Unit-V

Advanced Computer Forensics:

The information economy, fueled by the widespread use of computers, telecommunications, and the Internet, has dramatically changed how people conduct business, govern, entertain themselves, and communicate. Documents that would have once been written on paper and delivered in person or kept secure are now routinely created, sent, and stored electronically.

However, this increased speed and ease of communication have also raised privacy concerns. In today's electronic age, it is much easier for unauthorized individuals to intercept and manipulate messages compared to the era when face-to-face interactions were more common.

Advanced Encryption: Safeguarding Data

A notorious incident on German TV illustrated the vulnerability of computer data. During web browsing, a user's computer was scanned, revealing an installed banking program. Malicious operators remotely altered a file, directing the user's bank to send a payment to their account during the next online banking session.

This vulnerability extends to all connected computers. Data can be accessed and modified by unauthorized users without proper precautions. Even supposedly deleted data can be retrieved. Courts now often subpoena magnetic media as evidence, and forensic experts can reconstruct erased data. Encryption is the best defense.

Encryption transforms a document into an unreadable format for unauthorized users. The original document, or plaintext, is scrambled using an algorithm and a key. The key, a random string of numbers, determines the level of security, with longer keys providing stronger encryption.

Symmetric Encryption Algorithms

Symmetric encryption uses the same key for both encryption and decryption. Here are some popular algorithms:

1. **Data Encryption Standard (DES)**: Developed in the 1970s, DES is still used globally, although it has been largely replaced by AES.
2. **Triple DES**: This involves encrypting the output of DES with a different key for added security. However, most implementations use only two keys.
3. **International Data Encryption Algorithm (IDEA)**: Uses a 128-bit key and is considered secure for most attacks. It's used in PGP and Speak Freely.
4. **Blowfish**: A 64-bit block cipher with key lengths from 32 to 448 bits. Developed by Bruce Schneier, it's used in many products and is highly regarded.
5. **Twofish**: Also developed by Schneier, Twofish is considered very strong and is being extensively reviewed for security.
6. **RC4**: A stream cipher designed by Ronald Rivest, RC4's security is not well understood. It adds the output of a pseudorandom number generator to the plaintext bit by bit.

Public Key Encryption

Public key encryption, introduced by Martin Hellman and Whitfield Diffie in 1976, addresses many issues of symmetric encryption.In this scheme, Bob and Alice each create a pair of keys. A file encrypted with one key can only be decrypted with the other key of that pair.For instance, Bob can use Alice’s public key to encrypt a message, which only Alice can decrypt using her private key. The process works in reverse for messages from Alice to Bob.

Public-key encryption allows secure file exchange without needing a secure method to exchange keys, unlike symmetric encryption.Sender authentication verifies the sender's identity. For example, Bob can encrypt a message with his private key, and others can decrypt it using Bob’s public key to validate its origin.

Public-key encryption is essential for secure web transactions and email communication using S/MIME with a security certificate. One drawback is its higher computational demands compared to symmetric encryption. To reduce this, implementations often use symmetric encryption for the plaintext and then use public key encryption to encode the local key, sending both encrypted plaintext and key to the recipient.

Advanced Hacking

As networks expand and devices connect globally, the risk of system breaches increases. To safeguard your network, regular security audits and testing are crucial. Use hacking tools to simulate attacks and identify vulnerabilities. Run only necessary services and open required ports. Use a secure gateway to the Internet and ensure prompt application of updates and patches.

Tools of the Trade

Numerous online resources offer hacking tips and tools, making hacking more accessible. Hackers, including those with malicious intent, can easily find information to exploit vulnerabilities.

Future Threat: Advanced Malicious Code

Malicious code in software, while not new, poses increasing risks. Recent breaches, like the hack into Microsoft's source code, highlight the potential for popular software to be targeted.

Good and Bad Hackers

Hackers are not always malicious; some work to secure systems or notify vendors of vulnerabilities. While hacking can be destructive, building secure solutions is more challenging and rewarding. Despite efforts to curb hacking, it remains a persistent threat.

Idle Hands

Contrary to Hollywood portrayals, most hackers are smart but bored individuals, often starting young and stopping by their 30s. However, hacking is not limited by age, with individuals of various ages engaging in unauthorized activities.

Origins of Hacking:

Hacking didn't always mean breaking laws or messing up systems. Back in the 1960s, hackers at MIT were all about understanding computers deeply and pushing their limits. They followed a code: don't cause harm and leave no trace.

Changes Over Time: Hacking has evolved a lot in the last 43 years. Older hackers miss the old days when coding was an art and learning about systems was a challenge. They feel that today's hackers, especially the younger ones, focus more on flashy tricks than on understanding technology.

Bigger Dangers: While attention often goes to amateur hackers (script kiddies), experts worry more about the silent ones: criminal hackers and cyber terrorists.

White Hats: As hackers age, their interest in hacking often fades. Life gets busier, and their values change. Some stick to old tricks, some turn to real crime, but others use their skills for good, building software and making the internet safer.

Advanced Tracker Hackers

As computer crimes increase, the skills of computer forensics experts become more valuable. These experts investigate digital clues left on computers after hackers commit malicious acts.

Anonymity in Retrieving System Logs The 9-11 terrorist attacks led to legislation that allows federal agencies to intercept Internet traffic. The loss of the Web anonymity service hosted by ZeroKnowledge was another effect, though it was unrelated to the 9-11 activities. Web anonymizers let people visit websites without revealing their identities to website owners or local administrators who can log visited URLs.

Source Addresses A source address is an IP address in the header of an IP packet. If you spoof your source address, reply packets go to the address you've spoofed, and you won’t see the results.

Routing to the Rescue Surprisingly, the U.S. Navy has researched network anonymity, leading to the Freedom Network and possibly other anonymity systems. Proxying web requests through a third party that promises to keep its logs secret can provide some anonymity. Connecting via secure sockets layer (SSL) ensures that anyone sniffing the connection can only see that you’re visiting an anonymizer, not your final destination site, which is encrypted. However, this approach has limitations.

Onion Routing is a more advanced approach. Instead of using a single proxy, it uses a network of proxies. Each proxy relays and encrypts your packets. The first Onion Router chooses a route for your connection and encrypts your data

multiple times, each time using the public key for one of the routers in its network. Each layer of encryption resembles the skin of an onion, with the innermost layer encrypted by the key of the last router in its list. Your Onion Router must be a full participant in the network for Onion Routing to be effective.

Moving to Anomaly Tracking Traditional network-based Intrusion Detection Systems (IDS) detect malicious traffic by identifying known patterns, similar to how antivirus software works. They are effective at detecting known patterns.

Faster Systems Most IDSs can handle up to 400 Mbit/sec Ethernet, beyond which they become less efficient and start dropping packets. Vendors offering IDSs beyond 400 Mbits/sec are only looking at a subset of packets.

Moving to Appliances A trend in IDS products is the use of network-based IDS appliances. These appliances combine hardware and software into a preconfigured unit, eliminating the need to install and configure software on a PC.

Outsourcing Intrusion Detection Organizations concerned about unauthorized intrusions and DoS attacks can outsource their intrusion detection needs to Managed Security Service Providers (MSSPs). MSSPs monitor customers' IDSs via the Internet, which can be cost-effective.

Signs of Attempted and Successful Break-Ins Hackers are increasingly gaining root-privilege control of government computer systems, allowing them to perform actions like copying files or installing monitoring programs. Weak security measures in many agencies contribute to these successful attacks.

Forensics Threats to an enterprise's information infrastructure can come in various forms, including network intrusions and industrial espionage. Preserving the electronic crime scene and minimizing handling of disk drives are essential for good forensics.

Leave It to the Pros Data recovery remains a tedious and labor-intensive task, despite the efficiency of modern data-recovery tools.

Understanding Hacker Behavior Knowing how hackers think is only part of the battle. Understanding your network's vulnerabilities and taking necessary protective measures are also crucial.

Diagram Your Network Creating a network topology diagram helps identify vulnerable points in your network and plan security measures.

Always-On Means Always-Vulnerable Always-on Internet access with static IP addresses increases vulnerability. Commonly attacked ports include FTP (21), Telnet (23), SMTP (25), DNS (53), HTTP (80), POP3 (110), NNTP (119), IMAP (143), and SNMP (161).

Ways to Protect the Network Implementing firewall filtering, particularly stateful inspection firewalls, can protect against port attacks.

Seeing What the Hacker Sees Using tools like nmap can help you see your network from a hacker's perspective and identify vulnerabilities.

Software Vulnerabilities Hackers often exploit software security issues to gain access. Identifying and addressing these vulnerabilities is crucial.

Security Expert Web Sites Staying current with security updates and patches from vendors and following security experts' advice can help mitigate security risks.

The Problem at Present An IT worker recently faced federal criminal charges in Miami for allegedly downloading a virus into his employer’s computer system, causing a network crash for nearly two days. The U.S. Secret Service is handling twice as many cases involving insider attacks compared to 2004, and the FBI is investigating several such cases in New England alone.

Case Examples In the Miami case, Herbert Pierre-Louis, a hardware engineer at Purity Wholesale Grocers, is charged with computer sabotage for the incident in 1998. The damage exceeded the $6,000 threshold, making it a federal crime. In another case, a network consultant was charged with sabotaging the computer network at Steinberg Diagnostic Medical Imaging in Las Vegas by changing passwords.

Outlook and Response Atlanta-based Internet Security Systems Inc. (ISS) is concerned about "drive-by hackers" who can monitor traffic and hijack data over wireless networks. ISS has introduced WLAN security software and consulting practices to address this threat.

Summary Hackers target vulnerable systems indiscriminately, scanning hundreds of machines to find those they can exploit. They exploit known security holes and may use old, unused computers to gain access to networks. Security measures like firewalls are not always sufficient, as evidenced by attacks on major companies like Microsoft and eBay.

Conclusions

- Users must install security patches to prevent hackers from exploiting known vulnerabilities.
- Network security is compromised when old, unused computers remain connected to modems or networks.
- Encryption of important data, including remote backups, is essential to protect against attacks.
- Security measures must be regularly updated and monitored to ensure effectiveness.
- Intrusion detection systems (IDSs) play a crucial role in monitoring and detecting unauthorized access to networks.