Intrusion Detection and Response

Session 9

LEARNING OBJECTIVES

On completion of this session you should:

- Understand the impact of intrusion on corporate organization
- Be familiar with different types of intruders
- Understand the importance of early intrusion detection
- Describe common techniques used by the intruders
- Discuss different intrusion detection techniques
- Be familiar with the general guidelines for intrusion detection
- Discuss the strategies for response to intrusion
- Be familiar with the CERT recommendation for responding to intrusion

Contents

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 320-345. See Table 9.2 for the metrics used in intrusion detection.

Reading 2: For a review on Intrusion Detection Technology, read Section 2 of the online material Current State of Intrusion Detection Technologies at the CERT Coordination Centre at the Carnegie Mellon University.

Reading 3: For a comprehensive list of commercial intrusion detection products see CERIAS web site.

Reading 4: Read the online material "Intrusion Detection Checklist" at the CERT Coordination Centre at the Carnegie Mellon University

9.0 Introduction

It is not very uncommon to hear that the computer system of some big organization has been hacked. Many large companies like AT&T, universities, financial organizations have reported hacking. Even organization like CIA was no exception. More hackings actually take place than reported. Especially financial institutions tend not to report it because of loss of reputation and customer confidence. Intrusion, commonly known as hacking, is the unauthorized access or acquisition of higher than authorized access privileges into a computer system. Intrusion is one of biggest security threats to a network system. Early detection of intrusion and deployment of preventive measures are crucial for maintaining the security of the system. In this study guide, we will discuss how intrusion can be detected and preventive measures can be put in place.

9.1 Types of Intruder

J. Anderson has classified intruders in the following three categories [1]:

- Masquerader: an unauthorized user who penetrates a system's access control to exploit other's account; most likely an outsider.
- Misfeasor: a legitimate user but accesses data, programs or resources for which he/she is not authorized; generally an insider.
- Clandestine: an individual who seizes supervisory control and evades auditing and access control; may be an insider or outsider.

Study on intrusion at Bell Lab showed that the intruders attempt the followings:

1. copy the password file
2. run suspicious RPC calls
3. connect to nonexistent "bait" machine.

Another study shows that the levels of attacks are: a) high level attack by sophisticated hackers with a sound knowledge of technology, b) low level attack by a hacker who uses others' programs and spends countless hours looking for the weakest links.

9.2 Why is Early Intrusion Detection Necessary?

The best thing would be to prevent any kind of intrusion. Unfortunately, this can never be guaranteed. But early detection can save time, resources, money and reputation. The followings are important to consider:

1. If an intrusion is detected early enough, the intruder can be identified and excluded from the system before any damage is done. This may save the company from losing reputation and customer confidence.
2. A detection can determine which sensitive data, system, and network are attacked and what breaches (confidentiality, integrity or availability) have occurred. Appropriate response immediately after detection may mitigate the extent of damage and quickly bring the system back to current operational state.

3. A strong and efficient detection system can act as a deterrent for other hackers.

4. A detection enables the system administrators to collect information on intrusion techniques that can be used to review and reinforce the prevention policy.

9.3 Common Intrusion Techniques

Usually all systems store an encrypted form of the users' password and therefore, access to the password file is limited only to the system administrators. Surveys show that hackers usually use the following techniques to break passwords [1]:

1. Try default passwords of the standard accounts that come with the system (e.g., guest or everyone account in Windows NT).

2. Exhaustively try short passwords with combination of characters.

3. Try words in the systems online directory.

4. Collect information about the users and try to guess the password from that.

5. Try user's phone number, social security number, room number etc.

6. Try all legitimate license plate numbers of the state.

7. Use a Trojan horse to bypass restriction on access.

8. Tap the line between a remote user and the host system.

Although most the above techniques are based on guess, it can be highly effective when repeated attempts are made automatically and from a number of sources in a coordinated way. Trojan horse program opened by the system operator may run in a highly privileged mode and can be particularly dreadful. For example, it can copy the password file, delete the log files etc. A Trojan horse can be automatically invoked by a startup or exit routine. Recent survey shows that, over the years, the level of sophistication in attacking network systems has grown steadily.

9.4 Intrusion Detection Techniques

One important tool for intrusion detection is the audit record, e.g., log file. Some records of the ongoing activity by users are maintained in files and fed to an intrusion detection system for analysis. All network operating systems come with software that can do this, however, in this case data need further processing before applying to the detection system. Sophisticated software for collecting detection specific data is more useful. Such data may contain information like: initiator of an action, name of the action, receptor of the action, exception condition if occurred, resource usage, and time stamp. For example, a file 'copy' involves the execution of the user command, access validation, read from a file and write to another file. All these steps can be recorded in the audit file.

Normal users demonstrate a particular behavioural pattern that can be roughly estimated by statistical analysis. Intrusion detection techniques assume that the behaviour of an intruder differs from that of a typical user in a quantifiable way. It is relatively easy to distinguish a masquerader from a legitimate user while detecting a misfeasor is rather difficult. The following approaches to intrusion detection have been identified [1]:

Statistical anomaly detection: collects data related to legitimate users over a period of time to generate a behavioural pattern. Two methods are applied: threshold detection and profile based. The first method counts the number of occurrence of a specific event over an interval of time (e.g., log on number during a given time). If the counter value exceeds certain number, an intrusion is suspected.

In profile based method past behaviour of an individual or a group of similar users is created by considering a number of metrics. Useful metrics could be: a) counter - keeps track of occurrences of certain types of event (e.g., logon, command execution, password failure); b) gauge - measures the current value of some entity (e.g., number of logical connections of a user application); c) interval time - time gap between two related events; d) resource utilization. All these parameters are statistically analyzed to build a detection learning model. The learning model learns what is a normal behaviour and any deviation from that is treated as an intrusion.

Rule based detection: This scheme defines a set of rules to decide whether a behaviour is suspicious. There are two methods: anomaly detection and penetration identification. In the first method, historical audit records are analyzed to generate rules that describe the user behaviour pattern. Current behaviour is checked against these rules, any considerable violation signals intrusion. In the other method, rules are defined for identifying the known penetration or penetration weaknesses. Audit

records are generated and checked against the rules. If a match is found, then user's suspicion rating is increased. If this rating goes above a threshold, an anomaly is reported.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 320-345. See Table 9.2 for the metrics used in intrusion detection.

As a general guideline for intrusion detection the following steps are recommended by CERT [2]:

1. Monitor and inspect system resource usage
2. Monitor and Inspect network traffic and connections
3. Monitor and inspect user account and file access
4. Scan for viruses
5. Verify file and data integrity
6. Probe for system and network vulnerability
7. Reduce, scan, monitor, and inspect log files.

There are many commercial and public domain intrusion detection tools available. Some of the commercial products are: IDS (Cisco Systems), IPS (Captus Network), RealSecure (Internet Security Systems), CMDS (SAIC), ClearICE (Clarion Developer). Two public domain products are: Shadow and Network Flight Record jointly developed by the Naval Surface Warfare Centre, the National Security Agency, and the SANS Institute, USA.

Reading 2:
For a review on Intrusion Detection Technology, read Section 2 of the online material Current State of Intrusion Detection Technologies at the CERT Coordination Centre at the Carnegie Mellon University.

Reading 3:
For a comprehensive list of commercial intrusion detection products see CERIAS web site.

9.5 Response to Intrusions

Organizations should have a well prepared plan in place on how to respond when an intrusion is detected. The practices recommended by the CERT are the followings [2]:

Analyze all available information: capture and record system information, back up and isolate the compromised systems, examine logs, identify the attack used to gain access and what traces the intruder left behind.

Communication with relevant parties: Inform the other affected sites using a secure communication channel.

Collect and protect information: collect all relevant system and network logs from the compromised system, preserve evidence and contact law enforcement.

Contain the intrusion: temporarily shut down the system, disconnect the compromised system from the network, disable access, services and accounts, and monitor system and network activities.

Eliminate all means of intruder access: change passwords, reinstall compromised systems, restore executable programs from the original distribution, review system configurations, correct system and network vulnerabilities, and improve detection mechanism.

Return systems to normal operation: restore user data, re-establish availability of services and systems, and watch for signs of intruder's return.

Implement lesson learned: re-evaluate and upgrade security policy and revise security documents.

Reading 4:
Read the online material "Intrusion Detection Checklist" at the CERT Coordination Centre at the Carnegie Mellon University

9.6 Conclusion

In the Internet environment, it is practically impossible to prevent an intrusion. Therefore, an organization should have a well formulated intrusion detection and response strategy in place, and implement the best practices using the most sophisticated detection tools available. Another important issue is the user password. Users usually tend to pick easy-to-remember passwords. They need to be educated on how to select secure passwords. Different password selection strategies have been devised to assist users in selecting secure password.

9.7 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011.

[2] J.H. Allen, "The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001.