Th3 M1nD 0f 4 H4xxx0r

A guide to the world of Hacking from the //source.
What is a Hacker?

- **Hacker (computer security)** or *cracker*, who accesses a computer system by circumventing its security system.
- **Hacker (hobbyist)**, who makes innovative customizations or combinations of retail electronic and computer equipment.
- **Hacker (programmer subculture)**, who shares an anti-authoritarian approach to software development now associated with the free software movement.
- A hacker is by mainstream (MEDIA) definition someone who penetrates a computer system in order to use it for some malicious intent.
What is the real definition of a Hacker?

- An individual or group of individuals who are generally reclusive in nature, who may or may not have moral intentions and who enjoy the thrill of finding bread crumbs which lead to a loaf of bread.

- Bread – Jackpot. The intended computer a person who wants to penetrate.

- Can be defined in three categories:
  - White Hat
  - Grey Hat
  - Black Hat
White Hat Hackers

- White Hat - an ethical hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems. Ethical hacking is a term coined by IBM meant to imply a broader category than just penetration testing. White-hat hackers are also called "sneakers", red teams, or tiger teams. Access to a system is authorized, the hacking is ethical and legal.
Who are White Hat Hackers?

- Security professionals who are employed to uphold strict, defined measures to prevent data breaches and network penetration.
- Can be anyone
Grey Hat Hackers

- A grey hat, in the hacking community, refers to a skilled hacker whose activities fall somewhere between white and black hat hackers on a variety of spectra.
- It may relate to whether they sometimes arguably act illegally, though in good will, or to show how they disclose vulnerabilities.
- They usually do not hack for personal gain or have malicious intentions, but may be prepared to technically commit crimes during the course of their technological exploits in order to achieve better security. Whereas white hat hackers will tend to advise companies of security exploits quietly, grey hat hackers are prone to "advise the hacker community as well as the vendors and then watch the fallout"
Who are Grey Hat Hackers?

Leon Kaiser, Sam Hocevar, Andrew Alan Escher Auernheimer and Daniel Spitler are members of GoatSec

Adrian Lamo – The Homeless Hacker

Kevin David Mitnick

Sam Hocevar, Weev - Andrew Alan Escher Auernheimer

Leon Kaiser, Sam Hocevar, Andrew Alan Escher Auernhemier and Daniel Spitler are members of GoatSec
What is a Black Hat Hacker?

A Black Hat Hacker is a hacker who violates computer security for little reason beyond maliciousness or for personal gain. Black Hat Hackers are the epitome of all that the public fears in a computer criminal. Black Hat Hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. The way Black Hat Hackers choose the networks that they are going to break into is by a process that can be broken down into two parts. This is called the pre-hacking stage.

- **Part 1 Targeting**
  - Targeting is when the hacker determines what network to break into. The target may be of particular interest to the hacker, or the hacker may "Port Scan" a network to determine if it is vulnerable to attacks. A port is defined as an opening through which the computer receives data via the network. Open ports will allow a hacker to access the system.

- **Part 2 Research and Information Gathering**
  - It is in this stage that the hacker will visit or contact the target in some way in hopes of finding out vital information that will help them access the system. The main way that hackers get desired results from this stage is from Social Engineering, which will be explained below. Aside from Social Engineering hackers can also use a technique called Dumpster Diving. Dumpster Diving is when a hacker will literally dive into a dumpster in hopes to find documents that users have thrown away, which may contain information a hacker can use directly or indirectly, to help them gain access to a network.
Who are Black Hat Hackers?

- **Kevin Poulsen**: Also known as Dark Dante, Poulsen gained recognition for his hack of LA radio's KIIS-FM phone lines, which earned him a brand new Porsche, among other items.

- **Robert Tappan Morris**: Morris, son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act.

- **Jonathan James**: He installed a backdoor into a Defense Threat Reduction Agency server. The DTRA is an agency of the Department of Defense charged with reducing the threat to the U.S. and its allies from nuclear, biological, chemical, conventional and special weapons. The backdoor he created enabled him to view sensitive emails and capture employee usernames and passwords. James also cracked into NASA computers, stealing software worth approximately $1.7 million. According to the Department of Justice, The software supported the International Space Station's physical environment, including control of the temperature and humidity within the living space. NASA was forced to shut down its computer systems, ultimately racking up a $41,000 cost.
Hacktivism

- The nonviolent use of legal and/or illegal digital tools in pursuit of political ends
- The use of computers and computer networks as a means of protest to promote political ends
- First coined in 1998 by a member of the Cult of the Dead Cow hacker collective named Omega. “If hacking as "illegally breaking into computers" is assumed, then hacktivism could be defined as "the nonviolent use of legal and/or illegal digital tools in pursuit of political ends ".

Hacktivist Groups

- Anonymous
- Antisec Movement
- Legion of Doom
- Lulz Security
- Masters of Deception
- milw0rm
- Operation AntiSec
- P.H.I.R.M.
- Securax
- TESO
- w00w00
- Cult of the Dead Cow
Where do I fit into all of this?

- At 14, I was running Botnets out of China
- Member of IRC group called (BA) – Bar Arcade using Botnets to transfer files and DDoS rival groups
- At 20 I began reporting what I found and how I got into networks to help companies seal up security holes
- Participated in Tiger Trap 2011 and helped develop one of the two exploits which helped capture the flag (more on this later)
Tools of the trade

- Linux Laptop – Backtrack Linux, SamuraiOS
- Wireless Cracking – Gerix, wifi card with hacked firmware, wifi card that supports promiscuous mode (record and intercept packets)
- ZenMap – nMAP with a GUI
- MetaSpl0it Framework
- Cerberus RAT
- Botnet(s)
Backtrack Linux

- Based on Ubuntu Linux
- Includes most tools used by today’s PENTesters
- Wireless cracking tools
- Virus planting and detection tools
- Phishing Tools
- Vulnerability scanners
- Botnet controllers – scripted and IRC based
- DDoS controllers
Botnets and DDoS

- Flooding/DoS/DDoS - Using programs or multiple computers to send trillions of bytes to one location in an attempt to overload it.
Phishing

- "Hooks" victims like a fish to give the hacker their personal information. The victim gets tricked into thinking it's the legitimate website, but it's actually the hacker's website. When they attempt to log in, the website sends those credentials to the hacker.
- Real: http://login.wellsfargo.com/
- Fake: http://wellsfargologin.qibgh3.com/
- ALWAYS check the subdomain and domain before visiting a suspicious link.
Malware/RansomWare/Trojan Horses

- **Malware** – Software designed to clog up and destroy personal information and damage an operating system’s functionality
- **RansomWare** – Same as Malware but used to hold a computer and its user in a state of dysfunction until a ransom is paid – fakealert.Troj
- **Trojan Horse** – A file which is presumed as innocent (usually an .exe file) which gives an attacker access through a hole to control the computer
Usage of Malware in Industrial Systems

- SCADA - *supervisory control and data acquisition* – used for Industrial Control Systems – Used in most manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes. Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, wind farms, civil defense siren systems, and large communication systems.

- STUXNet – Malware specifically designed to attack industrial systems and display a fully functional normal screen of a working industrial system while in reality overloading and causing the system to shut down – transmitted via USB key and is permanent until system is completely reinstalled.

- Thought to have been designed and written by Israel and the US to stop the nuclear ambitions of Iran.

- First virus / weapon to work in Industrial Cyber Warfare.
In case your lost....
Currently India and Pakistan are in the middle of a massive cyber war

Anonymous has taken down web sites of almost every major governmental entity in the world

There are currently over 12,000,000,000 bots in the world being used for phishing, virus transmission, spamming and DDoS

63% are part of the ZEUS Botnet which is so large, owners have began leasing portions of it out
How Can You Help?!

- Protect your home and office networks by running periodical security scans and penetration tests
- Monitor strange activity on your firewalls
- Update all software especially Adobe Acrobat Reader and Microsoft products
- I personally suggest Trend Micro PC-Cillin for my antivirus if I’m using Windows
- Jerry likes Norton (blech)
- Be PRO-ACTIVE in groups such as ISACA, US-CERT, or even attend a Tiger Trap event
What is Tiger Trap?

- Red / Blue team hacking competition
- Digital Capture the flag
- Red = Attackers
- Blue = Defenders
- Network reconnaissance
- Multi WAN Network hosted by Louisiana Colleges – LATech, UNO, LSU, South Eastern, ULM (Monroe)
- Enterprise network architecture with a full SCADA system