Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Sniffers

Reference:

Drew Hamilton Lecture Notes

Ethical Hacker Exam Guide, 9th ed.

Ervin, Kelly and Lee, William

Understanding Sniffers

- Used to capture and scan traffic moving on the network
- Can be an active or passive measure
- Can give an in depth view of a network
- Protocols easy for sniffing because of clear text:
  - Telnet/rlogin
  - HTTP
  - Simple Mail Transfer Protocol
  - Network News Transfer Protocol
  - Post Office Protocol
  - File Transfer Protocol
  - Internet Message Access Protocol

Using a Sniffer

- Tools for sniffing
  - Wireshark
    - Wireshark Command Line Tools
      - Tshark
      - Dumpcap
      - Capinfos
      - Editcap
      - Mergecap
      - text2cap
  - Tcpdump
  - WinDump
  - OmniPeek
  - Dsniff

Reading Sniffer Output

- Be able to understand the sections of a packet
- Identify the three-way handshake
- Understand packet-analysis
- Know hexadecimal numbers
  - IP address
  - Determine the first octet at least for help in eliminating choices on the exam

Switched Network Sniffing

- MAC Flooding
  - CAM table overflow
- ARP Poisoning
  - Contaminates with improper gateway mappings
- MAC Spoofing
  - Attacker changes their MAC address to the address of an authenticated user
- Port Mirror or SPAN Port
  - Switched port analyzer
  - Difficult for an attacker to pull off because they need physical access

On the Defensive

- Mitigating Attacks
  - Use a hardware switched network for isolating traffic
  - Implement IP DHCP snooping on switches to prevent ARP poisoning and spoofing attacks
  - Prevent promiscuous mode
  - Encrypt sensitive traffic with Ipsec
  - Virtual Private Networks
- Mitigating MAC Flooding
  - Cisco IOS Mitigation
  - Juniper Mitigation
  - NETGEAR Mitigation

- Detecting Sniffing Attacks
  - Look for promiscuous mode, shouldn't be enabled
  - Run an NIDS

Conclusion

- Know the purpose of sniffing
  - Gather info that flows across the network
- Understand your targets
  - Know what type of info you are looking for
- Know what makes sniffing possible
  - Traffic is being sent in the clear (unencrypted)
- Know your defenses
  - IPSec, SSL, SSH, VPNs