

VoIP Penetration Testing: Product Overview



Introduction

The combination of voice and data has created a single network – unfortunately, this is also a new way for individuals to attempt to penetrate your computer systems. The integration of voice and data has led to new risks to security which must be addressed with equally new approaches to protecting data.

Called VoIP, the voice over internet protocol can be a new a management tool for business success or it can be an open window, which is easy for attackers to enter.

Overview

VoIP penetration testing is designed to find the “open window” into your system and close it. Rigorous testing is completed on the transmission technologies to determine where it is possible for the system to be breached. You are mistaken if you believe that the IP phones and related software have enough security controls in-built that they do not need any additional enhancements.

How can the VoIP system be compromised or how does it allow unethical and criminal intent be carried out?

There are many ways to breach VoIP security controls; eavesdropping for example is an old as the telephone itself. Inadequate security controls can lead to attackers accessing the server data through the transmission technology; individuals can effectively steal telephone calls; service interruptions and the use of sniffing tools.

Testing Process

VoIP penetration testing is a process whereby an attempt is made to purposely manipulate the VoIP system. All entry points into the WAN and/or LAN are tested and an attempt is made to gain access into the VoIP infrastructure. Sapphire will attempt to penetrate both the VoIP system and then use it to see how deep the attacker can penetrate into the computer system.

A VoIP test can be standalone or it can be one step in a larger security testing program. For example, password weaknesses can be tested for the component VoIP system or for the larger company-wide system. Naturally the broader the testing, the more secure the system will be after implementing recommended controls.



With penetration testing, ethical hackers will attempt an authorised penetration of the computer system. These include:

- Test ability to remotely access data network using VoIP technologies
- Look for vulnerabilities in system configuration enabling unauthorised access into system
- Test protection controls at each network layer
- Test remote IP phone locations
- Test ability to add IP address on the VoIP system through remote access
- Attempt to enter the main servers
- Look for ways for hackers to manipulate system at any point including Ethernet and cabling connections
- Look for vulnerability allowing sniffer software able to collect protocols
- Test traffic switching
- Determine if the ability exists to collect VoIP data
- Firewall testing between voice and data including potential for Tunnelling Attacks
- Wireless network security
- Testing of intrusion detection evasion capabilities

Why Test?

VoIP technology is relatively new and security controls have not kept up with the state-of-the-art technology. Any vulnerability in the voice and data network represents a point of vulnerability on the primary server. The only reason security for VoIP technology has not been a priority is because undesirables are only just beginning to turn their attention to this new way to access company data.

Testing modern infrastructures and applications is a complex process. Finding the open window can be difficult due to the complexity of today's systems and the ingenuity of hackers. It is amazing how often hackers are ahead of IT departments that have large budgets and highly qualified staff and are often able to breach million pound networks from their garages.

VoIP penetration testing includes testing technical aspects of the system, analysing employee security protocols, completing IT operational assessments, interpreting testing results and making recommendations for security improvements. It is about mitigating security risks to prevent data loss at any stage.