat by a computer. However, after he was beat there were "freestyle" chess championships where combinations of computers and people worked together on teams. The results were fascinating, those groups that had humans, computers and a solid process were able to beat more powerful computers alone."

https://www.linkedin.com/pulse/applying-machine-learning-security-without-phd-ken-westin

#9 The best defense is always to have a good offense

Good Jet Li: Bagua (Walk around the wall)

Bad Jet Li: Xing Yichuan (Break through the wall)

In Xingyi, every block is also an offensive strike.

Web Apps: Block & Strike (Or at least block!)

Akamai

IM

WAF

CITRIX

Barracuda

f5

VERACODE

RASP

CONTRAST SECURITY

PREVOTY

CLOUDFLARE

Cloud DMZ

SOHA

SENTRIX

Web protection platform

Signal Sciences

IMMUNIO

“WRCD”

(WAF-RASP-Cloud-DMZ)

#10 The “softer” styles of Kung Fu always lead to victory

Tai Chi Master (1993)

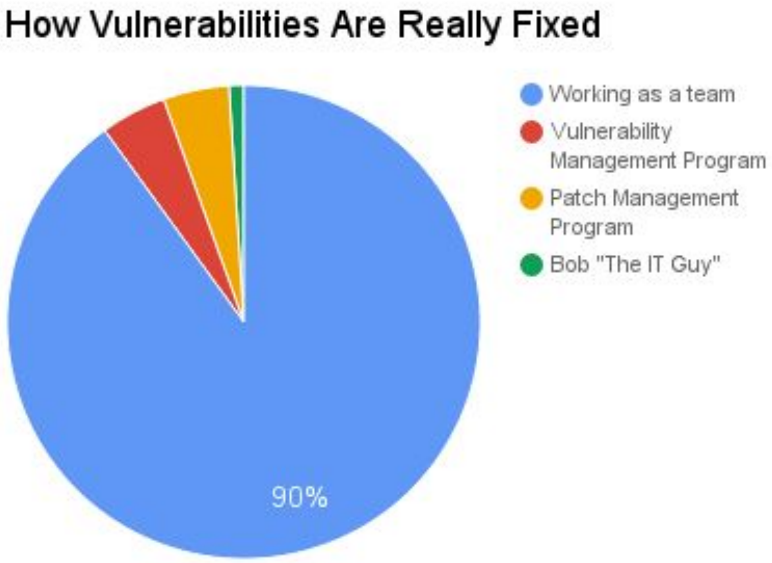
Kung Fu Hustle (2004)

“Who overcomes by force, hath overcome but half his foe.”

- John Milton

“Softer” styles of security

Communicating risk to the administrators and management



“Softer” styles of security

Developing an effective incident response program

“Softer” styles of security

Convincing an industry to produce more secure products

I am The Cavalry

Photo Credit: wired.com

You Don’t Need Expensive Tools To Win

You can fight with your hands or an umbrella

For training, you can use rocks, eggs, rope, wood, buckets

You Don’t Need Expensive Tools To Win

Incident Response: CyberCPR (https://www.cybercpr.com/)

Network Monitoring: Bro IDS (https://bro.org)

IDS: Suricata (https://suricata-ids.org/)

Vulnerability Scanning: OpenVas (http://www.openvas.org/)

Firewall: pfSense (https://pfsense.org/)

Threat Hunting: Microsoft Advanced Threat Analytics

Reach out to a security startup today!

Episode 3: Political & Social

#11 The bad guys are always in cahoots with the government

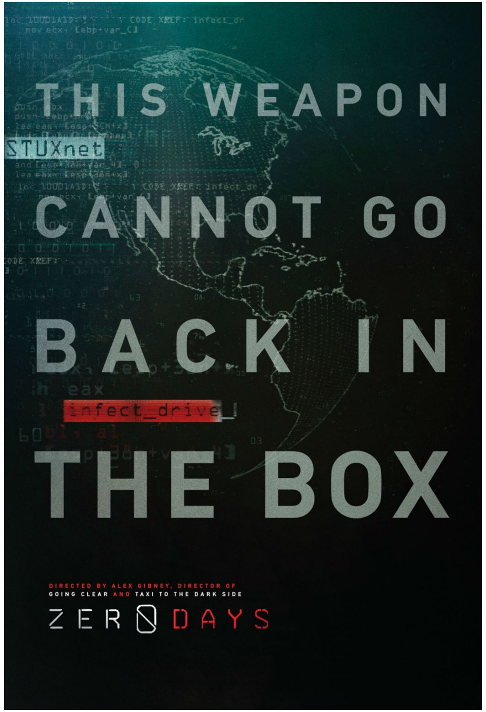
Many Kung Fu movies tackle the political and social issues throughout Chinese history

“Bad Guys” are usually associated with the Government

Take from that what you will...

State Sponsored Hacking

- This was the year when state-sponsored hacking became mainstream
- “Hacking” the US presidential election was a big story
- “Zero Days”, a documentary film on Stuxnet, was released.
- Several companies now offer “darknet” monitoring services.


THIS WEAPON CANNOT GO BACK IN THE BOX
STUXnet
infect_drive
DIRECTED BY ALEX GIBNEY, DIRECTOR OF GOING CLEAR AND TAXI TO THE DARK SIDE
ZER0 DAYS

#12 Protagonists Want to Learn Kung Fu Primarily to Take Revenge!

Gordon Liu’s character in *“8 Diagram Pole Fighter”* (1983) travels to the Shaolin Temple to learn Kung Fu in order to take revenge against the Government officials who murdered his family.

Revenge Hacking

Never a good idea

Tracking and locating attackers is about the extent

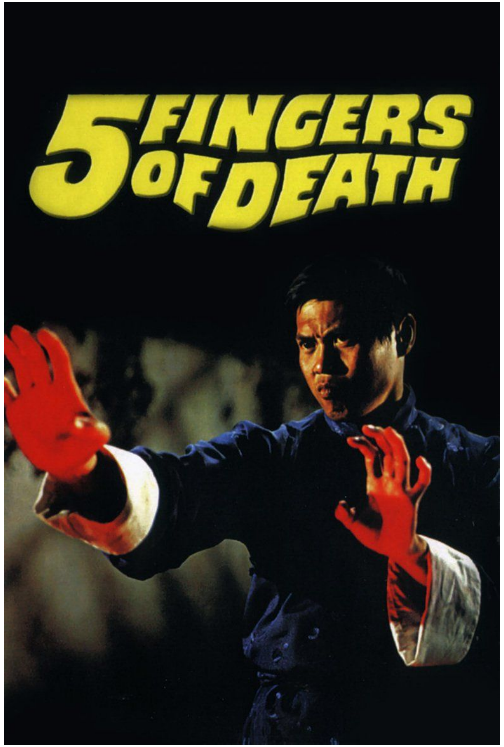
Even then, the FBI's "Playpen" operation has drawn much controversy

Anything more is still, largely, illegal

#13 The most popular Kung Fu movies aren’t always the best ones

King Boxer (AKA 5 Fingers Of Death) was released in 1972 and credited with starting the “Kung Fu” craze in the US.

It was just an okay Kung Fu movie...



The Most Popular Vendors Aren’t Necessarily The Best!

Large Anti-Virus vendors are trying to implement innovative detection features, and largely failing

Traditional security vendors (e.g. firewalls) are falling behind as everyone moves to the cloud and SaaS

Big players in SIEM are losing to smaller and innovative companies that do much more with the log data

#14 Students use Kung Fu to overcome personal challenges or shortcomings

Blind, mentally challenged and missing limbs are the basis for this classic 1978 film titled *“The Crippled Avengers”*. Guess what? They learn Kung Fu and take revenge...

Many Use Hacking To Help Overcome Personal Challenges

Confidence - We’re all trying to do the right thing and protect “Things”, and most people present their new ideas publically

Community - The security community is **<u>awesome</u>**

Challenges - There is always a new challenge in security as it constantly evolves

We have our own awkward hugs web site!

#15 The righteous path is fraught with peril, but always leads to a hero

The protagonist often has to endure several challenges in order to learn Kung Fu

They fail, and they get back up

Kung Fu - “Skill derived from effort”

Security is Hard.

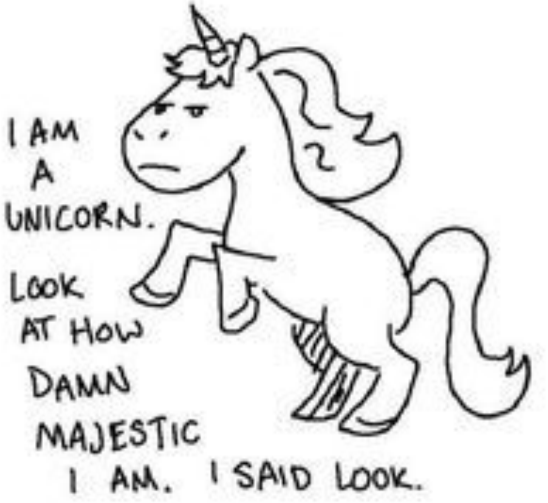
Things you never hear, or if you do people are lying:

"Securing my network was easy, I just did X"

"You can just do X and prevent breaches"

"I bought X and I've been secure ever since!"

Security is achieved through hard work and persistence.



#16 Sometimes are heros don’t start out as such

Now Good Guys...

Other Useless Kung Fu Movie Facts

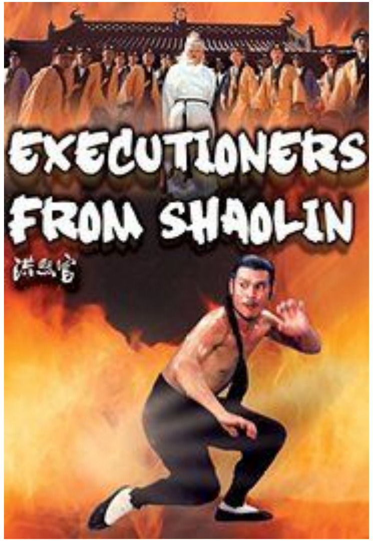
"Your Kung Fu is useless against me, now tell me who your lousy master is!"

Paul's Top Ten List of Kung Fu Movies to Watch Before You Die

1. Iron Monkey
2. Shaolin V. Lama
3. Once Upon a Time In China
4. 36th Chamber of Shaolin
5. Fist of Legend
6. Legendary Weapons of China
7. The Legend of the Drunken Master (Drunken Master II)
8. The 8 Diagram Pole Fighter
9. Enter The Dragon
10. Fearless

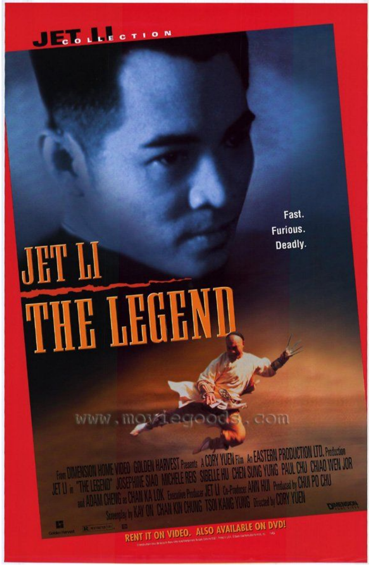
Five more for good measure:

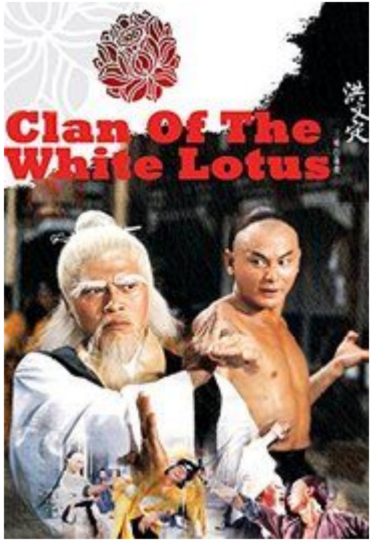
- Hero
- Executioners from Shaolin
- The Prodigal Son
- Five Deadly Venoms
- IP Man



Oh what the heck

- The Legend
- Tai Chi Master
- Wing Chun
- Crippled Avengers
- Clan of the White Lotus


JET LI COLLECTION
Fast.
Furious.
Deadly.
JET LI
THE LEGEND
www.moviegoods.com
From DIMENSION HOME VIDEO GOLDEN HARVEST Presents A CORY YUEN Film An EASTERN PRODUCTION LTD. Production
JET LI in "THE LEGEND" JOSEPHINE SIAO MICHELE REIS SIBELLE HU CHEN SUNG YUNG PAUL CHU CHIAO WEN JOR
and ADAM CHENG as CHAN KA LOK Executive Producer JET LI Co-Producer ANN HUI Produced by CHUI PO CHU
Screenplay by KAY ON CHAN KIN CHUNG TSOI KANG YUNG Directed by CORY YUEN
DIMENSION
Golden Harvest
RENT IT ON VIDEO. ALSO AVAILABLE ON DVD!



Best on screen martial artists

- Bruce Lee
- Jet Li
- Donnie Yen
- Gordon Liu
- Jackie Chan

We can’t all be the greatest on-screen martial arts masters of all-time, but I tried. (And yes that is a shovel....)

Ridiculous Kung Fu Facts

- People have moles, and moles have hair
- There will be extreme closeups
- The dubbing will be bad, like really bad
- Common phrases: *"But still…", "You must be tired of living!", "Buddha's name be praised", "still much to learn"*

http://www.earnshaw.com/memoir/kung-fu-flick-dubbing

Paul Asadoorian

paul@securityweekly.com

@securityweekly