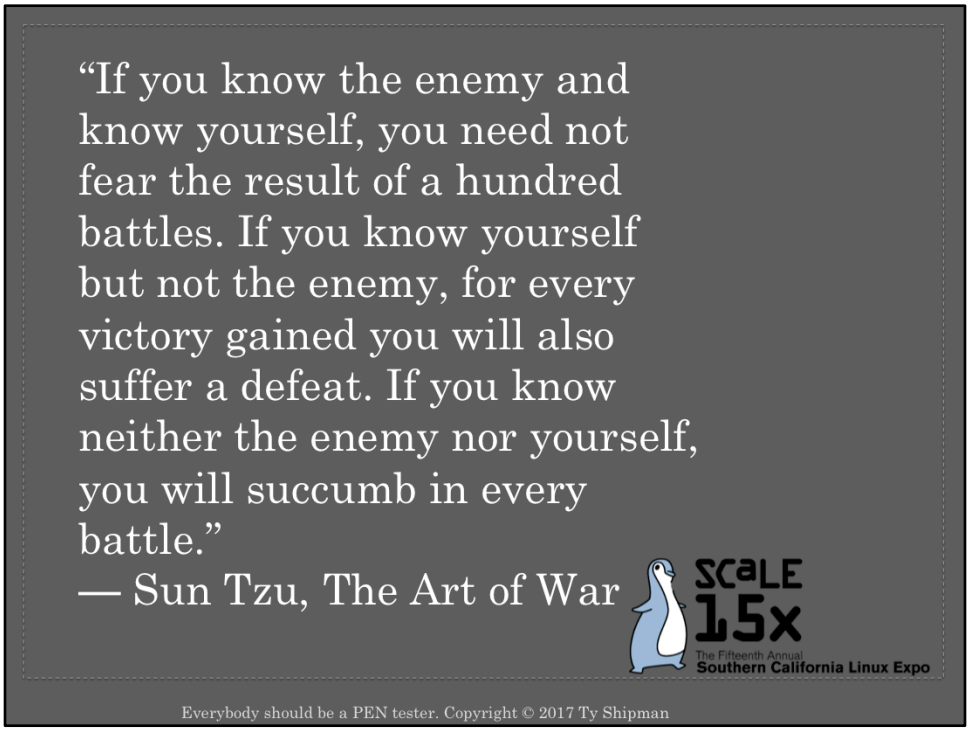
Please view my linked-in page (under See more) to get a copy of this presentation.

I can't post the names companies I work do consulting for much of the time; because they are trying to shore up their systems before bad things happen.

If you have any questions, please contact me via email.

Thanks,
Ty



Please hold questions to the end. This a LIGHTING talk with lots of info. Slides will be posted by the conference team, or look on my linked-in profile (under "See more…") for a link to download.

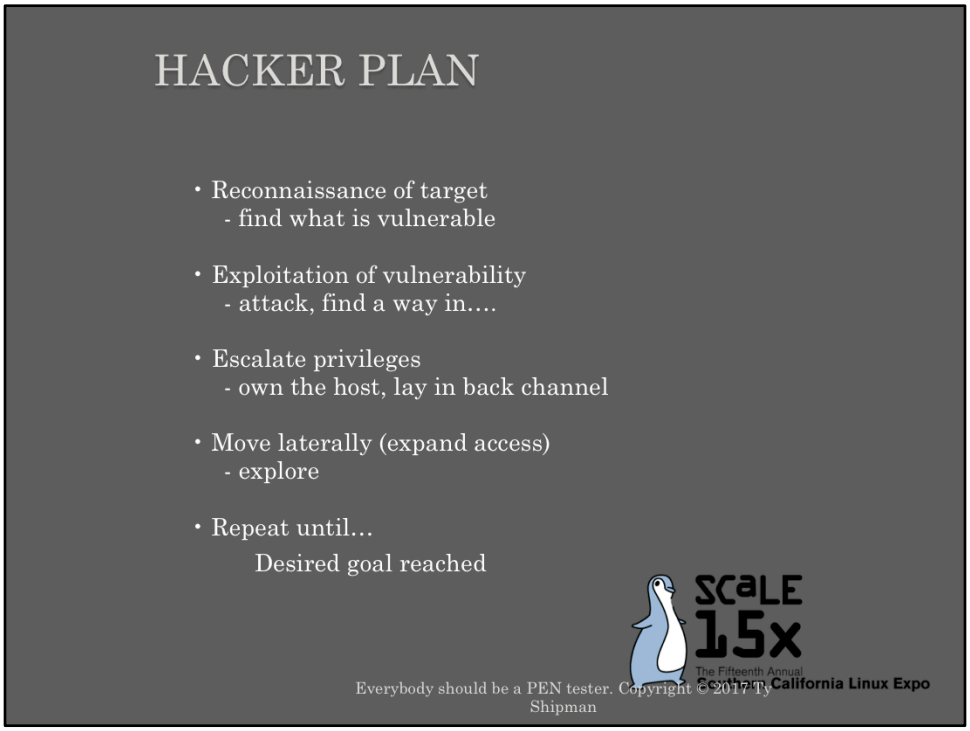
Do you know how well you are protecting your systems, can you prove it? Can you think like a hacker?

This talk is a result of a lesson I learned after taking a PEN test training class one weekend. More training and work after that was required to become a moderately successful PEN tester. I don't do PEN testing for a living yet; I just use my inadequate skills to scare my clients into hiring great PEN testers and adopting some of the solutions I suggest after I audit them.

1) I contend that if you do no know the basics of PEN testing (attack), you cannot adequately protect (defend) your environment. Nor do you understand why you are doing some of the tasks you are doing today to try to protect your environment.

2) Most people in this room or reading these slides either IT or DevOps professionals. You are wearing many hats; your overworked, and maybe even be underpaid. But if you cannot PEN test your hosts and applications at a basic level; thus alerting your team or yourself to the vulnerabilities that a script kiddy may find you are not doing an adequate job.

3) My presentation will layout an argument that I hope will cause you to go and seek a weekends worth (or more) of PEN test education. Why, you are a professional and need to keep you skills current, so add a new bolt to your quiver and maybe even get a raise. Who knows you might even jump to PEN testing as your next career.



The plan both hackers and PEN testers is roughly the same. Both want to get in and reach their desired goal. The PEN tester's goal is to prove they were on your system (screen dump of root/Admin login); hackers want… – you make the guess.

I will say this -- if a dedicated hacker team (organized crime, nation state) wants in, they will find a way. You want to make it harder so you don't end up a victim of a smash and grab hack; e.g. add bar to the windows and doors, outside lights, a roaming security guard, dogs, a mine field, ….

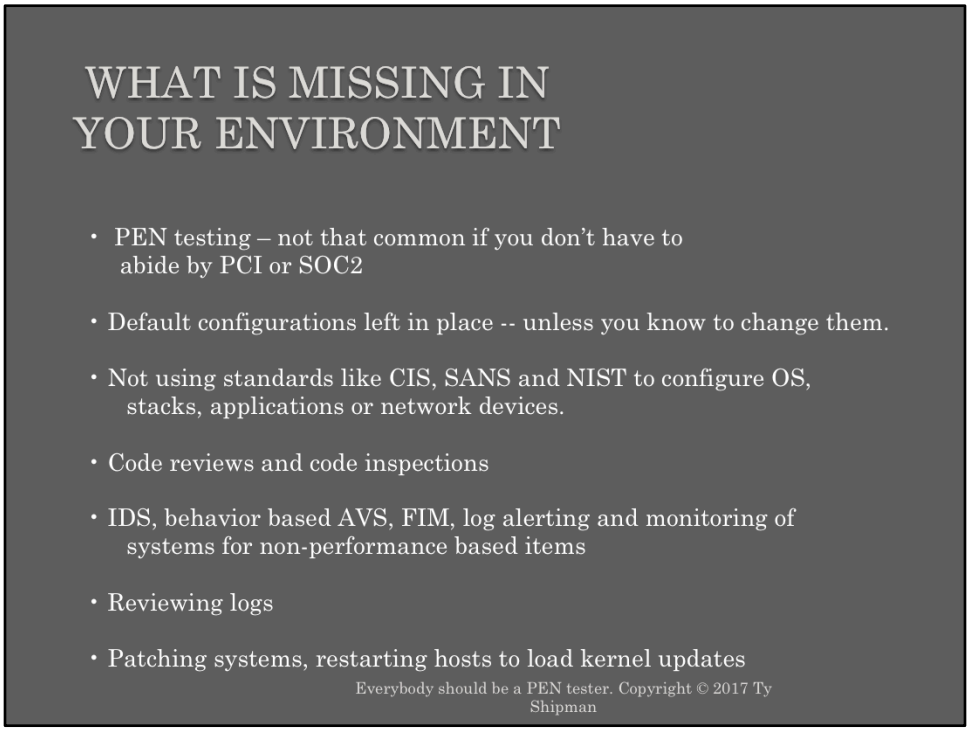
- Reconnaissance of target
  nmap, study API, applications, VUL Scan
  Old OS/software, vulnerable configuration on switches and software
  -- find weakness

- Exploitation of vulnerability
  Apply one of the known exploits (Metasploit module), or develop a new one

- Escalate
  Get to root/admin account so they own machine

- Move Laterally (expand access)
  Go deeper into environment

- Repeat until… Desired goal reach



I am going to make a lot of assumptions here, not all of them will be correct, but some will be. If any one of these is true, then you likely have vulnerabilities in your environment that can be exploited.

You don't work for a 250+ person company and likely don't have a dedicated security person/team to help you protect your environment.

You have never had a PEN tester come in and try to break into your systems.

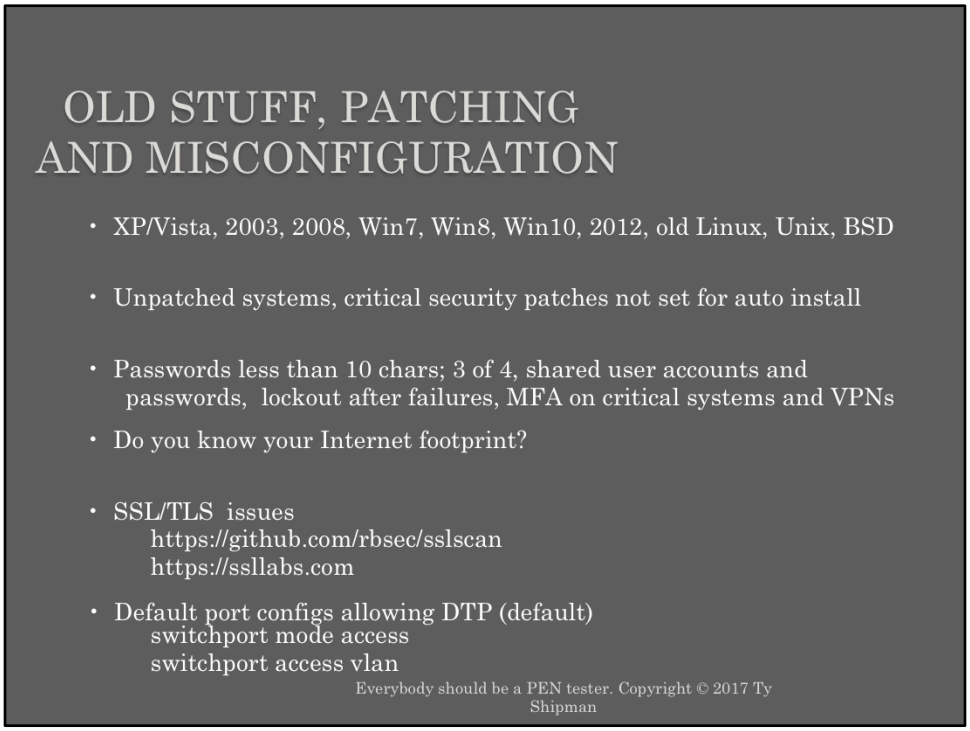
Like most IT/Network/DevOps people you have to learn new skills all the time and most solutions are taking snippets of code/configuration/knowledge from Google results and applying them – so you might not have a full picture of the issues at hand when it comes to security.

You don't configure your systems, application stacks using any standards. Did you know there are good security/hardening standards for Windows Servers, Apache, and Linux/Unix available? Look up CIS hardening standards.

You or your management think your firewall will keep the bad guys out. You need to add IDS, AVS system based on behavior, FIM and log management, monitoring and alerting systems.

You or your management think your IDS will help you stop hackers – it only alert you most of the time.

You don't aggressively patch your systems and application stacks.
When was the last time you restarted all your Linux 2.x or 3.x kernel systems? Are you on Linux Kernel 4.0 or have a live patching installed?



1). Old systems can be owned by bad actors in minutes, you learn how to own a host in the AM part of a basic PEN testing class. Anyone have an old card key management system around? How about the front desk security guard station host?

2). Failure to install critical security patches is like leaving a window open when you have bars on the front door.

Once a vulnerability is announced, there is usually an exploit available within 2-3 weeks on the Dark Web . The early versions cost several hundred dollars, later they go down to the 10s.

I have heard statics that say you can rent a Botnets for $1000-2000 that you can scan the Internet in less than 24 hours for a single vulnerability.

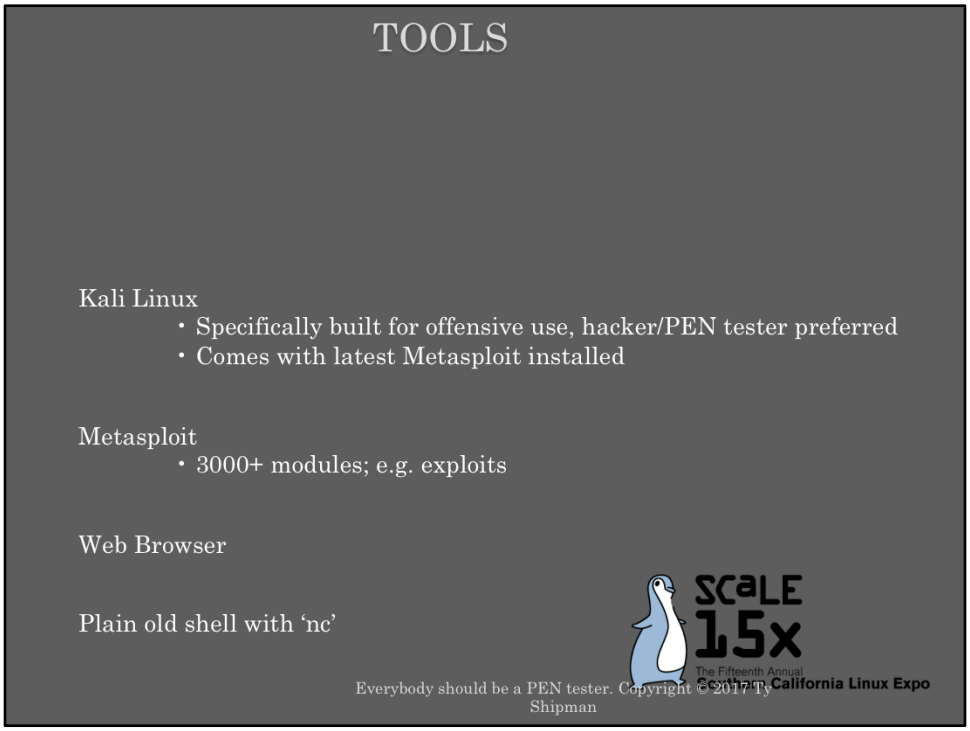
3). Brute forcing passwords on hosts and VPN are now a norm. Do you lockout after 6 attempts?

4). NMAP **ALL** your external IP address, find out what is open. Running on AWS, Google or Asure – review security rules.

5/6). SCALE 15X site received an A, my medical history site received a C before I reported issue, now A-.

7/8)..DTP – Dynamic Trucking Protocol – a bad actor can skip around your VLANS if not locked down. See https://digi.ninja/blog/abusing_dtp.php for more info.

Lastly, if you can do it, set switches to accept only 1 MAC address (Look up **'Sticky MAC**' or '**port-security mac-address**') – be careful here.

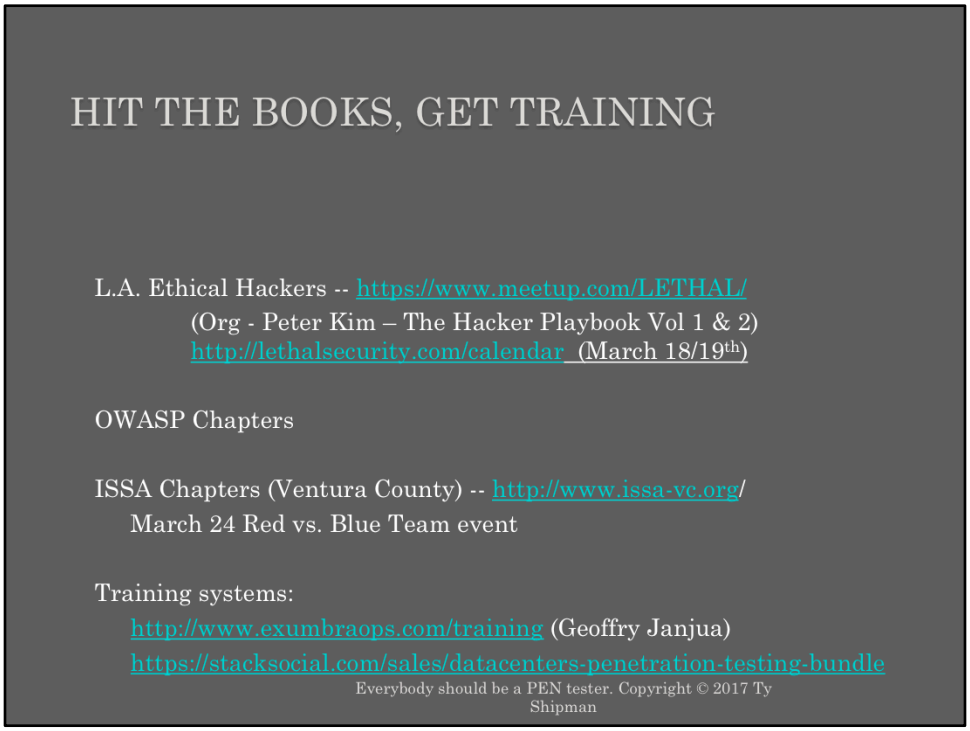


Both Kali and Metasploit have community versions that are free to use, they are maintained by security companies that specialize in offensive PEN testing.

nc ➔netcat

Metasploit is a great package. It has so many of the basic exploits (exploits are how to abuse a vulnerability, they include 0-day, remote attacks, shell code hacks). You need to do PEN testing that it is used by many script kiddies to break into system all over the place. Learning the basics takes a few hours, to really get a good grasp on the system you need about 30 hours.

Vendor	VUL
Microsoft	4700+
Oracle	4100+
Apple	3600+
PHP	550+
Google	2300+



Now that I have scared, let me tell you where you can get some skills to become a PEN tester to help you plug the leaks in your environment.

If you are not in the Southern California area, I suggest you look online for training by local OWASP, IEEE, ISSA and ACM chapters.

Beyond the links listed above you should subscribe to the NVD list that send out weekly and zero day alerts: https://nvd.nist.gov/