NETWORK ANALYSIS

Author: Arina Lachi

Technical University of Moldova

Abstract: *Packet sniffer's, are protocol analyzers meant to capture the packets that are seen by a machine's network interface. When a sniffer runs on a system, it grabs all the packets that come into and goes out of the Network Interface Card (NIC) of the machine on which the sniffer is installed. This means that, if the NIC is set to the promiscuous mode, then it will receive all the packets sent to the network if that network is connected by a hub. Fortunately, in a switched network, since switches do not broadcast the packets, sniffers cannot see any packet that is not having the destination address of the machine on which it is installed. A network analyzer can be a standalone hardware device with specialized software, or software that is installed on a desktop or laptop computer. Network analyzer is a tool, and like all tools, it can be used for both good and bad purposes.*

Keywords*: Network analyzer, sniffer, traffic, promiscuous mode, VPN, protect, intruder, method.*

Introduction

Network analysis (also known as traffic analysis, protocol analysis, sniffing, packet analysis, eavesdropping, and so on) is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. A network analyzer decodes the data packets of common protocols and displays the network traffic in readable format. A sniffer is a program that monitors data traveling over a network. Unauthorized sniffers are dangerous to network security because they are difficult to detect and can be inserted almost anywhere, which makes them a favorite weapon of hackers [1].

A network analyzer can be a standalone hardware device with specialized software, or software that is installed on a desktop or laptop computer. The differences between network analyzers depend on features such as the number of supported protocols it can decode, the user interface, and its graphing and statistical capabilities. Other differences include inference capabilities (e.g., expert analysis features) and the quality of packet decodes. Although several network analyzers decode the same protocols, some will work better than others for your environment.

A typical network analyzer displays captured traffic in three panes:

- **Summary** This pane displays a one-line summary of the capture. Fields include the date, time, source address, destination address, and the name and information about the highest-layer protocol.
- **Detail** This pane provides all of the details (in a tree-like structure) for each of the layers contained inside the captured packet.
- **Data** This pane displays the raw captured data in both hexadecimal and text format[5].

1. Network sniffer

System administrators, network engineers, security engineers, system operators, and programmers all use network analyzers, which are invaluable tools for diagnosing and troubleshooting network problems, system configuration issues, and application difficulties.

A network analyzer is used for[1,2]:

- Converting the binary data in packets to readable format
- Troubleshooting problems on the network
- Analyzing the performance of a network to discover bottlenecks
- Network intrusion detection
- Logging network traffic for forensics and evidence
- Analyzing the operations of applications
- Discovering faulty network cards
- Discovering the origin of virus outbreaks or Denial of Service (DoS) attacks
- Detecting spyware
- Network programming to debug in the development stage
- Detecting a compromised computer

- Validating compliance with company policy
- As an educational resource when learning about protocols
- Reverse-engineering protocols to write clients and supporting programs

When used by malicious individuals, sniffers can represent a significant threat to the security of a network. Network intruders use sniffing to capture confidential information, and the terms *sniffing* and *eavesdropping* are often associated with this practice. Intruders use sniffers on networks for[1,5]:

- Capturing cleartext usernames and passwords
- Discovering the usage patterns of the users on a network
- Compromising proprietary information
- Capturing and replaying Voice over IP (VoIP) telephone conversations
- Mapping the layout of a network
- Passive OS fingerprinting

2. Detecting Sniffers

As mentioned earlier, sniffers are a form of passive attack. They don't interact with any devices or transmit any information, thus making them very difficult to detect. Although tricky, detecting sniffers is possible. The easiest method is to check your network interfaces to see if they are in promiscuous mode.

Detecting promiscuous mode on Windows systems is difficult because there are no standard commands that list that type of information. However, there is a free tool called Promisc Detect (developed by Arne Vidstrom), which detects promiscuous mode network adapters for Windows NT, 2000, and XP. The following example shows the output of PromiscDetect: the D-link adapter is in normal operation mode, and the Intel adapter is running Wireshark:

```
C:\>promiscdetect
Adapter name:
- D-Link DWL-650 11Mbps WLAN Card
Active filter for the adapter:
- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a member of)
- Broadcast (capture broadcast packets)
Adapter name:
- Intel(R) PRO/100 SP Mobile Combo Adapter
Active filter for the adapter:
- Directed (capture packets directed to this computer)
- Multicast (capture multicast packets for groups the computer is a member of)
- Broadcast (capture broadcast packets)
- Promiscuous (capture all packets on the network)
WARNING: Since this adapter is in promiscuous mode there could be a sniffer running on this computer!
```

Since this adapter is in promiscuous mode there could be a sniffer running on this computer. Some sniffers cover their tracks by hiding PROMISC flags. Also, if a sniffer is installed on a compromised system using a rootkit, the intruder probably replaces commands such as **ifconfig**.

The following list describes several other methods that can be used to detect sniffers on the network[3]:

- **Monitor DNS Reverse Lookups** Some sniffers perform DNS queries to resolve IP addresses to host names. Performing a network ping scan or pinging your entire network address space can trigger this activity.
- **Send TCP/IP Packets with Fake MAC Addresses to All IP Addresses On the Same Ethernet Segment** Normally, the NIC drops packets with the wrong MAC address. However, when in promiscuous mode, some systems answer with a reset (RST) packet. This might also work in a switched environment, because switches forward broadcast packets that they don't have MAC addresses for. Many new sniffers have built-in defenses for this technique, altering the way they handle MAC addresses.
- **Carefully Monitor Hub Ports** Ideally, you have a network diagram and your cables are labeled. Then, if something unusual appears (e.g., a new device or a newly active hub port), it will recognize it. However, in reality, wiring closets and cabling can be a nightmare. If the hubs are being monitored with a protocol such as SNMP via a network management system, it important to be able to use the information to detect any unusual connects and disconnects.

- Use **ARP to Link IP Addresses to MAC Addresses** Normally, an ARP is sent out as a broadcast to everyone. However, it can also send out an ARP to a non-broadcast address, followed by a broadcast ping. No one should have your information in an ARP table except the sniffer that was listening to all of the traffic (including the non-broadcast traffic).Therefore the computer with the sniffer responds.
- **Use a Honeypot** A honeypot is a server that contains fake data and services to monitor the activity of intruders. In this case, an intruder can create fake administrator or user accounts on the honeypot, and then create connections across the network using cleartext protocols such as Telnet or FTP. If sniffers are monitoring for usernames and passwords, they will see the honeypot and the intruder will probably try to log into it. Honeypots run IDS to monitor activity, and special signatures can be added to trigger alerts when fake accounts are used.
- **Monitoring Host** This includes disk space, central processing unit (CPU) utilization, and response times. Sniffers gradually consume disk space as they log traffic, and can occasionally put a noticeable load on the CPU. As the infected computer's resources become more utilized, it begins to respond slower than normal [3,4].

3. Protecting Against Sniffers

Using switches is a network best practice that allows increased performance and security. While switches present a barrier to casual sniffing, the best method of protecting data is to use encryption, which is the best form of protection against traffic interception on public networks and internal networks. Intruders can still sniff the traffic, but the data appears unreadable. Only the intended recipient should be able to decrypt and read the data; however, some methods of encryption leave the packet headers in cleartext, thereby allowing intruders to see the source and destination addresses and map the network. However, the data contained within the packet is protected. Other forms of encryption also mask the header portion of the packet [4].

A VPN uses encryption and authentication to provide secure communication over an otherwise insecure network. VPNs protect the transmission of data over the Internet and over your internal network. However, if an intruder compromises either of the end nodes of a VPN, the protection is rendered useless. Different types of VPN families are not interchangeable, but they can be combined and used in multiples. The following list describes some of the VPN methods used today that protect data against sniffing [3]:

- **SSH** is an application-level VPN that runs over TCP to secure client-to-server transactions. This is often used for system logins and to administer servers remotely, and is typically used to replace Telnet, FTP, and the BSD commands. However, any arbitrary TCP protocol can be tunneled through an SSH connection and used for numerous other applications. SSH provides authentication using Rivest, Shamir, & Adleman (RSA) or Digital Signature Algorithm (DSA) asymmetric key pairs, and many encryption options for protecting data and passwords sent over the network. The headers in an SSH session are not encrypted, so an intruder can still view the source and destination addresses[5].
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)** SSL was originally developed by Netscape Communications to provide security and privacy to Internet sessions. It has been replaced by TLS, as stated in RFC 2246.TLS provides security at the transport layer and overcomes some security issues of SSL. It is used to encapsulate the network traffic of higher-level applications such as HTTP, Lightweight Directory Access Protocol (LDAP), FTP, SMTP, POP3, and IMAP. It provides authentication and integrity via digital certificates and digital signatures and the source and destination IP headers in a SSL session are not encrypted.
- **IP Security (IPSec)** is a network-level protocol that incorporates security into the IPv4 and IPv6 protocols directly at the packet level, by extending the IP packet header. This allows the ability to encrypt any higher-layer protocol. It has been incorporated into routing devices, firewalls, and clients for securing trusted networks to one another. IPSec provides several means for authentication and encryption, supporting a lot of public key authentication ciphers and symmetric key encryption ciphers. It can operate in *tunnel* mode to provide a new IP header that masks the original source and destination addresses in addition to the data being transmitted. Since IPSec uses protocols other than TCP and UDP, getting the IPSec traffic through a firewall or NAT device can be challenging.
- **Open VPN** is a tunneling SSL VPN protocol, which can encrypt both the contents of a packet and its IP headers. Open VPN uses a single TCP or UDP port; therefore, it can be easier to use in environments with challenging NAT and firewall architectures. Additionally, it can act as a virtual network bridge (a layer 2 VPN).

- **One-time passwords** (OTP) are another method to protect against sniffing. S/key, One-time Passwords In Everything (OPIE), and other one-time password techniques protect against the collection and reuse of passwords. They operate using a challenge-response method, and a different password is transmitted each time authentication is needed. The passwords that a sniffer collects are eventually useless since they are only used once. Smart cards are a popular method of implementing one-time passwords. However, OTP technologies cannot help protect your password after you enter it. E-mail protection is a hot topic for companies and individuals. Two methods of protecting e-mail (i.e., encrypting it in-transit and in storage) are Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME). Each of these methods also provides authentication and integrity using digital certificates and digital signatures [2].

Conclusion

Network analysis is the key to maintaining an optimized network and detecting security issues. Proactive management can help find issues before they turn into serious problems and cause network downtime or compromise confidential data. In addition to identifying attacks and suspicious activity, network analyzer can be used to identify security vulnerabilities and weaknesses and enforce company's security policy. Sniffer logs can be correlated with IDSes, firewalls, and router logs to provide evidence for forensics and incident handling.

A network analyzer allow it to capture data from the network (packet-by-packet), decode the information, and view it in an easy-to-understand format. Network analyzers are easy to find, often free, and easy to use; they are a key part of any administrator's toolbox.

A good networking and protocol reference should be on every administrator's bookshelf. It will come in handy when it discover some unknown or unusual traffic on its network.

As an administrator, it should know how to detect the use of sniffers by intruders. It should keep up-to-date on the methods that intruders use to get around security measures that are meant to protect against sniffing. As always, it also need to make sure that your computer systems are up-to-date with patches and security fixes to protect against rootkits and other backdoors.

It is important to remain up-to-date on the latest security technologies, encryption algorithms, and authentication processes. Intruders are constantly finding ways to defeat current security practices, thus more powerful methods are developed (e.g., cracking the Data Encryption Standard [DES] encryption scheme and its subsequent replacement with Triple Data Encryption Standard (3DES), followed by the Advanced Encryption Standard (AES).

Bibliography

1. Robert Shimonsky, *Sniffer Pro Network Optimization & Troubleshooting Handbook,* Syngress , 2002 г.
2. W. Richard Stevens, *TCP/IP Illustrated, Vol. 1: The Protocols (Addison-Wesley Professional Computing Series),* Addison-Wesley Professional; US edition ,1994.
3. Ануй Шах , *Сетевой трафик,* Университет штата Калифорния, Сакраменто,2011.
4. Daniel J. Nassar, *Network Performance Baselining*, Editura SAMS Publishing , 2000.
5. www.securityfocus.org/tools/category/4.