International Multilingual Research Journal

Printing Area™

ISSN 2394-5303

Two Day State Level Seminar on Ethical Hacking

Jointly Organized By

Department of Computer Science and Application

&

BCUD, Savitribai Phule Pune University

Convener
Dr. J.A. Khan
Principal

Coordinator
Ms. Khan Nazmin Wasim
Asst. Professor

Asst. Coordinator
Mr. Owyes Siddiqui
Asst. Professor

NATIONAL SENIOR COLLEGE
National Campus, Maulana Azad Road, Sarda Cirrcle, Nashik

|| Index ||

International Multilingual Research Journal

Printing Area

9850203295 7588057695

Editor Dr.Bapu G.Gholap

07

SECURITIES OF ETHICAL HACKING

Khan mahfooj Ab.Rahman
YEWS National senior college,Nashik

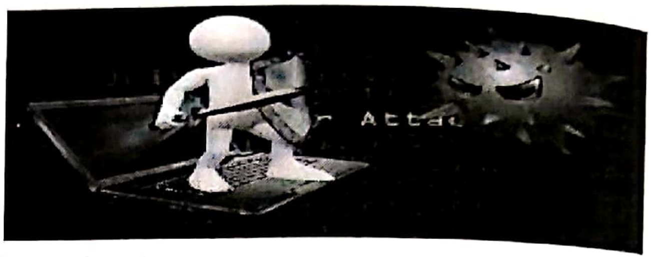
****

ABSTRACT:

Ethical hacking is the method to find out the fault lines and vulnerabilities in the system of computer network. It is an approach to illustrate the process of hacking in an ethical way for any network. The ethical hacker has the good purpose to do it. Actually, it has become a common opinion and outlook in our intellect world for hacker that he/she will be awful, extreme, unlawful and unethical. Basically, some of the hacker has even done very scantily with some organizations like they have stolen very vital information of their clients. In some of the government organizations and institutions, they have damaged high classified information like social security numbers(like face book ID and Twitter Account) and other susceptible information. That is the reason, hackers are not enjoying a very good status in society. To get rid of such conditions severalorganizations have hired various ethical hackers to keep a trackand a 24 hours vigilance on their significant system and computer network. Ethical hackers are supposing to test and check vulnerabilities and weaknesses in the present system.

At the time of thedevelopment of the Internet, computer security has become a major concern for all the businesses and governments' organization who are heavily dependent on the modern information technology. They want to be able to take advantage of the Internet for electronic commerce (E-COMMERCE), publicity and advertising, information sharing and its permitted access, and other pursuits and tracking down, but they are worried about the very possibility of being "hacked" today or tomorrow.

KEYWORDS: Legal hacking, computer securities, hacking securities,hacking insecurities.



Introduction:

Ethical hacking-also known as penetration testing or intrusion testing or red teaming has become a major concern for businesses and governments. Companies are worried about the possibility of being "hacked" and potential customers are worried about maintaining control of personal information.The expression "computer hacking" carries images of unscrupulous techies who use their skills to However, some companies have employed so-called "ethical hackers" to explore their own computer systems and find potential weaknesses. These "white hat" hackers can demonstrate how their "black hat" counterparts can damage vulnerable systems, while offering advice on how to protect their clients from such dangers. Ethical hacking can also ensure that vendor's claims about the security of their products are legitimate. Security Security is the condition being protected against danger or loss. In the general sense, security is a concept similar to safety those persons who is a passive person should not see those data.

Government agencies and business organizations today are in constant need of ethical hackers to combat the growing threat to IT security, says Jay Bavisi, co-founder of the EC Council. "A lot of government agencies, professionals and corporations now understand that if you want to protect a system, you cannot do it by just locking your doors," Bavisi says in an interview with Tom Field of Information Security Media Group [transcript below].

Bavisi, president and co-founder of the International Council of E-Commerce Consultants, created an ethical hacker standard now used by the Pentagon.

Securities:

The purpose of ethical hacking is to evaluate the security of a network or system's infrastructure. It entails finding and attempting to exploit any vulnerability to determine whether unauthorized access or other malicious activities are possible. Vulnerabilities tend to be found in poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures.

Security Computer security is required because most organizations can be damaged by hostile software or intruders. Moreover security is directly related to business. This is because if a company losses a series of credit card numbers of its customers then many customers would be hesitant to go back to the same company and that particular company will lose many customer and hence the business. There may be several forms of damage which are obviously interrelated which are produced by the intruders. These include: loss of confidential data damage or destruction of data damage or destruction of computer system loss of reputation of a company .There may be many more in the list due to security breaches. Ethical hacking is also known as penetration testing, intrusion testing or red teaming. With the growth of the Internet, computer security has become a major concern at the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses. 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. This scheme is called Ethical Hacking. This similar to auditors come into an organization to verify its bookkeeping records. This method of evaluating the security of a system has been in use from the early days of computers.[1]

Network Security:

Network security is more about defending and documenting defense's. You are finding out about firewalls and putting them up. You will find out about VPN server security and actually instantiate VPN servers. It's typically not about modelling an attack the way an attacker would. Those are very different things. Network security typically entails following best practices or common techniques in order to implement and operate in a secure manner. Ethical hacking is finding the weaknesses in those implementations, weaknesses and then feeding them back into a network security process that helps defend against them and repel those types of potential attacks from future occurrences.

One of the first examples of ethical hacking occurred in the 1970s, when the United States government used groups of experts called "red teams" to hack its own computer systems. It has become a sizable sub-industry within the information security market and has expanded to also cover the physical and human elements of an organization's defenses. A successful test doesn't necessarily mean a network or system is 100% secure, but it should be able to withstand automated attacks and unskilled hackers.

Network defence:

What are the benefits of ethical hacking? There are some benefits of ethical hacking are a little different than the benefits of network defence or perimeter defence, because ethical hacking helps any system owner or business owner find the vulnerabilities before an attacker does, in a way so that the attacker would find if they were actually committing an attack. Therefor ethical hacking uses these attacker techniques. That's why it actually uses the real tools, technologies, methodology and approaches that an attacker would.

Modelling:

Modelling an attack at every times finds vulnerabilities that cannot be found in any other way. It helps file both weak security areasand areas where an attacker can catch in, and also tough security areas. Areas where an attacker is thwarted and let down, takes perpetually. Those are the kinds of areas that we don't need to worry about, or maybe need to extend those areas or any security model is the key benefit of ethical hacking. That's in fact why individual hackerdoes this. Further, ethical hacking is in fact more of an attack modus operandi. It uses attacker tools, working behaviors and position of an attacker creating a an immensedissymmetry between ethical hacking and existing network security

Securities of ethical Hacking:

Testing Security Measures The primary advantage of having ethical hackers on a company's payroll is that the hackers are allowed to test a can help companies determine which of their computer security measures are effective, which measures need updating, and which ones pose little to no deterrent to dangerous intruders. The data from these tests allows management to make informed decisions on where and how to improve their information security. Finding Vulnerable Areas When the white-hat hacker's finish exploring the company's system, they turn in a report on the system's vulnerable areas. These areas can be related to the technology, based systems, such as administrators who give out passwords to unauthorized personnel.2[2]

In-securities of Ethical Hacking

As with all types of activities which have a darker side, there will be dishonest people presenting drawbacks. The possible drawbacks of ethical hacking include:[3] The ethical hacker using the knowledge they gain to do malicious hacking activities Allowing the company's financial and banking details to be seen .The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system Massive security breach. These are not common; however, they are something all companies should consider when using the services of an ethical hacker.2

Conclusion:

As we are witnessing that many type of threats are caused and affected now-a-days due to unethical hacking of our data or personal information, which is not secured. Any of the person can hack into our accounts and misuse our data. Thus, why security is very much necessary? Because, security is a paramount requirement of not only individuals but also to society and nation. The destiny of a nation is now locked and kept at the operation of one button on the very Key- Board of our Computer System of this high- tech age.

In this project, I have defined some of the measures, which can help us to secure our data. These measures are necessary because there are bunch of "black hat" hackers, which are always ready to hack into our accounts. And they can cause many type of internal harm to our data. Therefore, why precaution is to be taken and we should learn some measures and methods to safeguard our valuable data.

Reference:

http://seminarprojecttopics.blogspot.in/2012/08/ethical-hacking.html

https://nicholasdmc4.wordpress.com/2012/04/17/ethical-hacking

https://www.scribd.com/presentation/280428658/CSE-Ethical-Hacking

Note.

As a student, it is my small step to accomplish long academic journey. As a beginner, I have taken every precaution of a reference that should not go unnoticed. I am highly thankful and remain grateful to the entire authors, whose research papers, books and articles have been referred. By mistakes, if any authors have been left to be referred, I seek apology from them and hope honorable authors will cast their mercy and excuse me.

(Footnotes)

1.https://www.scribd.com/presentation/280428658/CSE-Ethical-Hacking

2. https://nicholasdmc4.wordpress.com/2012/04/17/ethical-hacking

❑❑❑

08

Cloud Computing

Farukh Shahzad
Computer Science,
YEWS National Senior College, Nashik

****

ABSTRACT

"Cloud" computing – a relatively recent term, defines the paths ahead in computer science world. Being built on decades of research it utilizes all recent achievements in virtualization, distributed computing, utility computing and networking. It implies a service oriented architecture through offering software's and platforms as services, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on demand services and may other things. The skyrocketing demand for a new generation of cloud-based consumer and business application is driving the need for next generation of datacenters that must be massively scalable, efficient, agile, reliable and secure. We believe that the next generation cloud evolution is a fundamental transformation and not just an evolutionary stack collaboration networks utilizing optimally distributed and managed computing, network and storage resources driven in real time by business priorities. This paper is a brief survey based of readings on "cloud" computing and it tries to address, related research topics, advantages, dis advantages, challenges ahead and possible applications. Cloud computing is location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand, as with the electricity grid. Cloud computing is a natural evolution of the widespread adoption

Youth Education & Welfare Society's

NATIONAL SENIOR COLLEGE

National Campus, Sarda Circle, Nashik. (MS)
Affiliated to Savitribai Phule Pune University, Pune.
Department of Computer Science & Application.
State level Seminar on
" Ethical Hacking"
January 15 & 16, 2018
Sponsored By :
BCUD, Savitribai Phule,Pune University

Certificate

This is to certify that Dr./Prof./Mr./Ms. Khan Mahfooj Ab. Rahman has Participated/Presented Paper/delivered lead lecture Entitled Securities of Ethical Hacking

at the Two Day State level Seminar on **"Ethical Hacking"** held on January 15 & 16, 2018, organized by the Department of Computer Science, National Senior College, Sarda Circle, Nashik-1. His/Her active participation /presentation in this seminar is highly appreciated.

(Prof. Nazmin W. Khan)
Co-ordinator

(Dr. Jawad A. Khan)
Principal & Convener

International Multilingual Research Journal

Printing Area™

ISSN 2394-5303

Two Day State Level Seminar on

Ethical Hacking

Jointly Organized By

Department of Computer Science and Application

&

BCUD, Savitribai Phule Pune University

Convener
Dr. J.A. Khan
Principal

Coordinator
Ms. Khan Nazmin Wasim
Asst. Professor

Asst. Coordinator
Mr. Owyes Siddiqui
Asst. Professor

NATIONAL SENIOR COLLEGE

National Campus, Maulana Azad Road, Sarda Cirrcle, Nashik

|| Index ||

International Multilingual Research Journal

Printing Area

9850203295 7588057695

Editor Dr.Bapu G.Gholap

beginner, I have taken every precaution of a reference that should not go unnoticed. I am highly thankful and remain grateful to the entire authors, whose research papers, books and articles have been referred. By mistakes, if any authors have been left to be referred, I seek apology from them and hope honorable authors will cast their mercy and excuse me.

(Footnotes)

1.https://www.scribd.com/presentation/280428658/CSE-Ethical-Hacking

2. https://nicholasdmc4.wordpress.com/2012/04/17/ethical-hacking

❑❑❑

08

Cloud Computing

Farukh Shahzad
Computer Science,
YEWS National Senior College, Nashik

****

ABSTRACT

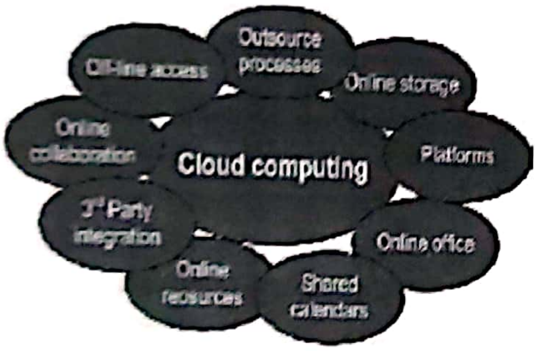
"Cloud" computing – a relatively recent term, defines the paths ahead in computer science world. Being built on decades of research it utilizes all recent achievements in virtualization, distributed computing, utility computing and networking. It implies a service oriented architecture through offering software's and platforms as services, reduced information technology overhead for the end-user, great flexibility, reduced total cost of ownership, on demand services and may other things. The skyrocketing demand for a new generation of cloud-based consumer and business application is driving the need for next generation of datacenters that must be massively scalable, efficient, agile, reliable and secure. We believe that the next generation cloud evolution is a fundamental transformation and not just an evolutionary stack collaboration networks utilizing optimally distributed and managed computing, network and storage resources driven in real time by business priorities. This paper is a brief survey based of readings on "cloud" computing and it tries to address, related research topics, advantages, dis advantages, challenges ahead and possible applications. Cloud computing is location-independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand, as with the electricity grid. Cloud computing is a natural evolution of the widespread adoption

of virtualization, service-oriented architecture and utility computing. Details are abstracted from consumers, who no longer have need for expertise in, or control over, the technology infrastructure "in the cloud" that supports them.

Keyword—Component, formatting, style, styling, insert.

Introduction

Utilizing computing or communication resources (hardware and software) which can provide service over network (may be on networked computers or internet) is known as Cloud Computing. Due to the cloud shaped symbol used in the infrastructure in system diagram, it is given the name as "Cloud". Cloud computing entrusts remote services with a user's data, software and computation.



History

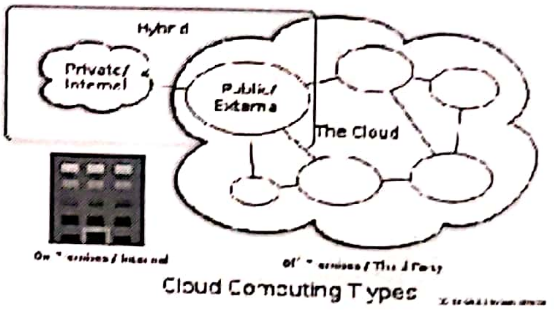
John McCarthy opined in the 1960s that "computation may someday be organized as a public utility." Almost all the modern-day characteristics of cloud computing". Cloud Computing was thoroughly explored in Douglas Parkhill's 1966 book, The Challenge of the Computer Utility. In 1950s when scientist Herb Grosch (the author of Grosch's law) postulated that the entire world would operate on dumb terminals powered by about 15 large data centers.

About Cloud Computing

Computing is a computing model, not a technology. In this model "customers" plug into the "cloud" to access IT resources which are priced and provided "on-demand". Essentially, IT resources are rented and shared among multiple tenants much as office space, apartments, or storage spaces are used by tenants. Delivered over an Internet connection, the "cloud" replaces the company data center or server providing the same service. Thus, Cloud Computing is simply IT services sold and delivered over the Internet.

Cloud Computing vendors combine virtualization (one computer hosting several "virtual" servers), automated provisioning (servers have software installed automatically), and Internet connectivity technologies to provide the service. These are not new technologies but a new name applied to a collection of older (albeit updated) technologies that are packaged, sold and delivered in a new way.

Types of Cloud Computing



PUBLIC CLOUD

Public cloud applications, storage, and other resources are made available to the general public by a service provider. These services are free or offered on a pay-per-use model. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access only via Internet (direct connectivity is not offered).

COMMUNITY CLOUD

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

HYBRID CLOUD

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

By utilizing "hybrid cloud" architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

Hybrid clouds lack the flexibility, security and certainty of in-house applications. Hybrid cloud provides the flexibility of in house applications with the fault tolerance and scalability of cloud based services.

PRIVATE CLOUD

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and it will require the organization to reevaluate decisions about existing resources. When it is done right, it can have a positive impact on a business, but every one of the steps in the project raises security issues that must be addressed in order to avoid serious vulnerabilities.

They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

HOW IT WORKS

In traditional enterprise computing, IT departments forecast demand for applications and capacity and invest time and money to develop those resources in-house or purchase them from others and operate them in-house. With cloud computing, institutions pro-cure IT services from remote providers, and campus constituents access these resources over the Internet. E-mail, for example, long considered a staple of an institution's IT operations, can be ob-tained from a range of sources, and a growing number of campuses contract with outside suppliers for this function. Software is hosted by the provider and does not need to be installed—or maintained— on individual computers around campus. In some cases, a large university or a consortium might become a provider of cloud ser-vices. Storage and processing needs can also be met by the cloud. Institutions pay only for the resources used, and users can access the applications and files they need from virtually any Internet connected computer. In a mature cloud computing environment, institutions would be able to add new IT services or respond to changes in capacity on the fly, saving capital costs that can be redirected to programs of strategic value to the institution.

SECURITY

The information housed on the cloud is often seen as valuable to individuals with malicious intent. There is a lot of personal information and potentially secure data that people store on their computers, and this information is now being transferred to the cloud. This makes it critical for you to understand the security measures that your cloud provider has in place, and it is equally important to take personal precautions to secure your data.

The first thing you must look into is the security measures that your cloud provider already has in place. These vary from provider to provider and among the various types of clouds. What encryption methods do the providers have in place? What methods of protection do they have in place for the actual hardware that your data will be stored on? Will they have backups of my data? Do they have firewalls set up? If you have a community cloud, what barriers are in place to keep your information separate from other companies? Many cloud providers have standard terms and conditions that may answer these questions, but the home user will probably have little.

After the internet boom, Amazon played a key role in the development of cloud computing by modernizing their data centers, which, like most computer networks, were using as little as 10% of their capacity at any one time, just to leave room for occasional spikes. Having found that the new cloud architecture resulted in significant internal efficiency improvements whereby small, fast-moving "two-pizza teams" could add new features faster and more easily, Amazon initiated a new product development effort to provide cloud computing to external customers, and launched Amazon Web Service (AWS) on a utility computing basis in 2006.

In early 2008, **Eucalyptus** became the first open-source, AWS API-compatible platform for deploying private clouds.

In early 2008, **OpenNebula**, enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid clouds, and for the federation of clouds. In the same year, efforts were focused on providing quality of service guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting to a **real-time cloud environment**. By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them" and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing... will result in dramatic growth in IT products in some areas and significant reductions in other areas."

On March 1, 2011, IBM announced the Smarter Computing framework to support Smarter Planet. Among the various components of the Smarter Computing foundation, cloud computing is a critical piece.

In 2012, Dr. Biju John and Dr. Souheil Khaddaj describe the cloud as a virtualized, semantic source of information: "Cloud computing is a universal collection of data which extends over the internet in the form of resources (such as information hardware, various platforms, services etc.) and forms individual units within the virtualization environment. Held together by infrastructure providers, service providers and the consumer, then it is semantically accessed by various users."

CHARACTERSTICS

Cloud computing exhibits the following key characteristics:

Agility improves with users' ability to re provision technological infrastructure resources

Application Programming Interface (API, accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers. Cloud computing systems typically use REST-based APIs.

Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure. This is purported to lower barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usage-based options and fewer IT skills are required for implementation (in-house). The e-FISCAL project's state of the art repository contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.

Virtualization technology allows servers and storage devices to be shared and utilization be increased. Applications can be easily migrated from one physical server to another.

Multitenancy enables sharing of resources and costs across a large pool of users thus allowing for:

Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.)

Peak-load capacity increases (users need not engineer for highest possible load-levels)

Utilization and efficiency improvements for systems that are often only 10–20% utilized.

Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.

Scalability and elasticity via dynamic ("on-demand") provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.

Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

ARCHITECTURE

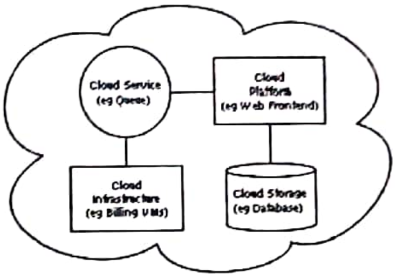


Figure 3: Cloud Computing Sample Architecture

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communi cating with each other over a loose coupling mechanism such as a messaging queue. Elastic provision implies intelligence in the use of tight or loose coupling as applied to mechanisms such as these and others.

THE INTERCLOUD

The Intercloud is an interconnected global "cloud of clouds" and an extension of the Internet "network of networks" on which it is based.

CLOUD ENGINEERING

Cloud engineering is the application of engineering disciplines to cloud computing. It brings a systematic approach to the high-level concerns of commercialisation, standardisation, and governance in conceiving, developing, operating and maintaining cloud computing systems. It is a multidisciplinary method encompassing contributions from diverse areas such as systems, software, web, performance, information, security, platform, risk, and quality engineering.

CLOUD GAMING

Cloud gaming, also called gaming on demand, is a type of online gaming that allows direct and on-demand streaming of games onto a computer, similar to video on demand, through the use of a thin client, in which the actual game is stored on the operator's or game company's server and is streamed directly to computers accessing the server through the client. This allows access to games without the need of a console and largely makes the capability of the user's computer unimportant, as the server is the system that is running the processing needs. The controls and button presses from the user are transmitted directly to the server, where they are recorded, and the server then sends back the game's response to the input controls.

Gaming on demand is a game service which will take advantage of a broadband connection, large server clusters, encryption and compression to stream game content directly to a subscriber. Game content isn't stored on the user's machine and game code execution occurs primarily at the server so a less powerful computer can be used than the game would normally require.

Acknowledgment

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression, "One of us (R. B. G.) thanks . . ." Instead, try "R. B. G. thanks". Put applicable sponsor acknowledgments here; DO NOT place them on the first page of your paper or as a footnote.

THE FUTURE OF CLOUD COMPUTING

Cloud computing may be a relatively new concept for some businesses and consumers. But even though some businesses are only starting to adopt and realizing the advantages of cloud computing, industry giants are already looking forward to the next big step of cloud computing. For now, cloud computing could be easily identified with grid computing wherein the "cloud" become the application for business purposes. Although grid computing is more focused on the server capabilities of the application, their similarities are based on the focus on providing online and on-time services to the enterprise. But cloud computing is so much more than simplified "cloud" processing. The business aim of getting things done no matter where they are without the necessary of a local or desktop software is realized. The ease of data processing with real time interaction and company-wide availability of data in an instant could be done through proper implementation of cloud computing. Best of all, these processes are aimed to be available with very little to no downtime. The future of cloud computing should be highly considered by businesses in any industry. The possibility of full adaptation of cloud computing by almost any industry is slowly starting to happen. If a business will not consider their future in cloud computing, the challenges as well as the advantages of cloud computing may not be addressed and fully harnessed.

CONCLUSION

Cloud computing is the next big wave in computing. It has many benefits, such as better hardware management, It also provides for better and easier management of data security, since all the data is located on a central server. Agility improves with user's ability to rapidly and inexpensively re-provision technological infrastructure resources. It largely based on the effective implementation of its architecture. There are some down sides as well to cloud computing. The biggest of them all is security. There is also the challenge of the end user connectivity. It might not work in areas where internet connection is weak. Implementing cloud computing through a platform is one of the most popular option for business today in online transition. Cloud computing can be private or public nature. It is general term for anything that involves delivering hosted services over the internet.

I hope you have learned a lot about cloud computing and the bright future it has in the coming years.

REFERENCES:

1.en.wikipedia.org/wiki/Cloud_computing

2. www.en.masterbase.com/support/glossary.asp

3. www.servepath.com/support

4. ets.tlt.psu.edu/learningdesign/web20glossary

5. www.financenewmexico.org

6.en.citizendium.org/wiki/Cloud_computing

7. Danielson, Krissi (2008-03-26). Distinguishing Cloud Computing from Utility Computing. Ebizq.net. Retrieved 2010-08-22.

8. "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner.com. Retrieved 2010-08-22.

9. Gruman, Galen (2008-04-07). What cloud computing really means. InfoWorld. Retrieved 2009-06-02.

10. Cloud Computing: Clash of the clouds. The Economist. 2009-10-15. Retrieved 2009-11-03.

11. Cloud Computing Defined 17 July 2010. Retrieved 26 July 2010.

12. NIST.gov - Computer Security Division - Computer Security Resource Center. Csrc.nist.gov. Retrieved 2010-08-22.

13. Writing & Speaking. Sellsbrothers.com. Retrieved 2010-08-22.

14. The Internet Cloud. Thestandard.com. Retrieved 2010-08-22.

15. What's In A Name? Utility vs. Cloud vs Grid. Datacenterknowledge.com. Retrieved 2010-08-22.

16. Distributed Application Architecture. Sun Microsystem. Retrieved 2009-06-16.

17. Service-Oriented Computing and CloudComputing: Challenges and Opportunities. IEEE Internet Computing. Retrieved 2010-12-04.

09

Password cracking & Security

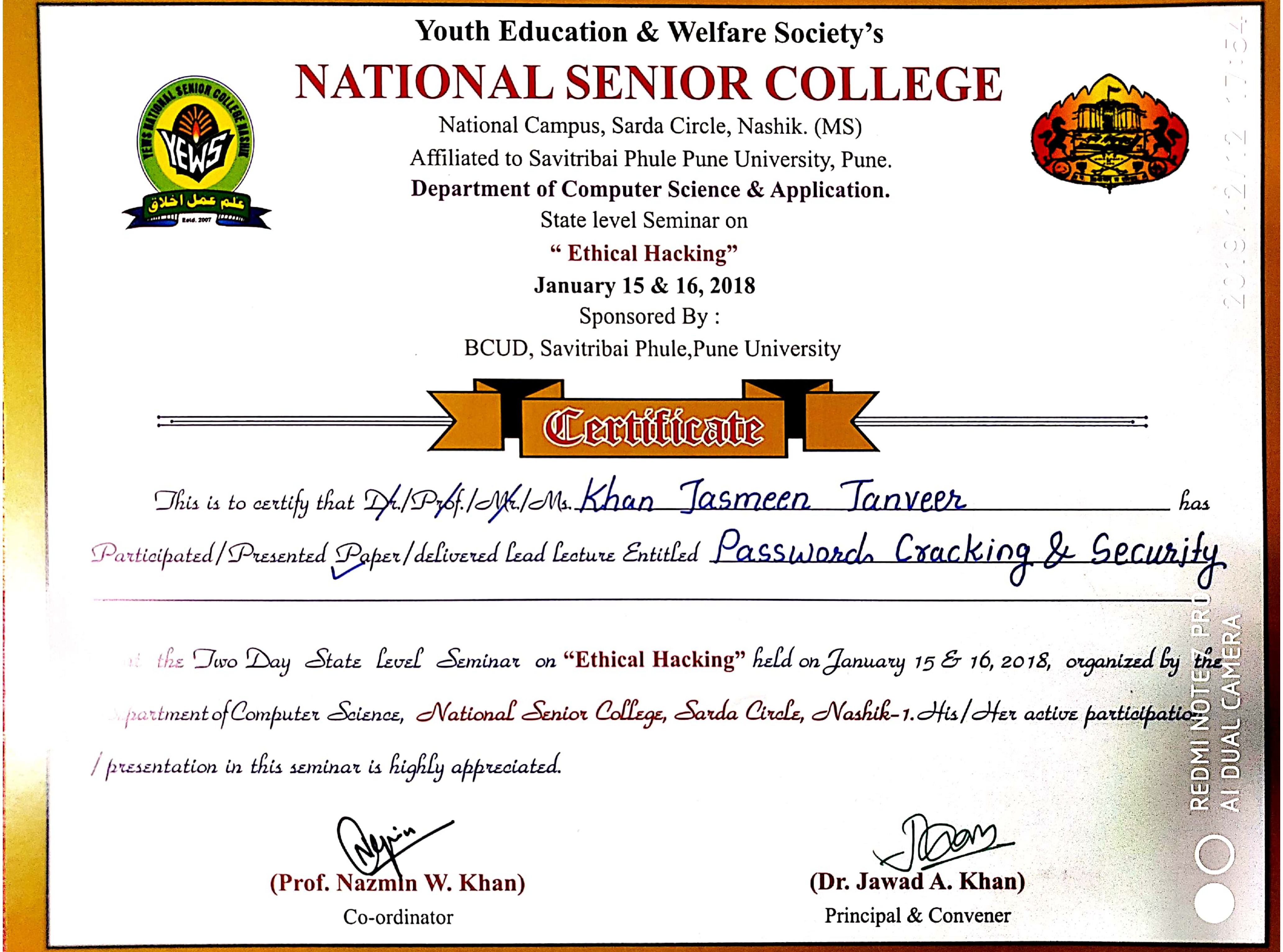
Khan Jasmeen Tanveer
YEWS National Senior College, Nasik

****

ABSTRACT:

Now a days, attacking the passwords is one of the most straight forward attack vectors, which authorize access to information system. There are numerous feasible methods, attempt to guess or crack passwords, with a different methods, approaches and tools. This paper analyse the possibilities of using the tools and gives an example of how to accomplish the password guesses in different methods with tests which can be demonstrated together. Password cracking is the process of recovering password from data. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk), to gain unauthorized access to a system, or as a preventive measure by system administrator to check for easily crack able passwords. Algorithms create hashes of passwords that are designed to protect passwords from being readily cracked. Security tokens constantly shift passwords so that even if a password is cracked, it can be used for a very limited amount of time. Password crackers use two primary methods to identify correct passwords brute force and dictionary searches. When a password cracker uses brute force, it runs through combinations of characters within unreversible length until it finds the combination accepted by the computer system.The words "cracking" and "hacking" refers to ethical cracking and ethical hacking and do not promote any illegal activity.[1]

KEYWORDS: password cracking attack,



Youth Education & Welfare Society's

NATIONAL SENIOR COLLEGE

National Campus, Sarda Circle, Nashik. (MS)
Affiliated to Savitribai Phule Pune University, Pune.
Department of Computer Science & Application.
State level Seminar on
" Ethical Hacking"
January 15 & 16, 2018
Sponsored By :
BCUD, Savitribai Phule,Pune University

Certificate

This is to certify that ~~Dr.~~/~~Prof.~~/~~Mr.~~/Ms. Khan Jasmeen Tanveer has Participated/Presented Paper ✓/delivered lead lecture Entitled Password Cracking & Security

at the Two Day State level Seminar on **"Ethical Hacking"** held on January 15 & 16, 2018, organized by the Department of Computer Science, National Senior College, Sarda Circle, Nashik-1. His/Her active participation / presentation in this seminar is highly appreciated.

(Prof. Nazmin W. Khan)
Co-ordinator

(Dr. Jawad A. Khan)
Principal & Convener

International Multilingual Research Journal

Printing Area™

ISSN 2394-5303

Two Day State Level Seminar
on
Ethical Hacking

Jointly Organized By

Department of Computer Science and Application
&
BCUD, Savitribai Phule Pune University

Convener
Dr. J.A. Khan
Principal

Coordinator
Ms. Khan Nazmin Wasim
Asst. Professor

Asst. Coordinator
Mr. Owyes Siddiqui
Asst. Professor

NATIONAL SENIOR COLLEGE
National Campus, Maulana Azad Road, Sarda Cirrcle, Nashik

|| Index ||

International Multilingual Research Journal

Printing Area

9850203295 7588057695

Editor Dr.Bapu G.Gholap

anything th nvolves delivering hosted services over the int et.

I ho, 'ou have learned a lot about cloud computing I the bright future it has in the coming yeaı

REFERENCES

1.en.w pedia.org/wiki/Cloud_computing

2. ww :n.masterbase.com/support/glossary.asp

3.v .servepath.com/support

4. .s.tlt.psu.edu/learningdesign/web20g' ary

5. www.financenewmexico.org

6.en.citizendium.org/wiki/Cloud_computing

7. Danielson, Krissi (2008-03-26). Distinguishing Cloud Computing from Utility Computing. Ebizq.net. Retrieved 2010-08-22.

8. "Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner.com. Retrieved 2010-08-22.

9. Gruman, Galen (2008-04-07). What cloud computing really means. InfoWorld. Retrieved 2009-06-02.

10. Cloud Computing: Clash of the clouds. The Economist. 2009-10-15. Retrieved 2009-11-03.

11. Cloud Computing Defined 17 July 2010. Retrieved 26 July 2010.

12. NIST.gov - Computer Security Division - Computer Security Resource Center. Csrc.nist.gov. Retrieved 2010-08-22.

13. Writing & Speaking. Sellsbrothers.com. Retrieved 2010-08-22.

14. The Internet Cloud. Thestandard.com. Retrieved 2010-08-22.

15. What's In A Name? Utility vs. Cloud vs Grid. Datacenterknowledge.com. Retrieved 2010-08-22.

16. Distributed Application Architecture. Sun Microsystem. Retrieved 2009-06-16.

17. Service-Oriented Computing and CloudComputing: Challenges and Opportunities. IEEE Internet Computing. Retrieved 2010-12-04.

09

Password cracking & Security

Khan Jasmeen Tanveer
YEWS National Senior College, Nasik

****

ABSTRACT:

Now a days, attacking the passwords is one of the most straight forward attack vectors, which authorize access to information system. There are numerous feasible methods, attempt to guess or crack passwords, with a different methods, approaches and tools. This paper analyse the possibilities of using the tools and gives an example of how to accomplish the password guesses in different methods with tests which can be demonstrated together. Password cracking is the process of recovering password from data. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk), to gain unauthorized access to a system, or as a preventive measure by system administrator to check for easily crack able passwords. Algorithms create hashes of passwords that are designed to protect passwords from being readily cracked. Security tokens constantly shift passwords so that even if a password is cracked, it can be used for a very limited amount of time. Password crackers use two primary methods to identify correct passwords brute force and dictionary searches. When a password cracker uses brute force, it runs through combinations of characters within unreversible length until it finds the combination accepted by the computer system.The words "cracking" and "hacking" refers to ethical cracking and ethical hacking and do not promote any illegal activity.[1]

KEYWORDS: password cracking attack,

password cracking program & data security.

INTRODUCTION:

Access control to information systems is often implemented via passwords; hence, attacking the passwords is one of the most straight forward attack vectors. Typical computer users nowadays require passwords for purposes logging into the system accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, e-banking etc. Furthermore, a password is a secret word or string of characters that is used for authenti cation in order to prove identity or gain access to a resource. The password should be kept secret from those which do not have allowed access.The processes of attempting to guess or crack passwords to gain access to a computer system or network. Crackers will generally use a variety of tools, scripts, or software to crack a system password. The goal of the cracker is to ideally obtain the password for root (UNIX) or system and administrator. Password cracks work by comparing every encrypted dictionary word against the entries in system password file until a match is found. If the password cracking is conducted online, the protection system usually locks out the users after they failed to login the system for more than three times to block the automated guessing software. However, the offline attacks usually escape from this. In the offline attack, hackers first break into a system to steal the encrypted password files or eavesdrop on an encrypted exchange on the internet. Then the password cracker can take as long as they need to try and crack the code without alerting the target system or individual user.

In most systems, passwords are stored in a protected (hash) form snooper that gains internal access to system cannot easily retrieve/ steal passwords every time a user logs in, password handling software runs the hash algorithm. Password cracking techniques are used to recover passwords from computer systems .Attackers use password cracking techniques to gain unauthorized access to the vulnerable system. Most of the password cracking techniques are successful due to weak or easily guessable passwords.Password cracking or 'password hacking' as is it more commonly referred to a cornerstone of Cyber security and security in general. Password hacking software has evolved tremendously over the last few years but essentially it comes down to several thing, firstly what systems are in place to prevent certain popular types of password cracking technique and secondly, what is the computing processing power of the hacker, Typically password hacking involves a hacker brute forcing their way into a website admin panel (or login page) and bombarding the server with millions of variations to enter the system. That requires CPU. Password and user account exploitation is one of largest issues in network security Password cracking is aterm used to describe the penetration of a network, system or resource with or without the use of tools to unlock a resource that has been secured with a password.[2]

Storing passwords

If you have to choose between weak passwords that your users can memorize and strong passwords that your users must write down, I recommend having readers write down passwords and store the information securely. Train users to store their written passwords in a secure place — not on keyboards or in easily cracked password-protected computer files (such as spreadsheets). Users should store a written password in either of these locations:

A locked file cabinet or office safe

An encrypted file or database, using such tools as

o PGP (www.pgpi.org for the free open-source version or www.pgp.com for the commercial version)

o Open-source Password Safe, originally developed by Counterpane(passwordsafe.sourceforge.net)[3]

what is password cracking:

Password cracking is the process of guessing or recovering a password from stored locations or from data transmission system. It is used to get a password for unauthorized access or to recover a forgotten password. In penetration testing, it is used to check the security of an application. If the password is strong enough with a combination of numbers, characters and special characters, this cracking method may take hours to weeks or months. A few password cracking tools use a dictionary that contains passwords. These tools are totally dependent on the dictionary, so success rate is lower.In the past few years, programmers have developed many password cracking tools.A password is the secret word or phrase that is used for the authentication process in various applications. It is used to gain access to accounts and resources. A password protects our accounts or resources from unauthorized access.[4]

10 Most Popular Password Cracking Tools

1. Brutus:

If you don't know, Brutus Password Cracker is one of the fastest, most flexible remote password crackers you can get your hands on –it's also free to download Brutus. It is available for Windows 9x, NT and 2000, there is no UN*X version available although it is a possibility at some point in the future .Brutus is one of the most popular remote online password cracking tools. It claims to be the fastest and most flexible password cracking tool. This tool is free and is only available for Windows systems. It was released back in October 2000.This tool has not been updated for many years. Still, it can be useful for you.

2. Rainbow cracking:

Rainbow Crack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. It crack hashes with rainbow tables. Rainbow Crack uses time-memory trade-off algorithm to crack hashes. It differs from brute force hash crackers. After computation, results are stored in the rainbow table. This process is very time consuming. But, once the table is ready, it can crack a password must faster than brute force tools.

3. Wfuzz:

Wfuzz is another web application password cracking tool that tries to crack passwords with brute forcing. Wfuzz is a tool designed to brute force web applications, it was created to facilitate the task in web applications assessments, and it's a tool by pen testers for pen tester. It can also be used to find hidden resources like directories, servlets and scripts.

Key features of Wfuzz password cracking tool:

Output in colored HTML
Brute force HTTP Password
POST and GET brute forcing

4. Cain and Abel:

Cain and Abel is a well-known password cracking tool that is capable of handling a variety of tasks. The most notable thing is that the tool is only available for Windows plat forms .can and able is a password recovery tool for

Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks .Cain & Abel is a useful tool for network administrators teachers, security consultants/ professionals, forensic staff, security software vendors, professional penetration tester and everyone else that plans to use it for ethical reasons.

5: John the Ripper:

John the Ripper is free and Open Source software, distributed primarily in source code form. If you would rather use a commercial product tailored for your specific operating system, please consider John the Ripper, which is distributed primarily in the form of "native" packages for the target operating systems and in general is meant to be easier to install and use while delivering optimal performance. John the Ripper is another well-known free open source password cracking tool for Linux, UNIX and Mac OS X. A Windows version is also available. This tool can detect weak passwords.

6: THC Hydra:

THC Hydra Download below, this software rocks, it's pretty much the most up to date and currently developed password brute forcing tool around at the moment. THC Hydra is a fast network logon password cracking tool. When it is compared with other similar tools, it shows why it is faster. New modules are easy to install in the tool. You can easily add modules and enhance the features. It is available for Windows, Linux, Solaris and OS X.

7. Medusa:

Medusa is also a password cracking tool similar to THC Hydra. Medusa is a speedy, massively parallel, modular, login brute-force for network services created by the geeks at Foofus.net. Medusa uses brute force attack to create passwords. It is also faster as compared to other password crackers. You can also perform a parallel attack. Suppose you want to crack passwords of a few email accounts simultaneously. You can specify the username list along with the password list.

8. OphCrack:

OphCrack is a free rainbow-table based password cracking tool for Windows. It is the most popular Windows password cracking tool, but can also be used on Linux and Mac systems. For cracking Windows XP, Vista and Windows 7, free rainbow-tables are also available.

Features:

•» Runs on Windows, Linux/Unix, Mac OS X,

•» Cracks LM and NTLM hashes.

•» Free tables available for Windows XP and Vista/7.

•» Brute-force module for simple passwords.

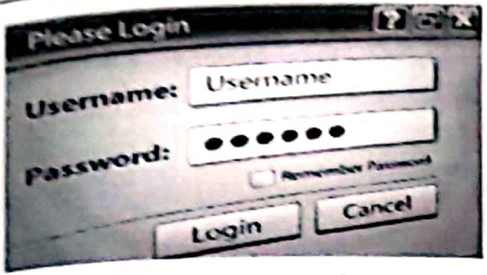
9: L0phtCrack:

L0phtCrack is a login & password auditor and recovery application originally produced by Mudge from L0pht Heavy Industries. In January 2009, L0phtCrack was acquired by the original authors Zatko, Wysopal, and Rioux from Symantec.L0phtCrack is an alternative to OPH Crack. It attempts to crack Windows password from hashes. For cracking passwords, it uses Windows workstations, network servers, primary domain controllers, and Active Directory. Lophtcrack is a login & password auditor and recovery application originally produced by Mudge from L0pht Heavy Industries.

10: Aircrack-NG:

Aircrack-NG is a Wi-Fi password cracking tool that can crack WEP or WPA passwords. Aircrack-NG is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It analyses wireless encrypted packets and then tries to crack passwords via its cracking algorithm.[56]

Five seven ways to protect your password from hackers :



1. Don't pick a weak password:

Password', '123456' or 'abc123' are horrible passwords because they're easy to guess. One way to build a strong password is to think of a phrase or sentence that other people wouldn't know and then use that to build your password. For example, think of a personal message like "I want to see more Indian women in technology" and then build your password from numbers, symbols and the first letters of each word—'iw2sm!. When you're asked to create or update a password for a site, avoid simple patterns that are easily guessed. SplashData and TeamsID suggest you select something that's 12 characters or longer, using letters, numbers and other symbols.

2.Different accounts need different passwords:

While it's certainly easier to use the same password on multiple accounts, remember that doing so can increase your defenceless ness' Not only can hackers use that password to access other important accounts of yours, you're also opening yourself up to security from a larger number of people trying to crack many different accounts.

Just like you wouldn't use the same key for your home, car and office, you should never use the same password across different websites. Some websites allow you to add an extra layer of security to your account by enabling a one-time password. Often referred to as an 'OTP', this will require you to enter another 'key' or code to unlock your account in addition to your password. If you regularly visit a large number of sites and worry you'll forget which password to use, this next tip will come in handy.

3. Consider a password manager:

Password managers keep track of the various usernames and passwords you use on various accounts, not only boosting safety but saving you time by automatically filling in the username/password fields. They'll also syn chronize your passwords across different devices, meaning you won't be stumped if you logon to a site from your smartphone but registered on your laptop. There are several options to choose from, including offerings from Norton, Dash line, Last Pass.

4. Don't share your password:

This seems like common sense, but some people still freely give their passwords to others. Globally, says Norton, 31 percent of millennial are likely to share theirs. And one-third of the people who say they' we shared their password in the U.S. have shared the password to their bank account. Don't be one of those people.

5. update your software:

It seems we're notified almost daily about some program or another that requires an update.If you do forget your password or get locked out, you need a way to get back into your account. Many services will send an email to you at a recovery email address if you need to reset your password. So it's important to make sure your recovery email address is up-to-date and is linked to an account you can still access.

6. If Biometric is an option:

Take it Smart phones, tablets and laptops are increasingly letting you log on with a finger print instead of a password. That's not only more secure, it also prevents you from forgetting your password.HSBC is one company embracing the movement, launching voice recognition and touch security services for up to 15 million U.K. customers who access their accounts through their mobile devices.

7. Check your settings always:

Social networking sites allow you to share photos, videos, status updates and much more. Many of these services offer privacy settings and controls that help you decide who can see your content before you post it.[7] & [8]

Linux and UNIX

The following countermeasures can help prevent password cracks on Linux & UNIX systems:

Use shadowed MD5 passwords.

Help prevent weak passwords from being created. You can use either built-in operating-system password filtering (such as crackle in Linux) or a password auditing program (such as unpassed or passes).

Check your /etc./passed file for duplicate root UID entries. Hackers can exploit such entries as root backdoors.[9]

CONCLUSION:

In day to day life we know about hackers, in this time every person's account and personal information is not secure any person can crack our passwords and misuses our data that's why security is necessary.

Many authentication schemes depend on secret passwords. Unfortunately, the length and of the passwords users choose remain fixed over time. As a result, password scheme are failing to withstand off-line password guessing attacks. So it's our responsibility to safe our data with the help of strong passwords, & also remember that password.

REFERENCE:

https://www.google.co.in/search?q=information+of+password+cracking&oq=information+of+password+cracking.

https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords.

https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords.

ACKNOWLEDGMENT:

As a student, it is my small step to accomplish long academic journey. As a beginner, I have taken every precaution of a reference that should not go unnoticed. I am highly thankful and remain grateful to the entir authors, whose research papers, books an articles have been referred. By mistakes, if any authors have been left to be referred, I seek apology from them and hope honourable authors will cast their mercy and excuse me. This research paper would not have been possible without the support and encouragement of my colleague and friends & this research was supported/partially supported by colleague we are thankful to our colleagues who provided opportunity for fetch your expertise.

(Footnotes)

1. file:///C:/Users/Admin/Downloads/khan%20pdf.pdf

2. file:///C:/Users/Admin/Downloads/khan%20pdf.pdf

3. file:///C:/Users/Admin/Downloads/khans.cc%20file.pdf

4. http://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

5. http://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

6.https://www.google.co.in/search?q=ten+tools+of+password+cracking&oq=ten+tools+of+password+ cracking&aqs=chrome..69i57.9374j0j7 &sourceid=chrome&ie=UTF-8

7.https://www.cnbc.com/2016/02/24/8-ways-to-protect-your-passwords-from-identity-theft-online.html

8. Ibid

9. file:///C:/Users/Admin/Downloads/khans.cc%20file.pdf

□□□

International Multilingual Research Journal

Printing Area

ISSN 2394-5303

Two Day State Level Seminar
on

Ethical Hacking

Jointly Organized By

Department of Computer Science and Application
&
BCUD, Savitribai Phule Pune University

Convener
Dr. J.A. Khan
Principal

Coordinator
Ms. Khan Nazmin Wasim
Asst. Professor

Asst. Coordinator
Mr. Owyes Siddiqui
Asst. Professor

NATIONAL SENIOR COLLEGE
National Campus, Maulana Azad Road, Sarda Cirrcle, Nashik

|| Index ||

International Multilingual Research Journal

Printing Area

9850203295 7588057695

Editor Dr.Bapu G.Gholap

10

Cyber Crime & Its Prevention Techniques

Khan Shohira Aqueel
YEWS National Senior College Nasik.

ABSTRACT:

The internet, as we know, has grown swiftly over the last thirty years. As the world moves online, new opportunities for computer misuse and criminal activity have arisen. Cybercrime is a relatively new phenomenon. Cyber criminals carry out online frauds and other criminal activities such as email espionage, credit card fraud, financial frauds, online defamation, spreading of viruses, data theft, obscenity, online pornography, phishing and violence and so on. Cybercrime is becoming ever more serious.[1]Finding from the 2002 computer crime and security survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in information age.

It has become very important for us to be aware of the various cybercrimes that has being committed with the help of computers. To keep our increasingly cyber-dependent society safe and secure, researcher in cyber-security must constantly keep abreast of current threats in order to innovate new and better ways to counter them. This paper is an attempt to provide a glimpse of various types of cybercrimes prevalent in modern technological society and what steps can be taken to protect ourselves from these cybercrimes.

KEYWORDS: Cyber-crime, Cyber Attacks, Electronic crime, cybercrime preventions.

INTRODUCTION:

The first recorded cybercrime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan, and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is first recorded cybercrime.[2]

Today computers have come a long way, with neutral networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a billions operations per second. Cyber-crime en compasses criminal actions that target computers, internet, or network utility, damaging functionality or infiltrating systems and processes. Cybercrime is the criminal activity done using computers and internet. This includes anything from downloading illegal music file to stealing millions of dollars from online bank accounts.[3]Cybercrime also includes non-monetary offences, Such as creating and distributing viruses on other computers or posting confidential business information on the internet. Computer and computer network used as a tool or a target or a place of criminal activity. Crime committed using a computer and internet to steal a person's identification or illegal imports or malicious programs. Cyber crime is nothing but where the computer used as an object or subject of crime. Cybercrime is the latest and perhaps the most complicated problem in the cyber world.

TYPES OF CYBERCRIME:

When any crime is committed over the

internet it is refered to as a cybercrime. There are many types of cyber crimes .

HACKING:

It is a term that defines sending an illegal instruction to any other computer or network. This is a type of crime takes place wherein a person's computer information can be accesed by an another person by which his sensitive information can be used by another person which can cause a measure harm to his personal data and information. In hacking, the criminal uses a variety of software to enter a person's computer and a person may or may not be aware that his computer is being accessed from a remote location.

MALICIOUS SOFTWARE:

Malicious software or Malware are Internet-based software or programs that are used to disrupt a network. Malware includes computer viruses,worms,trojan horses, spyware, crimeware and other unwanted softwares.These softwares are design to infiltrate computer system without any owner's informed consent. These softwares are used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.[4]

PIRACY OR THEFT:

This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.[5]

IDENTITY THEFT:

Identity theft is also known as identity fraud. It is a crime which occurs when someone uses another's personally identifying information like their name,bank account number, debit card & credit card details and other sensitive information to siphon money or to buy things online in the victim's name. This has become a major problem with people using the Internet for cash transactions and banking services.

WEB JACKING:

This term is derive from term hi jacking. In this kinds of offences the hacker gains access and control over website of anothor.He may also change the information on site.In this kind of attack, the actual website is never touched. Instead, the system (DNS) that resolves website URL to IP address is compromised. The internet works on the principle that every computer and website has a unique IP address. To browse a website, we simply type in URL into the browser. The browser makes DNS request to get the real address of the website.Only then can it connect to website. In a webjacking attack, DNS entries are modified so that the real website's URL now points to anothor website's IP address. Hence the DNS server replies with the malicious site IP address, Whichthe browser then connect to and display to us.This attack may be donefor fullfill political objectives or for money.[6]

PHISHING:

Phishing is a type of social engineering attack often used to steal users data, including login credentials & credit card details etc. phishing attacks typically rely on social networking techniques applied to email or other electronic communication methods, including direct messege send over social networks,SMS text messeges.In phishing, the attacker would create a situation were users believe that they are dealing with an authorized party,such as bank or any known social media sites.The attacker will then ask the user for sensitive information such as username,passwords and credit card informationetc. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identity theft.[7]

PREVENTIONS:

Below are some technical solutions to

prevent you being hacked and scammed.

USE ANTI-VIRUS SOFTWARE AND SECURITY SOFTWARE:

Antivirus software or anti-malware software is computer software used to prevent, detect and remove malicious software. Antivirus software is a program that is designed to find and neutralize malware and viruses. Some of these software include McAfee, Norton and Stopzilla. These programs are able to scan your computer's hard drive and identity files that are malicious or suspicious. Hackers are constantly churning out new viruses and malware that is designed to steal financial information, website passwords and other sensitive information from innocent victim. Millions of new viruses pop up each year and new threats are discover every day.

In this constantly changing environment, it is impossible to completely avoid the threat of viruses but using trustworthy antivirus software can minimize your risk for infection and damage done. [8]

TWO-STEP VERIFICATION:

Two steps verification helps protect you by making it more difficult for someone else to sign in to your account. It uses two different forms of identity: your password, and contact method (also known as security info). Even if someone else finds your password, they will stop if they don't have access to your security info. This is also why it is important to use different passwords for all your accounts

If you set up two step verification with an email address, phone number, or authenticator app. When you sign in on a new device or from a new location, you will get a security code to enter on sign in page.

If your email or cloud service offers it - Gmail, Drop box, Apple and Face book do - take the trouble to set this up. In addition to entering your password, you are also asked to enter a verification code sent via SMS to your phone. So a hacker might crack your password, but without the unique and temporary verification code should not be able to access your account. Keying in a password or code 40-plus times a day might seem like a hassle but it is your first line of defense.[9]

ONLY SHOP ONLINE ON SECURE SITES:

Online retail has made shopping easier than ever, but it has also increased the likelihood of your private information ending up in the hands of wrong person. Before entering your card details, always ensure that the locked padlock or unbroken key symbol is showing in your browser. Additionally, the beginning of the online retailer's internet address will change from "http" to "https" to indicate a connection is secure. Be wary of sites that change back to http once you've logged on.

DIFFERENT SITE, DIFFERENT PASSWORDS:

Keeping a common password for all online accounts is a lot like having the same key for all locks. Only difference being that it is a lot easier to get hold of the online key. A single strong password just isn't enough any more. When people reuse the same password for their email,their bank account or any other site across the internet, then it won't take long for black hat hackers to identify multiple places they can use your stolen password. You must use different strong passwords on every site where you have an account-at least, every important site.[10]

DON'T STORE YOUR CARD DETAILS ON WEBSITES:

Err on the side of caution when asked if you want to store your credit card details for future use. Mass data security breaches (where credit card details are stolen en masse) aren't common, but why take the risk? The extra 90 seconds it takes to key in your details each time is a small price to pay.[11]

INSTALL FIREWALL:

Firewall software prevents hackers from getting into your computer system so be always have this switch on. To access your firewall setting, go to "windows control panel" and click on "Firewall".

CONCLUSION:

Obviously, cybercrime is on the rise, but so is the awareness and ability to get rid of it. In today's world, cybercrime is everyone's problem because every individual, every institutions and every organization is heavily dependent on it. Cybercrime seriously affects individuals, businesses, and national security due to the pervasiveness of the internet. User awareness is the key to secure computer/ network, so we must pay attention to all those issues and protect the world from cybercrime. "As internet technology advances so does the threat of cybercrime. In times like these we must protect ourselves from cybercrime. Antivirus software, frequently changing password or ID number, Never open suspicious emails and only navigate to trusted sites." The prevention is always better than cure. It is always better to take certain precaution while operating the net.

REFERENCES:

1) www.wikipedia.org
2) www.retailitinsight.com
3) www.ssijmar.in
4) www.cyberlawcentre.org
5) www.crossdomainsolutions.com
6) www.justia.com
7) https://mumbaimirror.indiatimes.com

ACKNOWLEDGMENT:

As a student, it is my small step to accomplish long academic journey. As a beginner, I have taken every precaution of a reference that should not go unnoticed. I am highly thankful and remain grateful to the entire authors, whose research papers, books and articles have been referred. By mistakes, if any authors have been left to be referred, I seek apology from them and hope honourable authors will cast their mercy and excuse me. This research paper would not have been possible without the support and encourage ment of my colleague and friends & this research was supported/partially supported by colleague we are thankful to our colleagues who provided opportunity for fetch your expertise.

(Footnotes)

1.https://www.techopedia.com/definition/2387/cybercrime

2 . http://cybercrime.planetindia.net/intro.htm

3 .www.wikieducator/computer_crime_and_criminals

4. https://en.m.wikibooks.org/wiki/information_security_in_education/malicious_software

5. www.crossdomainsolutions.com/cyber_crime/

6. https://www.digital4n6jornal.com/web_jacking

7. https://en.m.wikipedia.org/wiki/phishing

8. http://blog.technicalities.com.au/index.php/8-measures-prevent-cybercrime/

9. http://searchsecurity.techtarget.com/definition/two-step-verification

10.https://mumbaimirror.indiatimes.com/mumbai/other/12-ways-to-protect-tourself-from-cyber-crime/articlesshow/20025280.cms?prtpage=1

11. ibid

❑❑❑

International Multilingual Research Journal

Printing Area

ISSN 2394-5303

Two Day State Level Seminar
on

Ethical Hacking

Jointly Organized By
Department of Computer Science and Application
&
BCUD, Savitribai Phule Pune University

Convener
Dr. J.A. Khan
Principal

Coordinator
Ms. Khan Nazmin Wasim
Asst. Professor

Asst. Coordinator
Mr. Owyes Siddiqui
Asst. Professor

NATIONAL SENIOR COLLEGE
National Campus, Maulana Azad Road, Sarda Cirrcle, Nashik

|| Index ||

International Multilingual Research Journal

Printing Area

9850203295 7588057695

Editor Dr.Bapu G.Gholap

11

COMPUTER SECURITY: HACKERS AND VIRUSES

KHAN RIZWANA ABDURRAHMAN
YEWS NATIONAL SENIOR COLLEGE,NASHIK

****

ABSTRACT:

Even after thirty years of work on computer security, almost all the systems in service today are 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. Because there's been little damage, people decide that they don't need much security. Most of the time it 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.

KEYWORDS: Computer Security, viruses and hackers.

INTRODUCTION:

Its been more than 30 years that people have been working on computer system security. During this time there have been many intellectual successes. Notable among them are the subject/object access matrix model access control lists multilevel security using information flow and the star-property,public key cryptography, and cryptography protocols . In spite of these successes, it seems fair to say that in an absolute sense, the security of the hundreds of millions of deployed computer systems is terrible: a determined and competent attacker could destroy most of the information on almost any of these systems, or steal it from any system that is connected to a network. Even worse, the attacker could do this to millions of systems at once. The Internet has made computer security much more difficult than it used to be. In the good old days, a computer system had a few dozen users at most, all members of the same organization. It ran programs written in-house or by a few vendors. Information was moved from one computer to another by carrying tapes or disks.

COMPUTER SECURITY:

DEFINITION:

Computer security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.1[1]

GOALS OF COMPUTER SECURITY:

Integrity

Guarantee that the data is what we expect

Confidentiality

The information must just be accessible to the authorized people

Reliability

Computers should work without having unexpected problems

Authentication

Guarantee that only authorized persons can access to the resources

COMPUTER SYSTEM ASSETS:

Hardware

Threats include accidental and deliberate damage

Software

Threats include deletion, alteration,

damage

Backups of the most recent versions can maintain high availability

Data

Involves files

Security concerns for availability, secrecy, and integrity

Statistical analysis can lead to determination of individual information which threatens privacy.

VIRUSES:

DEFINITION:

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code.[1] Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive.[2]

WHAT IS COMPUTER VIRUS:

Computer virus refers to a program which damages computer systems and/or destroys or erases data files Virus is a small piece of program that can infect other programs by modifying them to include a copy of itself.

COMPUTR VIRUS HISTORY:

1988: Robert Morris made a worm that invaded ARPANET computers disabled 6,000 computers on the network by overflowing their memory banks with copies of itself

1991: Norton Anti-Virus software

1999: "Melissa" virus-infected thousands of computers very fast by sending copies of itself to 50 names in the address book on Outlook e-mail Led to an estimated $80 million in damage and record sales of anti-virus products.

2000: "I Love You" virus

-was sent by email and infected 10 % of computers in only one day

-created by a young Filipino computer student who did not get punished because then the Philippines had no laws against hacking which led to the European Union's global Cybercrime Treaty.

2001: "Nimda" virus.

-had 5 ways of infecting systems

2004: MyDoom spreads through emails and file-sharing software faster than any previous virus or worm.

Allows hackers to access the hard drive of the infected computer.

An estimated one million computers running Windows are affected by the fast-spreading Sasser computer worm.

The worm does not cause irreparable harm to computers or data, but it does slow computers and cause some to quit or reboot without explanation.

2006: Discovery of the first-ever malware Trojan horse for Mac OS X

2008: Tor pig is a Trojan horse which affects Windows, turning off anti-virus applications. It allows others to access the computer, modifies data, steals confidential information and installs malware on the victim's computer.

2009: Conficker infects anywhere from 9 to 15 million Microsoft server systems.

French air force, Royal Navy warships and submarines, Sheffield Hospital network, UK Ministry of Defence, German Bundeswehr and Norwegian Police were all affected.

DIFFERENCE BETWEEN VIRUS AND WORM:

The difference between a worm and a virus is that a virus does not have a propagation vector. i.e., it will only effect one host and does not propagate to other hosts. Worms propagate and infect other computers. Majority of threats are actually worms that propagate to other hosts.

TYPES OF COMPUTER VIRUS:

Time Bomb
Logical Bomb
Worm
Boot Sector Virus
Macros Virus
Script Virus
Trojan Virus.3[3]

TIME BOMB:

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met.

A time bomb is a virus program that performs an activity on a particular date

LOGICAL BOMB:

A logical bomb is a destructive program that performs an activity when a certain action has occurred.

Other way for the logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company.

WORM VIRUS:

A worm is also a destructive program that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

BOOT SECTOR VIRUS:

A boot sector virus infects boot sector of computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk.

Boot-sector viruses infect computer systems by copying code either to the boot sector on a floppy disk or the partition table on a hard disk. During startup, the virus is loaded into memory. Once in memory, the virus will infect any non-infected disks accessed by the system.

MACROS VIRUS:

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications).

A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it, macro virus is loaded into main memory and destroys the data stored in hard disk.

SCRIPT VIRUS:

Commonly found script viruses are written using the Visual Basic Scripting edition (VBS) and the JavaScript programming languages.

A Script Virus usually comes from webpage advertisements and is therefore wide-spread.

TROJAN VIRUS:

Trojan Horse is a destructive program. It usually pretends as computer games or application software. If executed, computer system will be damaged.

Trojan Horse usually comes with monitoring tools and key loggers.

These actions can include:

Deleting data
Blocking data
Modifying data
Copying data

VIRUS DETECTION:

Given a known computer virus V, consider the problem of detecting an infection by V.

The most straightforward approach to

solving this problem is just to scan incoming messages by <V>.

But virus can easily evade this technique by altering their text in ways that have no effect on computation that V performs.

For example, source code could be modified to add blanks in meaningless places or to add leading 0's to numbers.

Executable code could be modified by adding jump instructions to the next instruction.

So the practical virus detection problem can be stated as "Given a known virus V and an input message M", does M contain the text of a program that computes the same thing V computes?

We know the equivalence question is not decidable for turing machines, using that the equivalence question for arbitrary programs is also not decidable.

So, we can't solve the virus problem by making a list of known viruses and comparing new code to them.

Suppose that, instead of making a list of forbidden operations, we allowed users to define a "white list" of the operations that are to be allowed to be run on their machines.

Then the job of a virus filter is to compare incoming code to the operations on the white list.

Any code that is equivalent to some allowed operation can be declared safe. But now we have EXACTLY THE SAME PROBLEM. No test for equivalence exists.

HACKERS:

DEFNITION:

Computer hackers are unauthorized users who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent. Their clever tactics and detailed technical knowledge help them access information you really don't want them to have.[4]

TYPES OF HACKERS:

White hat

breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software.

Black hat

a black hat hacker who violates computer security for little reason beyond maliciousness or for personal gain . Black hat hackers break in to secure networks to destroy data or make the network unusable for those who are authorized to use the network.

Grey hat

A grey hat hackers is a combination of a black hat and a white hat hacker. A grey hacker may surf the internet and hack in to a computer system for the sole purpose of notifying the administrator that their system has a security defect

Ex: then they may offer to correct the defect for a fee

Script Kiddie

A script kiddie is some one who looks out to exploit vulnerability with not so much as trying to gain access to administrative or root access to the system

Underemployed Adult Hackers

Former Script Kiddies

Can't get employment in the field

Want recognition in hacker community

Big in eastern European countries

Ideological Hackers

hack as a mechanism to promote some political or ideological purpose

Usually coincide with political events

Crackers

Are the people aiming to create software tools that make it possible to attack computer systems or crack the copy protection of use-fee software. A crack is therefore an executable program created to modify the original software to as to remove its protection.

Carder's

Mainly attack chip card systems (particularly bank cards)

to understand how they work and to exploit their flaws. The term carding refers to chip card piracy.

HACKERS ACCESS YOUR INTERNET:

In 1988 a "worm program" written by a college student shut down about 10 percent of computers connected to the Internet. This was the beginning of the era of cyber attacks.

Today we have about 10,000 incidents of cyber attacks which are reported and the number grows.

Once inside hackers can..

Modify logs

To cover their tracks

To mess with you

Steal files

Sometimes destroy after stealing

A pro would steal and cover their tracks so to be undetected

Modify files

To let you know they were there

To cause mischief

Install back doors

So they can get in again

Attack other systems.[5]

COMMON ATTACKS:

Spoofing

Definition

An attacker alters his identity so that some one thinks he is some one else

Email, User ID, IP Address, ...

Attacker exploits trust relation between user and networked machines to gain access to machines

Types of Spoofing:

IP Spoofing

Email Spoofing

Web Spoofing

DENIAL OF SERVICE (DOS):

Definition

Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it.

Types:

Crashing the system or network

Send the victim data or packets which will cause system to crash or reboot.

Exhausting the resources by flooding the system or network with information

Since all resources are exhausted others are denied access to the resources

Distributed DOS attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks

PASSWORD ATTACKS:

A hacker can exploit a weak passwords & uncontrolled network modems easily

Steps

Hacker gets the phone number of a company

Hacker runs war dialer program

If original number is 555-5532 he runs all numbers in the 555-55xx range

When modem answers he records the phone number of modem

Hacker now needs a user id and password to enter company network

Companies often have default accounts e.g. temp, anonymous with no password

Often the root account uses company name as the password

For strong passwords password cracking techniques exist

PASSWORD SECURITY:

Password hashed and stored

Salt added to randomize password & stored on system

Password attacks launched to crack encrypted password

PASSWORD ATTACK- PROCESS:

Find a valid user ID

Create a list of possible passwords

Rank the passwords from high probability to low

Type in each password

If the system allows you in – success !

If not, try again, being careful not to exceed password lockout (the number of times you can guess a wrong password before the system shuts down and won't let you try any more)

PASSWORD ATTACKS- TYPES:

Dictionary Attack

Hacker tries all words in dictionary to crack password

70% of the people use dictionary words as passwords

Brute Force Attack

Try all permutations of the letters & symbols in the alphabet

Hybrid Attack

Words from dictionary and their variations used in attack

Social Engineering

People write passwords in different places

People disclose passwords naively to others

Shoulder Surfing

Hackers slyly watch over peoples shoulders to steal passwords

Dumpster Diving

People dump their trash papers in garbage which may contain information to crack passwords

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.

ETHICAL HACKERS : NOT CRIMINAL HACKERS

Completely trustworthy.

Strong programming and computer networking skills.

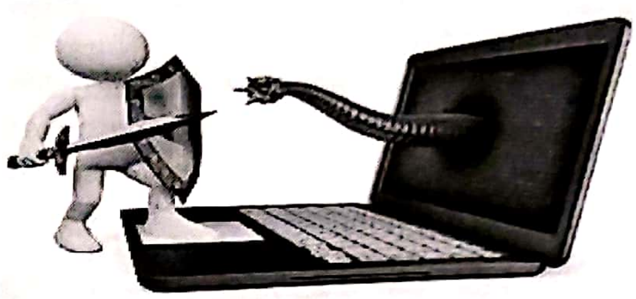
Learn about the system and trying to find its weaknesses.

Techniques of Criminal hackers-Detection-Prevention.

Published research papers or released security software.

No Ex-hackers.

PROTECTING:



SECURETY STRATEGIES:

Firewall

allows normal Web browser operations but prevents other types of communication

checks incoming data against a list of known sources

data rejected if it does not fit a preset profile

Network Sniffer

displays network traffic data

shows which resources employees use and Web sites they visit

can be used to troubleshoot network connections and improve system performance

Antivirus Software

detects and deletes known viruses

Internet allows antivirus software to update itself to detect newer viruses.

Some popular anti-virus programs:

McAfee

Norton Utilities

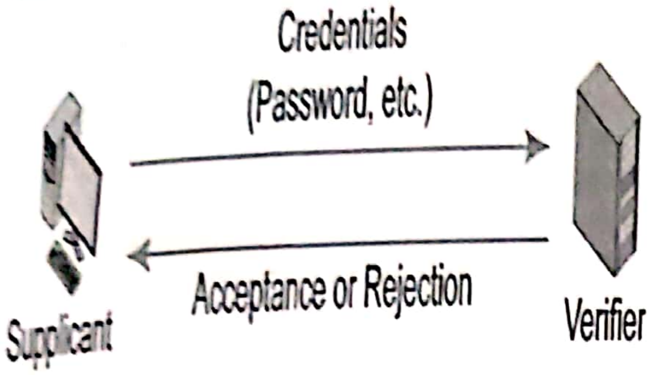
Inoculan

F-Secure

Internet Guard Dog

PC-cillin

AUTHENTICATION:



PASSWORD AUTHENTICATION:

Reusable Passwords

Strings of characters typed to authenticate the use of a username (account) on a computer.

They are used repeatedly and so are called reusable passwords.

Benefits

Ease of use for users (familiar)

Inexpensive because built into operating systems

Often Weak (Easy to Crack)

Word and name passwords are common.

spot, mud, helicopter, veterinarian

They can be cracked quickly with dictionary attacks.

Word and name passwords are never adequately strong, regardless of how long they are.

Passwords Should Be Complex

Should mix case, digits, and other keyboard characters ($, #, etc.).

Complex passwords can be cracked only with brute force attacks (trying all possibilities).

Passwords Also Should Be Long

Should have a minimum of eight characters.

Each added character increases the brute force search time by a factor of about 70.

ACCESS CONTROL:

Controlling Access to Resources

If criminals cannot get access, they cannot do harm.

Authentication

Proving one's identity

Cannot see the other party

HELPFUL HINTS TO AVOID VIRUSES:

Obtain software only from trusted sources.

Use a safe Web browser and e-mail client.

Scan all newly-obtained disks, programs, and files.

ACTIONS TO PREVENT VIRUS INFECTION:

Don't share Drive C: without a password and without read-only restrictions.

Empty floppy drives of diskettes before turning on computers, especially laptops.

Forget opening unexpected e-mail attachments, even if they're from friends

Get trained on your computer's anti-virus software and use it.

Have multiple backups of important files.

This lowers the chance that all are infected.

Install security updates for your operating system and programs as soon as possible.

Jump at the chance to learn more about your computer. This will help you spot viruses.

CONCLUSION:

Computer Security is a continuous battle

As computer security gets tighter hackers are getting smarter

REFERENCESS:

http://www.spamlaws.com/virus-comtypes.html

http://dataanalysis.vsb.cz/Data/Vyuka/PVB11%20Hacking.pdf

mputer%20Viruses.pdfhttp:/vxheaven.org/lib/pdf/Self-Replicating%20Turing%20Machines%20and%20co

http://www.spamlaws.com/virus-types.html

https://www.bing.com/search?q=computer+security+definition+&form=PRACE1&pc=ACTE&httpsmsn=1&refig=06c7d0e0621c4ee58f3c 044b04bbf6d4&sp=-1&pq=computer+security+ definition+&sc=2-29&qs=n&sk=&cvid=06c7d0e0621c4ee58f3c044b04bbf6d4

https://www.bing.com/search?q=definition+of+computer+virus&qs=n&form=QBRE&sp=-1&pq=definition+of+computer+virus&sc=8-28&sk=&cvid=D2506637401148O3B00DCEE9A91CED9D

ACKNOWLEDGMENT:

As a student, it is my small step to accomplish long academic journey. As a beginner, I have taken every precaution of a reference that should not go unnoticed. I am highly thankful and remain grateful to the entire authors, whose research papers, books and articles have been referred. By mistakes, if any authors have been left to be referred, I seek apology from them and hope honorable authors will cast their mercy and excuse me. This research paper would not have been possible without the support and encouragement of my colleague and friends & this research was supported/partially supported by colleague we are thankful to our colleagues who provided opportunity for fetch your expertise.

(Footnotes)

1. https://www.bing.com/search?q=computer+security+definition+&form=PRACE1&pc=ACTE&httpsmsn=1&refig=06c7d0e0621c4ee58f3c044b04bbf6d4&sp=-1&pq=computer +security+definition+&sc=2-29&qs=n&sk=&cvid=06c7d0e0621c4ee58f3c044b04bbf6d4

2. https://www.bing.com/search?q=definition+of+computer+ virus&qs=n&form=QBRE&sp=-1&pq=definition+of+computer+virus&sc=8-28&sk=&cvid=D2506637401148O3B00DCEE9A91CED9D

3. http//:www.spamlaws.com/virus-types.html

4. https://www.bing.com/search?q=computer+hacking&FORM=R5FD5

5. http://www.spamlaws.com/virus-types.html

❑❑❑

Youth Education & Welfare Society's

NATIONAL SENIOR COLLEGE

National Campus, Sarda Circle, Nashik. (MS)
Affiliated to Savitribai Phule Pune University, Pune.
Department of Computer Science & Application.
State level Seminar on
" Ethical Hacking"
January 15 & 16, 2018
Sponsored By :
BCUD, Savitribai Phule,Pune University

Certificate

This is to certify that ~~Dr.~~/~~Prof.~~/~~Mr.~~/Ms. Khan Rizwana Ab. Rahman *has Participated/[✓ Presented] Paper/delivered lead lecture Entitled* Computer Security : Hackers and Viruses

at the Two Day State level Seminar on **"Ethical Hacking"** *held on January 15 & 16, 2018, organized by the Department of Computer Science, National Senior College, Sarda Circle, Nashik-1. His/Her active participation / presentation in this seminar is highly appreciated.*

(Prof. Nazmin W. Khan)
Co-ordinator

(Dr. Jawad A. Khan)
Principal & Convener