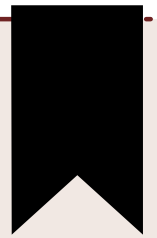
Introduction to Ethical Hacking



Hacking before you get hacked!

About Me

Who is a Hacker?

- **HACKER** *noun.* 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities….

  2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.
- **Old School Hackers**
- **Script Kiddies or Cyber-Punks or a Packet Monkey**
- **Professional Criminals or Crackers**
- **Coders and Virus Writers**

Ethical Hacking

- **Ethical hacking** – defined “methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems’ operating environments.”
- Security has been a major issue and concern for business, government and citizens as the Internet grows.
- Solution to security problems can be solved by a “hacker minded” individual.
- Now, Saving a business from the embarrassment of being hacked, is to have independent computer security professionals attempt to break into their computer systems before the bad guys...

What do Ethical hackers do?

- The main purpose of having an independent security professional evaluate a system/application security is to seek for answers and truth!
- How prepared are you? How secure is a system or application deployed.
- The overall questions that arise from these penetration testings are:
  - What can an intruder see on the target systems?
  - What can an intruder do with that information?
  - Does anyone at the target notice the intruder's at tempts or successes?
  - What are you trying to protect?
  - What are you trying to protect against?
  - How much time, effort, and money are you willing to expend to obtain adequate protection?

What skill sets should a good Ethical Hacker have?

How to program/script (Python/C/asm)

Using Linux & other Open-source Tech

Basics of OSI model and Networking

Basics of System Internals

- Other:

Hiding traces, post exploitation skills, Exploit Research, understanding Business Impacts and

How to mitigate and report found vulnerabilities

Modes of Ethical hacking

- Insider attack
- Outside attack
- Social engineering
- Physical Entry
- Stolen equipment attack
- Bypassed authentication attack

Hats Hackers Wear :)

- **White Hats :** skills used for defensive/offensive security analysts
- **Gray Hats:** offensively and defensively. Hacks for different reasons, depends with situation.
- **Black Hats:** Highly skilled malicious, destructive crackers.
- Others:

  Hactivisim – hacking for social and political cause.

  Ethical hackers – determine what attackers can gain access to, what they will do with the info, and can they be detected?

Anatomy of an attack..

- **Reconnaissance** – attacker gathers information; can include social engineering and other background check.
- **Scanning** – searches for open ports (port scan) probes target for vulnerabilities.
- **Gaining access** – attacker exploits vulnerabilities to get inside system.
- **Maintaining access** – creates backdoor through use of Trojans; once attacker gains access makes sure he/she can get back in.
- **Covering tracks** – deletes files, hides files, and erases log files. So that attacker cannot be detected or penalized.

Any question(S)?