How Ethical Hackers Play an Important Role for any Organization.?

[1] Vikas Kumar, [2] Rahul Kumar Chawda

[1] BCA Student, [2]Assistant professor
[1] Computer Science Department,
[1] Kalinga University, Atal Nagar, Chhattisgarh, India

Abstract: *"*It is truth universally acknowledge, that an Organization in possession of a good fortune, must be in want of an Ethical hacker,".
In Today's networked world every Organization needs to make sure that it is properly protected against all intrusion, now a day No One is safe over Internet, the network may be protected with firewall and Proxies. The internal hosts may have antivirus and IPS. The server behind the latest IPS/IDS or Firewall, but there is no certainty that a breach will not happen. Unless the whole security systems are tested by an attack itself, but before a full blown down attack is launched by a hacker, smart Organizations make sure that an ethical hacker puts their defense through a battery of tests so that an ethical hacker puts their defense through a battery of tests so that a real attack can never take place.

Index Terms – Ethical Hacking, Hacker, Needs, Types, Scope

I. INTRODUCTION

Hacking means many things but in the context of computer networks and systems, it is the act of breaking in, either with the intention of stealing or just bragging rights, Malicious hacking or breaks- ins into systems and network cost organizations billions of dollars every year.
Organization that are attacked by hackers pay a huge monetary price, in term of loss of productivity, loss of data, loss of Reputation. A small Business may even be wiped out if its confidential data is stolen. Customer are unwilling to trust online shopping sites or banks if they report even a minor breach of security.
The effect of hacking is multifold and sometimes the repercussions are felt for years, with the victim organization still trying to build up its lost reputation,

II. Who is Hacker?

A hacker is like a common man but his Thinking is out of common man Thinking, they are expert in programming, networking, Operating Systems and applications, They may even their own hacking tools.

a. **Ethical Hackin**g: An ethical hacker attempts to hack his way pass the systems security, finding any weak points in the security that can be exploited by other hackers.

III. What hacker can do?

There are a numbers of reason why hackers try to break in, but primary among them is money.

a. Steal Confidential data
b. Steal Personal information
c. Steal bank account number
d. Steal passwords
e. Destroy data
f. Encrypt personal data

III. Types of Hacker:

a. Black Hat hacker:

A black hat hacker breaks into computer networks or systems with a purely malicious intention, either to steal sensitive information or destroy data or disable services.

b. White Hat Hacker :

White hat hacker tries to attack an Organization's defense and get in – but his intention is not to steal or destroy. He hacks into systems to see how vulnerable they are. And provides valuable feedback to the security and systems administrator. About the loopholes in the security and how best they can be plugged.

c. Gray Hat hacker:

Gray hat hacker does not mind who he is working for,as long as the money is coming, He is available for hire, he can be an Ethical Hacker and Help an organization protect itself.

IV. Who are at the risk of Hacking Attacks.

Internet Security firms –their servers and web sites contain the best security, therefore making them a very challenging target for hacker.

High-profile media-friendly targets –include large corporations' sites, political party sites, celebrity sites etc.

Anyone with a website although e-commerce sites are far more attractive to hackers than community pages.

Always-on board band connection.

Practically everyone with internet access is vulnerable to attacks.

V. Network Security Challenges:

As today's networks are becoming more and more complex with a variety of device connected and services being offered, it is becoming very difficult to manage all the network resources and keeping track of vulnerabilities and applying patches in order to secure the network.

VI. Understand the need to Hack your own Systems:

"To catch a Hacker, think like a Hacker."

Its help to shore up an organization's defenses by attacking them himself, the results of the attack will them reveal what is safe and what need to be patched or reconfigured to improve security. Ethical hacking is basically an audit of the security systems of an organization.

That's the basis for ethical hacking. The law of averages works against security with the increased number and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way.

VII. Scope and limits of Ethical Hacking:

1. An Ethical Hacker should have a signed contract with the client organization, clearly defining the scope of the ethical hacking attack, this document outlines which parts of the systems should be targeted and which part should be untouched by the hacker.
2. The ethical hacker can perform attacks both form the external and internal networks.
3. The ethical hacker will perform a series of penetration test and vulnerability audit in the course of the attack.
4. Any vulnerabilities discovered should be revealed only to the client and no one else.
5. After the completion of the attack, a detailed report should be submitted to the client, identifying all the loopholes and vulnerabilities. The report should also contain recommendations for fixing these loopholes.

a. Penetration testing:

Penetration testing or pen test in short is an authorized attack on the security infrastructure and the host and server on a network, A penetration test attacks Operating systems, applications, routers,firewall and other network elements to uncover potential vulnerabilities. A

b. Vulnerability audit:

A vulnerability audit is a careful evaluation of all the IT resources in an Organization to uncover any Potential weakness and put mitigation procedures in place.

A Vulnerability audit includes the following

- Taking stock of all the IT resources
- Assign a metric of importance to each resource.
- Uncover security vulnerabilities and threats to that resources
- Patch up the most serious vulnerabilities.

VIII. Why Ethical Hacking is necessary:

a) Ethical Hacking can be considered as an audit of the organization's network security.
b) The findings of an ethical hacker help the organization in identifying potential weakness in the networks and help them patch those weaknesses.
c) Proper implementation of security patches in a network minimizes the chances of a hacking attack.

IX. Security, Functionality and Usability Triangle

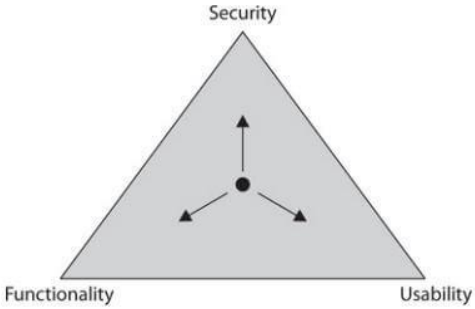

Fig 1.1 –Represent Security,Functionality,and Usability.
(Image Credit: Google)

- Network security define how strong in the security implementation.
- Functionality defines the feature availability.
- Ease of use defines how simple is it to configure and maintain the network.
- Moving towards any one corner of the triangle compromise the other two feature.