Packet Sniffers, Port Scanners, Phishers, and More:
The Top 5 Techniques of Today's Cybercriminal

Hundreds of times per day, hackers worldwide use the internet to probe IT infrastructures in search of vulnerabilities. Their objective is the exploitation and collection of sensitive data that can be used for profit, bragging rights, or both.

Understanding the techniques of a hacker can help you better prepare your defenses

1. Vulnerability and Port Scanners

While vulnerability and port scanners are used to decide where to attack, they do not breach anything on their own.

- **A vulnerability scanner** is a tool that can quickly assess computers on a network in an attempt to identify vulnerabilities.
- **Port scanners** check which ports on an individual computer are available to access. Both tools can be used by hackers to identify potential entry points.

Both scanners should be used regularly in a defensive cybersecurity program to identify vulnerabilities for intervention.

2. Packet Sniffers

Packet sniffers are pieces of hardware or software designed to monitor network traffic—between computers on a network, as well as between networked computers and the internet. Similar in concept to a "wiretap" on a phone line, packet sniffers can capture passwords and other data while in transit over a network.

3. Password Attack Techniques

Password attacks are processes used by hackers to discover passwords for a system or organization. Some common password attacks include:

- **Brute Force**. Attempting to crack or guess a password by trying as many possibilities as time and resources permit.
- **Dictionary or Library Attack**. Attempting to crack a password using an electronic dictionary list or listing of commonly used passwords.
- **Social Engineering**. Gaining the trust of someone and getting them to give access to their password. Methods may include phishing and telephone calls.
- **Malware**. Spyware that gets installed on a computer that monitors all keystrokes and reports back to the hacker.
- **Password Spray**. Attempting to gain access to a list of accounts/usernames by using a list of commonly used passwords.
- **Credential Stuffing**. Compromised username and password combinations are injected into various online accounts until a match is found. The account is then available for the hacker's use.
- **Pass the Hash**. An attack that allows the hacker to gain access to a user account using only the password hash. A password hash is the system-level conversion of a user password to a string of characters that cannot be directly reversed into the password. The technique does not involve decrypting the hash or the password but allows the user to convince the system that the hash it is passing belongs to the account they are attempting to access.

BLUE ORANGE® COMPLIANCE

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com

Packet Sniffers, Port Scanners, Phishers, and More:
The Top 5 Techniques of Today's Cybercriminal

4. Social Engineering

Social engineering is the manipulation of the natural human tendency to trust and avoid conflict, with the objective of gaining access to sensitive information. Using social engineering, a hacker may pose as a trustworthy contact to get the victim to do something outside of normal operations, such as disclose a password. The hacker will typically ask for just a little information at a time so that the encounter remains comfortable for the victim and a trust bond is developed.

These encounters can occur over the phone or online, with hackers often posing as a person of authority such as a network administrator, technical support representative, or an employee from a trusted vendor. Help desks can be particularly vulnerable to social engineering because those employees are trained to provide information and assistance. While some hackers use social engineering as their primary tactic, others may resort to it as an alternate strategy if the IT system of their intended victim is configured too securely.

Hackers often pose as a person of authority such as a network administrator, technical support representative, or an employee from a trusted vendor.

It is sometimes difficult to recognize real-life examples of social engineering attacks because the crime is not easily traced. The employee that was victimized may not realize he/she disclosed sensitive information to an untrustworthy source or may be unwilling to admit the disclosure, hence the incident goes unreported. Moreover, social engineering breaches often leave no physical evidence or an easily identifiable entry point, so if a breach does occur, the method may remain a mystery.

5. Phishing

Phishing, a form of social engineering, is an attempt to acquire sensitive information such as usernames, passwords, bank account information, credit card details, and social security numbers by masquerading as a trustworthy entity. As our society shifts to relying more on electronic communication, phishing attacks are becoming increasingly effective and widespread.

As companies shore up their security footprints, hackers are forced to be more creative to get in. They will often try to prey on unsuspecting or unknowing users who they hope are too busy to pay attention to the details. Phishing attacks are effective largely because they convince the recipient to bypass critical thinking. A prize needs to be claimed immediately or there is a problem with a user's account that must be dealt with. Phishing attacks push users into thinking emotionally and acting without thinking.

Cyberattacks are an ongoing and ever-evolving threat to healthcare providers. **The key is to be prepared**. Develop a system of protecting against cyberthreats, detecting them, responding to them, and recovering from them. With a solid system in place, a provider can prevent attacks and mitigate the effects of breaches should they occur.

To learn how BlueOrange Compliance can help you protect your organization and the people you serve, call 855.500.6272 or visit www.blueorangecompliance.com