Seminar
On
Ethical Hacking

Submitted To:
www.studymafia.org

Submitted By:
www.studymafia.org

Content

- Introduction
- Ethical Hacking
- Hackers
- Types of Hackers
- Hacking Process
- Why do We need Ethical Hacking
- Required Skills of an Ethical Hacker

Content…

- What do hackers do after Hacking?
- Advantages
- Disadvantages
- Future Enhancements
- Conclusion

Introduction

- Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal.
- Ethical hacking, is legally breaking into computers and devices to test an organization's defenses.

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.

Hackers

- A person who enjoys learning details of a programming language or system
- A person who enjoys actually doing the programming rather than just theorizing about it
- A person capable of appreciating someone else's hacking
- A person who picks up programming quickly
- A person who is an expert at a particular programming language or system

Types of Hackers

- Black Hat Hacker
- White Hat Hacker
- Grey Hat Hacker

Black-Hat Hacker

- A black hat hackers or crackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities.

- That is black hat hackers use their knowledge and skill for their own personal gains probably by hurting others.

White-Hat Hacker

- White hat hackers are those individuals professing hacker skills and using them for defensive purposes.
- This means that the white hat hackers use their knowledge and skill for the good of others and for the common good.

Grey-Hat Hackers

- These are individuals who work both offensively and defensively at various times.
- We cannot predict their behavior.
- Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

Hacking Process

- Foot Printing
- Scanning
- Gaining Access
- Maintaining Access

Foot Printing

- Whois lookup
- NS lookup
- IP lookup

Scanning

- Port Scanning
- Network Scanning
- Finger Printing
- Fire Walking

Gaining Access

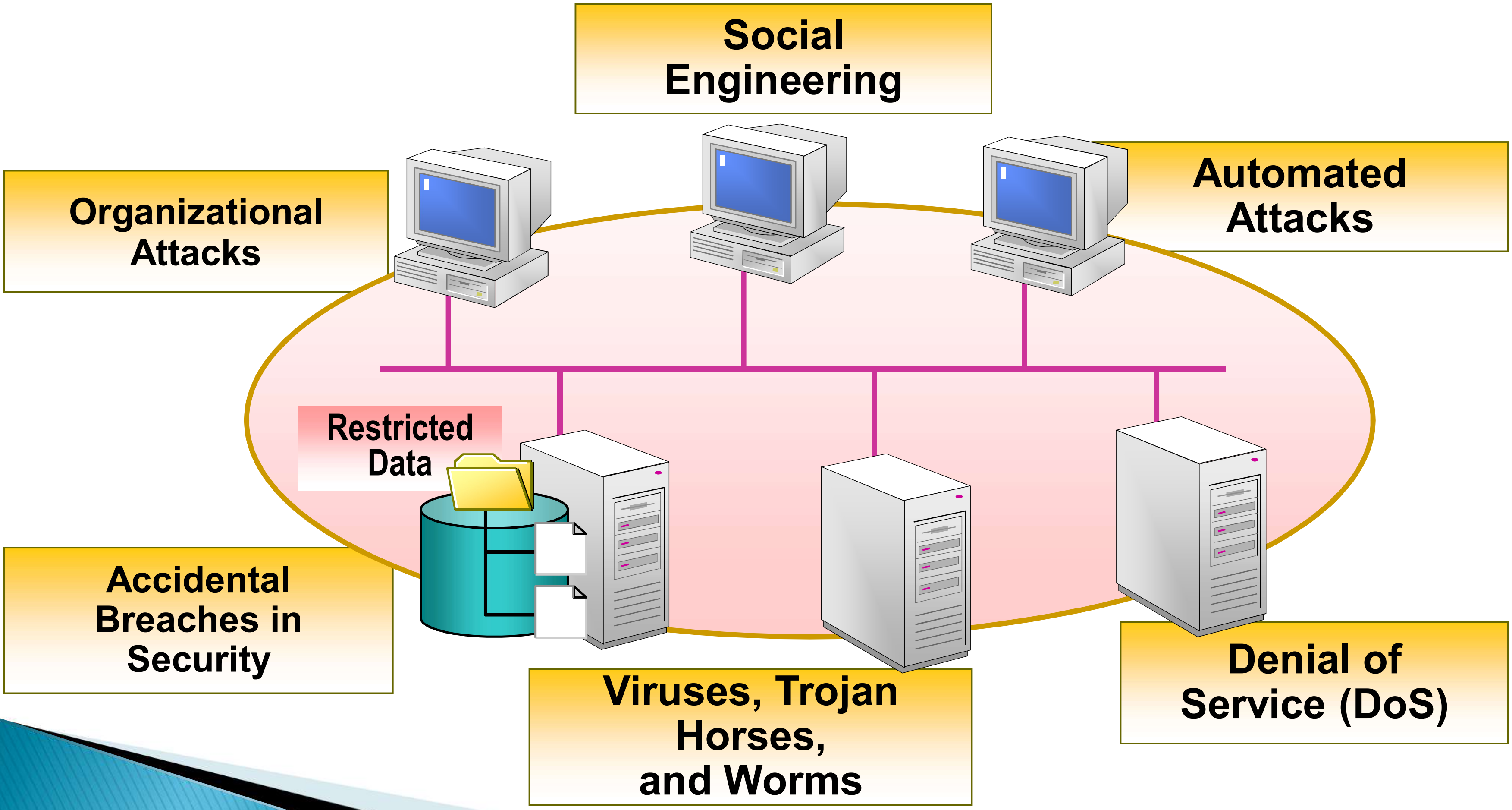
- Password Attacks
- Social Engineering
- Viruses

Maintaining Access

- Os BackDoors
- Trojans
- Clears Tracks

Why Do We Need Ethical Hacking

Protection from possible External Attacks



Required Skills of an Ethical Hacker

- 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.

Required Skills of an Ethical Hacker….

- Routers: knowledge of routers, routing protocols, and access control lists

- Mainframes

- Network Protocols: TCP/IP; how they function and can be manipulated.

- Project Management: leading, planning, organizing, and controlling a penetration testing team.

What do hackers do after hacking?...

- Patch Security hole
  - The other hackers can’t intrude
- Clear logs and hide themselves
- Install rootkit (backdoor)
  - The hacker who hacked the system can use the system later
  - It contains trojan virus, and so on
- Install irc related program
  - identd, irc, bitchx, eggdrop, bnc

What do hackers do after hacking?

- Install scanner program
  - mscan, sscan, nmap
- Install exploit program
- Install denial of service program
- Use all of installed programs silently

Advantages

- ‘’To catch a thief you have to think like a thief”
- Helps in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique

Disadvantages

- All depends upon the trustworthiness of the ethical hacker

- Hiring professionals is expensive.

Future Enhancements

- As it an evolving branch the scope of enhancement in technology is immense.
- No ethical hacker can ensure the system security by using the same technique repeatedly.
- More enhanced software’s should be used for optimum protection.

Conclusion

- In the preceding sections we saw the methodology of hacking, why should we aware of hacking and some tools which a hacker may use.
- Now we can see what can we do against hacking or to protect ourselves from hacking.
- The first thing we should do is to keep ourselves updated about those software's we and using for official and reliable sources.
- Educate the employees and the users against black hat hacking.

References

- www.google.com
- www.wikipedia.com
- www.studymafia.org

Thanks