Computer Security with Hackers

MIS 604 IT Solutions to Business Problems

Spring 2002

ali saleh albuhomoud

March 24, 2018

Put the question at the end of the explanation

introduction

Crisis Internet has grown very fast and security has lagged behind. Legions of hackers have emerged as impedance to entering the hackers club is low. It is hard to trace the perpetrator of cyber attacks since the real identities are camouflaged It is very hard to track down people because of the ubiquity of the network. Large scale failures of internet can have a catastrophic impact on the economy which relies heavily on electronic transactions. 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.

Computer Crime The Beginning

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. A 16-year-old music student called Richard Pryce, better known by the hacker alias Datastream Cowboy, is arrested and charged with breaking into hundreds of computers including those at the Griffiths Air Force base, Nasa and the Korean Atomic Research Institute. His online mentor, "Kuji", is never found. Also this year, a group directed by Russian hackers broke into the computers of Citibank and transferred more than 10$millionfromcustomers'accounts.Eventually, Citibankrecoveredallbut$400,000 of the pilfered money.

Computer Crime - 1995

In February, Kevin Mitnick is arrested for a second time. He is charged with stealing 20,000 credit card numbers. He eventually spends four years in jail and on his release his parole conditions demand that he avoid contact with computers and mobile phones. On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus. Mr Pile, who called himself the Black Baron, was sentenced to 18 months in jail. The US General Accounting Office reveals that US Defense Department computers sustained 250,000 attacks in 1995.

Why Security?

Some of the sites which have been compromised U.S. Department of Commerce NASA CIA Greenpeace Motorola UNICEF Church of Christ Some sites which have been rendered ineffective Yahoo Microsoft Amazon

Why do Hackers Attack?

Because they can A large fraction of hacker attacks have been pranks Financial Gain Espionage Venting anger at a company or organization Terrorism.

Types of Hacker Attack???

Active Attacks Denial of Service Breaking into a site Intelligence Gathering Resource Usage Deception Passive Attacks Sniffing Passwords Network Traffic Sensitive Information Information Gathering

Modes of Hacker Attack

Over the Internet

Over LAN

Locally

Offline

Theft

Deception

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

IP Spoofing Flying-Blind Attack

Definition: Attacker uses IP address of another computer to acquire information or gain access

Attacker changes his own IP address to spoofed address

Attacker can send messages to a machine masquerading as spoofed machine

Attacker can not receive messages from that machine

IP Spoofing Source Routing

Definition: Attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies.

The path a packet may change can vary over time.

To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network.

Password Attacks - 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 wont let you try any more)

Buffer Overflow Attacks

Programs which do not do not have a rigorous memory check in the code are vulnerable to this attack Simple weaknesses can be exploited If memory allocated for name is 50 characters, someone can break the system by sending a fictitious name of more than 50 characters Can be used for espionage, denial of service or compromising the integrity of the data Examples:

NetMeeting Buffer Overflow

Outlook Buffer Overflow

AOL Instant Messenger Buffer Overflow

SQL Server 2000 Extended Stored Procedure Buffer Overflow

hackers

Many people disagree about the definition of hackers. Many people link Hackers to hackers because they are always influenced by the media as criminals and saboteurs, some of whom are considered creative developers, because many of the projects were the result of group work of hackers. These projects include Linux, Wikipedia, and open source projects, and there is another term, the cracker. This term has emerged to distinguish between good hacker and corrupt hacker. The cracker is the one who always carries out subversive, criminal and intrusive actions that occur to corporate systems. He deserves the title of pirate computer, while the hacker is always trying to invent solutions and always seeks to creativity what he is doing.

Conclusions

Computer Security is a continuous battle As computer security gets tighter hackers are getting smarter Very high stakes

Hacker is the weapon of the world

thanks for listening