COMPUTER SECURITY IN THE TODAY'S ERA

Dr.Nikunj Raval
(E-mail:nikunjraval2@gmail.com)

Abstract **:** After thirty years of work on computer security, why are almost all the systems in service today extremely vulnerable to attack? The main reason is that security is expensive to set up and a nuisance to run, so people judge from experience how little of it they can get away with. Since there's been little damage, people decide that they don't need much security. In addition, setting it up is so complicated that it's hardly ever done right. While we await a catastrophe, simpler setup is the most important step toward better security. In a distributed system with no central management like the Internet, security requires a clear story about who is trusted for each step in establishing it, and why. The basic tool for telling this story is the "speaks for" relation between principals that describes how authority is delegated, that is, who trusts whom. The idea is simple, and it explains what's going on in any system I know. The many different ways of encoding this relation often make it hard to see the underlying order.

Introduction

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.
In this digital era, we all want to keep our computers and our personal information secure and hence computer security is important to keep our personal information protected. It is also important to maintain our computer security and its overall health by preventing viruses and malware which would impact on the system performance.

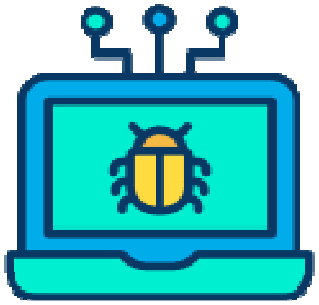
The components of a computer system that needs to be protected are:

Hardware, the physical part of the computer, like the system memory and disk drive
Firmware, permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user
Software, the programming that offers services, like operating system, word processor, internet browser to the user

Computer security threats

Computer security threats are possible dangers that can possibly hamper the normal functioning of your computer. In the present age, cyber threats are constantly increasing as the world is going digital. The most harmful types of computer security are:

Viruses



A computer virus is a malicious program which is loaded into the user's computer without user's knowledge. It replicates itself and infects the files and programs on the user's PC. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all.

Computer Worm

A computer worm is a software program that can copy itself from one computer to another, without human interaction. The potential risk here is that it will use up your computer hard disk space because a worm can replicate in great volume and with great speed.

Phishing

Disguising as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing in unfortunately very easy to execute. You are deluded into thinking it's the legitimate mail and you may enter your personal information.

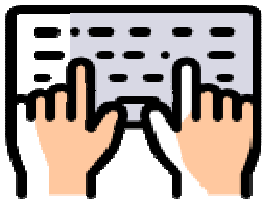
Botnet

A botnet is a group of computers connected to the internet, that have been compromised by a hacker using a computer virus. An individual computer is called 'zombie computer'. The result of this threat is the victim's computer, which is the bot will be used for malicious activities and for a larger scale attack like DDoS.

Rootkit

A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit will be able to remotely execute files and change system configurations on the host machine.

Key logger



Also known as a keystroke logger, keyloggers can track the real-time activity of a user on his computer. It keeps a record of all the keystrokes made by user keyboard. Keylogger is also a very powerful threat to steal people's login credential such as username and password.

These are perhaps the most common security threats that you'll come across. Apart from these, there are others like **spyware, wabbits, scareware, bluesnarfing** and many more. Fortunately, there are ways to protect yourself against these attacks.

Why is Computer Security Important?

In this digital era, we all want to keep our computers and our personal information secure and hence computer security is important to keep our personal information protected. It is also important to maintain our computer security and its overall health by preventing viruses and malware which would impact on the system performance.

Computer Security Practices

Computer security threats are becoming relentlessly inventive these days. There is much need for one to arm oneself with information and resources to safeguard against these complex and growing computer security threats and stay safe online. Some preventive steps you can take include:

Secure your computer physically by:

- Installing reliable, reputable security and anti-virus software.
- Activating your firewall, because a firewall acts as a security guard between the internet and your local area network.

- Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available.
- Avoid clicking on email attachments unless you know the source.
- Change passwords regularly, using a unique combination of numbers, letters and case types.
- Use the internet with caution and ignore pop-ups, drive-by downloads while surfing.
- Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats.
- Perform daily full system scans and create a periodic system backup schedule to ensure your data is retrievable should something happen to your computer.

What is a Firewall?

A cyber security firewall is a network security system which can either be a hardware or software that protects the trusted network from unauthorized access from external networks and external threats.

It uses the mechanism of filtering of data by using a defined set of policies rules, that help restrict access to the applications and system.s

It acts like a gatekeeper and monitors and control incoming and outgoing network traffic.

Any specific traffic, in the form of requests for access, requests for data, to a resource behind the firewall and inside the trusted network, will be inspected, analyzed and is allowed to pass.

Various Implementations of Firewalls

- They are hardware firewalls, ranging from entry levels, mid-range to high end depending on a load of simultaneous hits on the entity we are protecting
- The expected user base
- There are software-based firewalls
- Some implementations work with a combination of software and a hardware firewall
- Large organizations install high end dedicated hardware firewalls
- Small app vendors and Individuals can setup basic software firewalls on their personal devices

Expectations of a Firewall Implementation

Implementing a firewall does the following things:

- Ensure that all traffic from the external world onto the system or application is mandatorily routed through the firewall
- The rules defined ensure isolation and detection of all possibilities of unauthorized incoming traffic
- Denial of unauthorized traffic
- Passing of all authorized traffic
- Learning and improvisation of rules
- Identification of a right fit firewall for the expected load is imperative to ensure performance is not impacted

Advantages and Disadvantages of Firewall

- *Advantage* is an outcome of the effectiveness of the implementation of rules and controls on the firewall. The firewall is effective when it can handle all possible external threats.
- *A disadvantage* is that firewalls cannot prevent internal threats, virus attacks and authentic mechanisms used by hackers (like username password).

Organizations have to implement other mechanisms and controls to circumvent these threats. Threats like, intrusion detection systems and intrusion prevention systems. Attacks from the internet of virus, trojans, spyware, ransomware, denial of service, malware, can be foiled by implementing an antivirus and other prevention and detection systems alongside firewalls.

Types of Firewalls

- Any access that happens to the application inside a trusted network is broken down to multiple packets. To recognize the authenticity of a packet there are packet filtering firewalls. These are very popular and are used to block packets from a specific source or another network. Hence, when the network is attacked by unknown packets, the firewall recognizes it as a threat and raises an alarm and blocks it.
- A firewall can work to mask or hide the internet address of the trusted private trusted network from the external public network hence unwarranted access cannot happen.
- Application-level gateways or **proxy-based firewalls** are becoming the need of the hour.
- Today the dependencies and advent of cloud-based applications have diverted focus to control applications access. Hence one may

want to block complete application services (like FTP, telnet, Http).

- Eg. FTP access allows a user to copy files from one network to another. By blocking FTP service it is unavailable to a malicious user who tries to connect to this network and to copy content.

There are multiple solutions to detect and prevent malicious behavior and attacks. Because there are many ways to avoid attacks a need is felt to find integrated solutions for firewalls, antivirus, anti-spam, and intrusion detection and intrusion prevention. Such solutions will be the next-generation innovation in the field of Cyber Security.

"Cybersecurity Threats are much more than a matter of IT," IBFS Global Chief Information Security Officer & Board Advisor, Société Générale.
Cybersecurity is a domain that has stayed in the shadows for most of its lifetime. Only a handful of leading organizations have dedicated teams that preserve their privacy and secure their systems. But, there was never a large-scale global adoption of cybersecurity as a profession or even as an IT domain.
Until as recently as 2010, security and privacy of data in organizations was the responsibility of each and every professional working there. Unfortunately, this approach has become outdated in today's fast-paced world where hackers are years ahead when compared to tech professionals. Let's understand this better with an infographic:

Cybersecurity Threats: Modern Trends
As evident from the above image, the state of cybersecurity and our digital privacy has been deteriorating in the last couple of years. This begs the question, "*Are our digital identities and data safe?*"
Like most questions in the IT industry, shifting of technology trends solved most of the questions presented by cybersecurity threats. Companies, organizations, and even influencers have recently started building up their own cybersecurity teams. In fact, ethical and consulting hackers can score jobs that offer salaries up to $106,000 per annum, according to Indeed.com.

Cybersecurity threats are real and will keep getting more complex as hackers learn to adapt to security strategies. This makes cybersecurity one of the most dynamic domains with more learning involved than any other IT sector. Fortunately, there are hundreds, if not thousands of openings in the job market for entry-level professionals who are looking to get into a cybersecurity role. Additionally, there are no solid prerequisites to get into this awesome domain. Although, a beginner-level of networking will be a plus. You can also get a competitive edge in the market if you bag up Cybersecurity certifications like CompTIA Security+, CEH, and many more.

Each time we hear a word Hacking the first thing people relate it to is malicious cyber practices. Is that completely true though? In this article we will put forth the debate on Hacking vs Ethical Hacking comparing these two terms to understand them better.

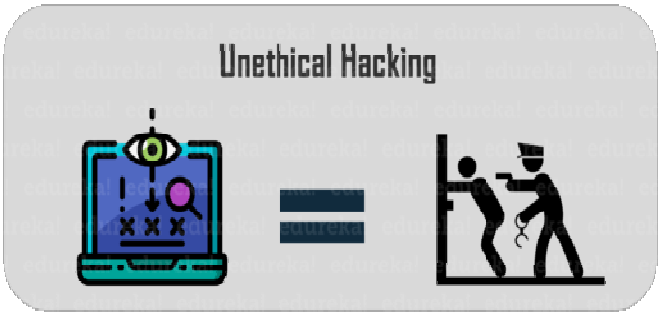
Following pointers will be covered in this article,

- General Perspective Towards Hacking And Ethical Hacking
- White Hat Hackers vs Black Hat Hackers
- Categories Of Hacking
- Hackers vs Crackers

So let us get started General Perspective Towards Hacking And Ethical Hacking
Hacking is referred to as the illegal or legal practices of accessing data stored in any system by experts. These experts are termed as Hackers. Hackers have all the knowledge related to programming and its concepts. The mistakes that are done by programmers while developing or working on a software are picked up by hackers to encroach the security framework of the software.
Ethical hacking is conducted by hackers as well but their intention behind hacking is not for malicious purposes. Their services are used to check and build on software security and thus help to develop the security system of a framework in a business or organization to prevent potential threats. Ethical hackers are referred to as White Hats, who end up provide protection from the Black Hats who are the unethical hackers. Ethical hacking is adopted by many almost every organization.
Moving on with this article on Hacking vs Ethical Hacking,**Hacking vs Ethical Hacking**
White Hat Hackers vs Black Hat Hackers
Black Hat Hackers' objective:

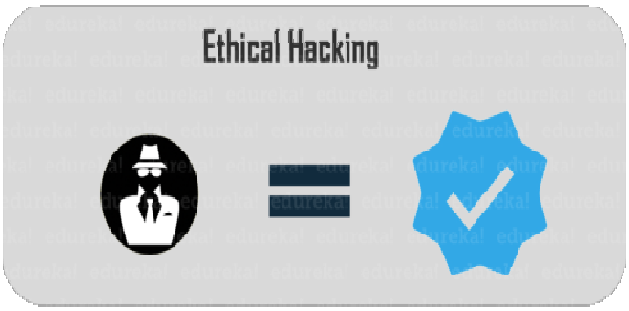
- To steal valuable information from another user
- To steal money through transactions and accounts
- To get access to free music and videos
- Downloading free hacking software which is considered an illegal activity

- To steal valuable information from military/navy organizations etc
- To access restricted networking spaces



White Hat Hackers' objective:

- To improve the security framework in a system
- Developing high security programming language like Linux
- Developing most of the security software for organizations
- Checking and updating security softwares
- Developing programs like pop up blocker, firewall and ad blocker



The types of Black Hat hackers are:

- Phreakers – Hackers who hack the telephone networks
- Crackers – Hackers who remove the security wall of a software by using software patches
- Carders – Hackers who attack ATM or credit cards to retrieve user information
- Script Kiddies – Hackers who want to attack computer systems for no purpose

Categories Of Hacking

- Windows Hacking
- Database Hacking
- Web Hacking
- Network Hacking

Other methods of Hacking

Phishing

In this kind of hacking, hackers use their skills to hack passwords of emails or websites. People usually receive phishing emails in their inbox. The hackers usually derive login information of the users by their emailids by asking them to log in and redirecting it to their website.

BotnetsSometimes, robots do the hacking job through botnets.

Keyloggers

This is a relatively new technique adopted by hackers to breach information. Hackers install a device on a motherboard port and whatever is typed on the keyboard, is stolen.

Hackers vs Crackers

It is commonly assumed and accepted that hackers help to build security whereas crackers aim to break security. There is a major difference between how the two work although they both engage in hacking of some sort. Hackers usually have an advanced level knowledge regarding computer security and possess all the technical knowledge required as well but are not necessarily skilful as hackers. Few of them are skilled enough to develop their own software and tools. Hackers aim to counter attack threats posed by crackers to the computer systems as well as internet security across networks.

On the other hand, crackers are well aware that their activities are illegal and thus are criminal activities hence they try to cover their tracks. Even though crackers may be highly skilled in breaching systems, professional hackers can restore the security of the breached system and catch the cracker with their skills and competency. Crackers possess highly advanced and technical knowledge and can create software and tools that are powerful enough to damage and exploit systems after analyzing the system's weak areas. Most of the times, crackers do not leave their mark behind as they are very efficient and careful in executing their work.

However they pose a serious threat to the internet security. It is well established that hackers are ethical professionals whereas crackers hack into systems illegally and without consent. Apart from this major difference, another difference is with regards to their understanding of computer systems and security systems. Hackers can write codes in many languages and possess in depth knowledge of computer languages like C, C++, HTML and Java. They also understand how these languages work and what these codes do. On the other hand, crackers do not have an upper hand here.

They do not possess much knowledge about computer programming. Their work and the intent behind it makes them poles apart from each other and is main point of difference between the two.

Conclusion

Thus it is safe to say that hackers break into systems entirely to check for gaps in it and rectify them to update the systems whereas crackers break into the systems with the intention of exploiting them and for personal gains. This is not only unethical but is also an illegal and criminal activity. White Hats are employed by organizations to carry out hacking after being subjected to a legal contract. On the other hand, Black Hats do not succumb to any approval or agreement as they intend to violate the security of any system that they desire. While a cracker encroaches on personal data and information and uses is to his own advantage, the hacker commits the same action to help a company or an individual to ward off attacks from these crackers.

Every commercial or application services exposed on the internet will have its own security requirements based on the functionality. A detailed study and feasibility analysis must be done before implementing the most appropriate of security control systems. To beat the world of threats and hackers, the focus has to be on implementation and then continual improvisations to meet all the possible current and future threats. A firewall is one of the many solutions available in today's world cybersecurity to control these external threats.

That's it, folks! This brings us to the end of this "Cybersecurity Firewall" article. If you wish to learn cybersecurity and build a colorful career in cybersecurity, then check out our Cybersecurity Certification Training which comes with instructor-led live training and real-life project experience. This training will help you understand cybersecurity in-depth and help you achieve mastery over the subject.

You can also take a look at our newly launched course on CompTIA Security+ Certification which is a first-of-a-kind official partnership between Edureka& CompTIA Security+. It offers you a chance to earn a global certification that focuses on core cybersecurity skills which are indispensable for security and network administrators.

Bibliography

1] A.V.R. Mayuri (2012), "Phishing Detection based on Visual-Similarity" Conference Proceedings from "International Conference on Network and Cyber Security - 2012" SRK Institute of Technology, Vijayawada, A.P.

2] Alok Bansal, SuyashJhawas, Dharmendra Sharma, Rashmi Tiwari, Rajiv Tripathi (2011), "Internet Users Resistance towards Online Purchases: - An Exploratory Study", Proceedings from Conference on Information and Communication Technologies Enhancing Business Competencies through Innovative Practices (2011), Prestige Institute of Management & Research, Indore.

3] Amit Sharma (2010), "Cyber Wars and National Security - A paradigm shift from Means to Ends" Proceedings from Conference on Cyber Security, "Emerging Cyber Threats & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai.

4] B.G.Gupta (2010), "Security Convergence – Physical & Information" Proceedings from Conference on Cyber Security, "Emerging Cyber Threats & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai & Challenges, (2010)" CII, Confederation of Indian Industry, Chennai

Websites:

https://www.britannica.com/technology/computer-security#
https://www.edureka.co/blog/what-is-computer-security/
https://www.simplilearn.com/what-is-computer-security-article