In network security, "intruders" are unauthorized individuals or entities who want to obtain access to a network or system to breach its security. Intruders can range from inexperienced hackers to professional and organized cyber criminals. In this article, we will discuss everything about intruders.

What are Intruders in Network Security?

Intruders are often referred to as hackers and are the most harmful factors contributing to security vulnerability. They have immense knowledge and an in-depth understanding of technology and security. Intruders breach the privacy of users and aim to steal the confidential information of the users. The stolen information is then sold to third parties, aiming to misuse it for personal or professional gains.

Types of Intruders

- **Masquerader:** The category of individuals that are not authorized to use the system but still exploit users' privacy and confidential information by possessing techniques that give them control over the system, such category of intruders is referred to as Masquerader. Masqueraders are outsiders and hence they don't have direct access to the system, they aim to attack unethically to steal data.
- **Misfeasor:** The category of individuals that are authorized to use the system, but misuse the granted access and privilege. These are individuals that take undue advantage of the permissions and access given to them, such category of intruders is referred to as Misfeasor. Misfeasors are insiders and they have direct access to the system, which they aim to attack unethically for stealing data/ information.
- **Clandestine User:** The category of individuals who have supervision/administrative control over the system and misuse the authoritative power given to them. The misconduct of power is often done by superlative authorities for financial gains, such a category of intruders is referred to as Clandestine Users. A Clandestine User can be any of the two, insiders or outsiders, and accordingly, they can have direct/ indirect access to the system, which they aim to attack unethically by stealing data/ information.

Keeping Intruders Away

- **Access Control**: Implement strong authentication mechanisms, such as two-factor authentication (2FA) or multi-factor authentication (MFA). Regularly review and update user access permissions to ensure they align with job roles and responsibilities.
- **Network Segmentation**: Divide your network into segments to limit lateral movement for intruders. For example, separate guest Wi-Fi from internal networks. Use firewalls and access control lists (ACLs) to restrict communication between segments.
- **Regular Patching**: Keep software, operating systems, and applications up to date. Patch known vulnerabilities promptly. Monitor security advisories and apply patches as soon as they are released.
- **Intrusion Detection and Prevention Systems (IDPS)**: Deploy **Intrusion Detection and Prevention Systems (IDPS)** solutions to detect and prevent suspicious activities. Set up alerts for any unauthorized access attempts.
- **Security Awareness Training**: Educate employees about phishing, social engineering, and safe online practices. Regularly conduct security awareness sessions.
- **Encryption**: Encrypt sensitive data in transit (using protocols like HTTPS) and at rest (using encryption algorithms). Use strong encryption keys and rotate them periodically.

Different Ways Adopted by Intruders

- Regressively try all short passwords that may open the system for them.
- Try unlocking the system with default passwords, which will open the system if the user has not made any change to the default password.
- Try unlocking the system by personal information of the user such as their name, family member names, address, and phone number in different combinations.
- Making use of a Trojan horse for getting access to the system of the user.
- Attacking the connection of the host and remote user and getting entry through their connection gateway.
- Trying all the applicable information, relevant to the user such as plate numbers, room numbers, and locality info.

How to Protect From Intruders?

- By being aware of all the security measures that help us to protect ourselves from Intruders.
- By increasing the security and strengthening the security of the system.
- In case of any attack, first, reach out to cyber security experts for a solution to this type of attack.

- Try to avoid becoming a survivor of cybercrime.

Conclusion

In Conclusion Intruder *i*s a unauthorized person or entity that tries to access the system without the permission. Understanding the different types of invaders and applying strong security measures like access controls, network segmentation, frequent patching, IDPS, security awareness training, and encryption may successfully protect systems and data from unauthorised access and cyber threats.

Who is treated as intruders on a network?

Intruders are attackers who attempt to breach the security of a network.

What is the difference between a hacker and an intruder?

An intruder is typically an unauthorised person attempting to obtain access, but a hacker is anyone who utilizes their abilities to investigate, modify, or upgrade technology systems, regardless of authority.

How can I protect against intruders?

- Access Control
- Network Segmentation
- Regular Patching
- Security Awareness Training
- Encryption