Introduction to Ethical Hacking

Peter Muia - KENET


REDIT BANK
519 9860 1535 9007
YOUR NAME HERE

What is Ethical Hacking?

- **Ethical hacking** – defined "*methodology adopted by ethical hackers to discover the vulnerabilities existing in information systems' operating environments.*"
- With the growth of the Internet, computer security has become a major concern for businesses and governments.
- In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems.

Working principle of ethical hacker :

“TO CATCH A THIEF , THINK LIKE A THIEF……”

Ethical Hacking

- Independent computer security Professionals breaking into the computer systems.
- Neither damage the target systems nor steal information.
- Evaluate target systems security and report back to owners about the vulnerabilities found.

HACKING VS CRACKING

HACKING WITH MALICIOUS INTENTION IS CRACKING

- The basic difference is hackers do not do anything disastrous.
- Cracking yield more devastating results.
- Cracking is crime.
- Cyber crime are the results of cracking ,not hacking

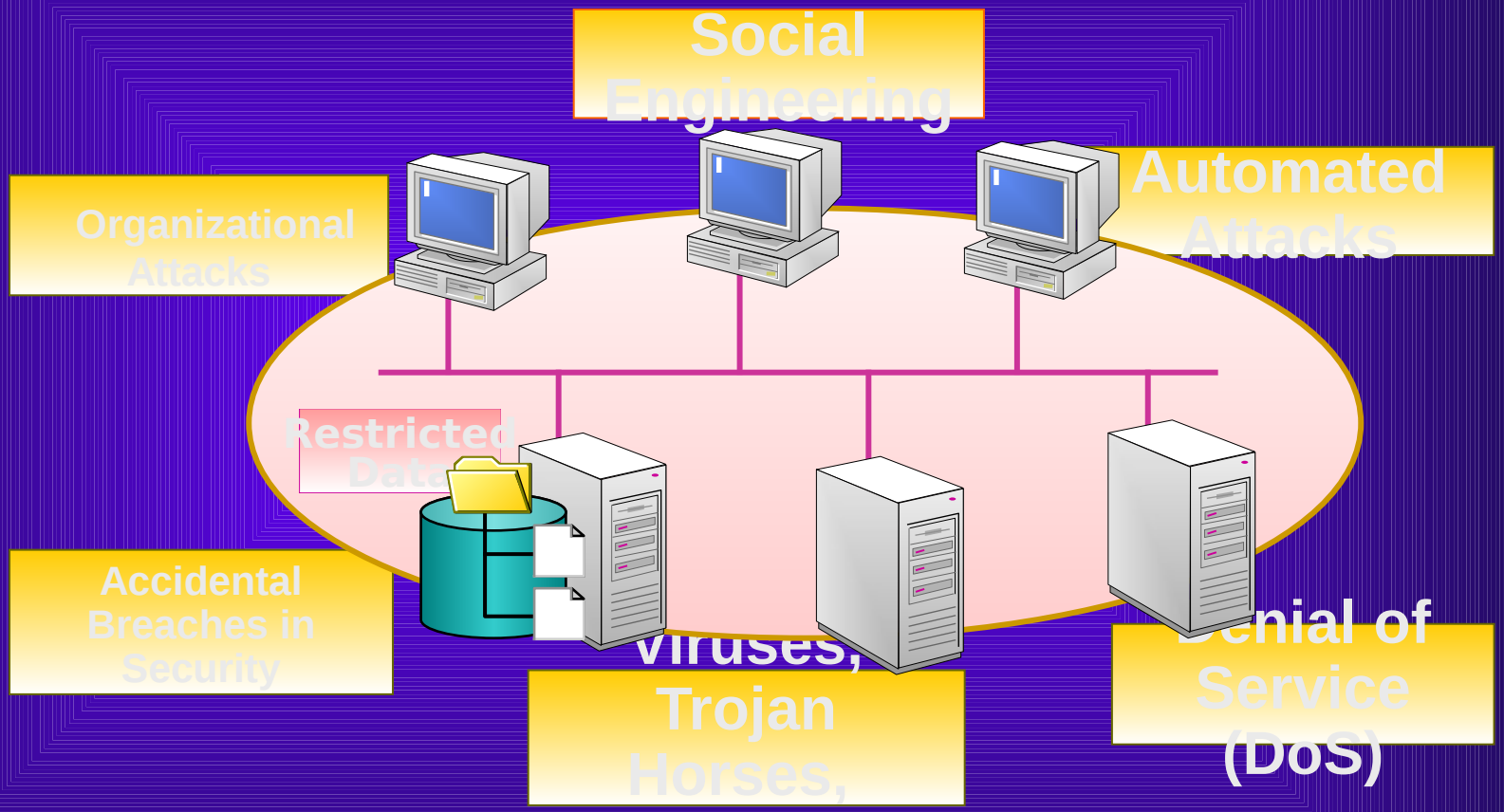
Who are Ethical Hackers?

- "*One of the best ways to evaluate the intruder threat is to have an independent computer security professionals attempt to break computer systems*"
- Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy.
- Ethical hackers typically have very strong programming and computer networking skills.
- They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., Linux or Windows 2000) used on target systems.
- These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors.

Required Skills of an Ethical Hacker

- **Routers:** knowledge of routers, routing protocols, and access control lists
- **Microsoft:** skills in operation, configuration and management.
- **Linux:** knowledge of Linux/Unix; security setting, configuration, and services.
- **Firewalls:** configurations, and operation of intrusion detection systems.
- **Servers**
- **Network Protocols:** TCP/IP; how they function and can be manipulated.
- **Project Management:** knowledge of leading, planning, organizing, and controlling a penetration testing team.

Why Do We Need Ethical Hacking



What do Ethical Hackers do?

An ethical hacker's evaluation of a system's security seeks answers to these basic questions:

- 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 attempts 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?

Modes of Ethical Hacking

- Insider attack
- Outsider attack
- Stolen equipment attack
- Physical entry
- Bypassed authentication attack (wireless access points)
- Social engineering attack

Hacker classes

- **White Hat Hackers: -** specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.
- **Black Hat Hackers: -** The villain or *bad guy*, especially in a western movie in which such a character would stereotypically wear a black hat in contrast to the hero's white hat.
- **Gray Hat Hackers: - A** skilled hacker whose activities fall somewhere between white and black hat hackers on a variety of spectra
- **Hactivism** – hacking for social and political cause.
- **Ethical hackers** – determine what attackers can gain access to, what they will do with the information, and can they be detected.

Why do people hack??

- To make security stronger (Ethical Hacking)
- Just for fun, Show off
- Hack other systems secretly & Steal important information, Financial Gain
- A large fraction of hacker attacks have been pranks
- Venting anger at a company or organization
- Terrorism

Modes of Hacker Attack

- Over the Internet
- Over LAN
- Locally
- Offline
- Theft
- Deception

Ethical Hacking - Process

1) Preparation
2) Foot Printing
3) Enumeration & Fingerprinting
4) Identification of Vulnerabilities
5) Attack – Exploit the Vulnerabilities
6) Gaining Access
7) Escalating Privilege
8) Covering Tracks
9) Creating Back Doors

1.Preparation

- Identification of Targets – company websites, mail servers, extranets, etc.
- Signing of Contract
  - Agreement on protection against any legal issues
  - Contracts to clearly specifies the limits and dangers of the test
- Specifics on Denial of Service Tests, Social Engineering, etc.
- Time window for Attacks
- Total time for the testing
- Prior Knowledge of the systems
- Key people who are made aware of the testing

2.Footprinting

Collecting as much information about the target

- DNS Servers
- IP Ranges
- Administrative Contacts
- Problems revealed by administrators

Information Sources

- Search engines
- Forums
- Databases – whois, ripe, arin, apnic
- Tools – PING, whois, Traceroute, DIG, nslookup, sam spade

Finding remote computer

- Lets say a Hacker decides to break into the computer of one of his facebook friends.
- Then his first step will be to find the IP address of his friend computer.
- So lets discuss what are the possible ways of finding the IP address of any remote computer.

Finding Remote Computer's IP Address

- Through Instant messaging software
- Through IRC Chat

MSN , Yahoo , g-talk

- If you are chatting on other messengers like MSN, YAHOO etc. then the following indirect connection exists between your system and your friend's system:

Your System------Chat Server----→ Friend's System

Friend's System---------Chat Server-------→ Your System

- Thus in this case, you first have to establish a direct connection with your friend's computer by either sending him a file or by using the call feature.

Then, goto MSDOS or the command line and type:

netstat -n

This command will give you the IP Address of your friend's computer.

Instant Messenger

Ask your friend to come online and chat with you.

Case I: If you are chatting on ICQ, then the following connection exists between your system and your friend's system:

Your System------DIRECT CONNECTION----→ Friend's System

Friend's System---------DIRECT CONNECTION-------→ Your System

Now, goto command line and type:

netstat -n

This command will give you the IP Address of your friend's

Getting IP from Website

- One can easily log the IP Addresses of all visitors to their website by using simply JAVA applets or JavaScript code.
- By using PHP scripts it is possible to determine user’s O.S and Browser’s.
- Same can be used to determine the exact geographical location of the visitors.

3.Enumeration & Fingerprinting

- Specific targets determined
- Identification of Services / open ports
- Operating System Enumeration

Methods

- Banner grabbing
- Responses to various protocol (ICMP &TCP) commands
- Port / Service Scans – TCP Connect, TCP SYN, TCP FIN, etc.

Tools

Nmap, FScan, Hping, Firewalk, netcat, tcpdump, ssh, telnet, SNMP Scanner

4. Identification of Vulnerabilities

- Insecure Configuration
- Weak passwords
- Unpatched vulnerabilities in services, Operating systems, applications
- Possible Vulnerabilities in Services, Operating Systems
- Insecure programming
- Weak Access Control

4.Identification of Vulnerabilities

Methods

- Unpatched / Possible Vulnerabilities – Tools, Vulnerability information Websites
- Weak Passwords – Default Passwords, Brute force, Social Engineering, Listening to Traffic
- Insecure Programming – SQL Injection, Listening to Traffic
- Weak Access Control – Using the Application Logic, SQL Injection

4.Identification of Vulnerabilities

Tools

Vulnerability Scanners - Nessus, ISS, SARA, SAINT

Listening to Traffic – Ethercap, tcpdump

Password Crackers – John the ripper, LC4, Pwdump

Intercepting Web Traffic – Achilles, Whisker, Legion

Websites

Common Vulnerabilities & Exposures – http://cve.mitre.org

Bugtraq – www.securityfocus.com

5.Attack – Exploit the Vulnerabilities

- Obtain as much information (trophies) from the Target Asset
- Gaining Normal Access
- Escalation of privileges
- Obtaining access to other connected systems

Last Ditch Effort – Denial of Service

5.Attack – Exploit the Vulnerabilities

Network Infrastructure Attacks

- Connecting to the network through modem
- Weaknesses in TCP / IP, NetBIOS
- Flooding the network to cause DOS

Operating System Attacks

- Attacking Authentication Systems
- Exploiting Protocol Implementations
- Exploiting Insecure configuration
- Breaking File-System Security

5.Attack – Exploit the Vulnerabilities

Application Specific Attacks

- Exploiting implementations of HTTP, SMTP protocols
- Gaining access to application Databases
- SQL Injection
- Spamming

5.Attack – Exploit the Vulnerabilities

Exploits

- Free exploits from Hacker Websites
- Customised free exploits
- Internally Developed

Tools – Nessus, Metasploit Framework

6. Gaining access:

- Enough data has been gathered at this point to make an informed attempt to access the target

Techniques

- Password eavesdropping
- File share brute forcing
- Password file grab
- Buffer overflows

7. Escalating Privileges

If only user-level access was obtained in the last step, the attacker will now seek to gain complete control of the system

Techniques

- Password cracking
- Known exploits

8. Covering Tracks

- Once total ownership of the target is secured, hiding this fact from system administrators becomes paramount, lest they quickly end the romp.

Techniques

- Clear logs

9. Creating Back Doors

- Trap doors will be laid in various parts of the system to ensure that privileged access is easily regained at the whim of the intruder

Techniques

- Create rogue user accounts
- Schedule batch jobs
- Infect startup files
- Plant remote control services
- Install monitoring mechanisms
- Replace apps with trojans

Final Report

- Collection of all discoveries made during evaluation.
- Specific advice on how to close the vulnerabilities.
- Testers techniques never revealed.
- Delivered directly to an officer of the client organization in hard-copy form.
- Steps to be followed by clients in future.

Ethical Hacking - Commandments

- Working Ethically
- Trustworthiness
- Respecting Privacy
- Not Crashing the Systems


Thank You!

Suggestions?