Wireless Attacks

MODULE 13

Contents

13.1 Learning Objectives 3

13.2 Introduction 3

13.3 Wireless Fidelty (Wi-Fi)(802.11) 3

13.3.1 Capturing 802.11 frames 4

13.4 Wireless Security 7

13.4.1 Attacks 8

13.5 Wireless Attacks Detection Techniques 10

13.5.1 Wireless Access Point Monitoring 10

13.5.2 Wireless Client/Node Monitoring 10

13.5.3 General Wireless Traffic Monitoring 11

13.6 Wireless Intrusion Detection Systems 11

13.6.1 Snort-wireless 11

13.6.2 WIDZ 12

13.6.3 Bro 12

13.7 Summary 12

13.8 Check Your Progress 13

13.9 Answers to Check Your Progress 13

13.10 Further Reading 14

References, Article Source & Contributors 14

Wireless Attacks

13.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define wireless networking.
- Capture frames for forensic analysis.
- Corelate various attacks in wireless networking to the forensics.
- Perform wireless intrusion detection techniques using available tools.

13.2 INTRODUCTION

Wireless forensics is a sub-discipline of network forensics. The main goal of wireless forensics is to provide the methodology and tools required to collect and analyse (wireless) network traffic that can be presented as valid digital evidence in a court of law. The evidence collected can correspond to plain data or, with the broad usage of Voice-over-IP (VoIP) technologies, especially over wireless, can include voice conversations. Analysis of wireless network traffic is similar to that on wired networks; however, there may be the added consideration of wireless security measures. Wireless networks have entered in a paramount way in the day-to-day life of people as well as enterprises. The wireless has added convenience of mobility and thus introduced risks on the traditional networks.

We will first look into wireless technologies (mainly 802.11) through the wireless frame layer (OSI Layer) and understand how they can be captured, extracted and analysed. After that we will learn various wireless attacks and the intrusion detection systems in wireless layers.

13.3 WIRELESS FIDELTY (WI-FI)(802.11)

The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.[1] However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance. Many devices can use Wi-Fi, e.g. personal computers, video-game consoles, smartphones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network access point. Such an access point (or hotspot) has a range of about 20 meters (66 feet) indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.

Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses, such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. A service set is the set of all the devices associated with a particular Wi-Fi network. The service set can be local, independent, extended or mesh. Each service set has an associated identifier, the Service Set Identifier (SSID), which consists of 32 bytes that identifies the particular network. The SSID is configured within the devices that are considered part of the network, and it is transmitted in the packets. Receivers ignore wireless packets from other networks with a different SSID.

The 802.11 logical architecture consists of several components (see *Figure 1*): station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS). STAs and Aps are hardware devices. The wireless STA has an adapter card, PC Card, or an embedded device to facilitate wireless connectivity. The wireless AP provides access to wireless STAs by becoming a bridge between STAs and the existing network backbone for network access.

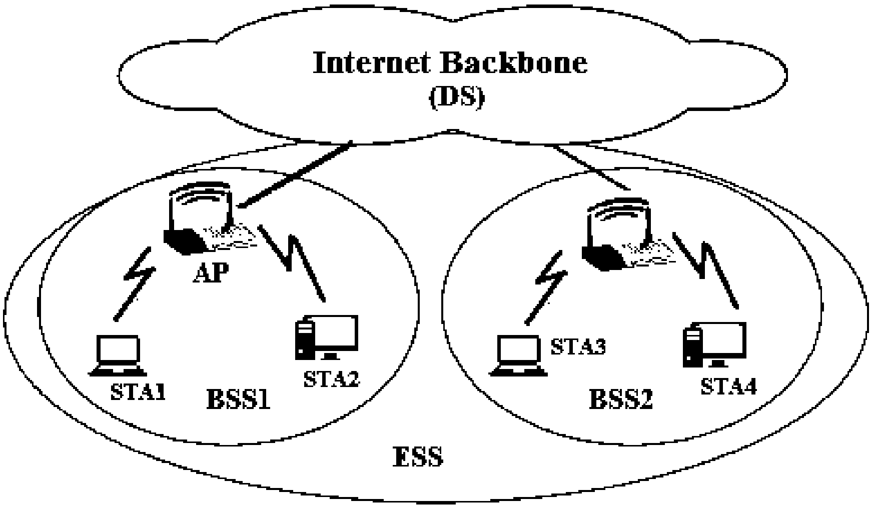


Figure 1: 802.11 components.

13.3.1 Capturing 802.11 frames

Air being the media, data packets is open for anyone to be sniffed. The sniffer setup must be equipped with appropriate hardware and software. Various ways of sniffing into wireless frames are using capabilities of monitor mode, using software like kismet and packet analysers etc.

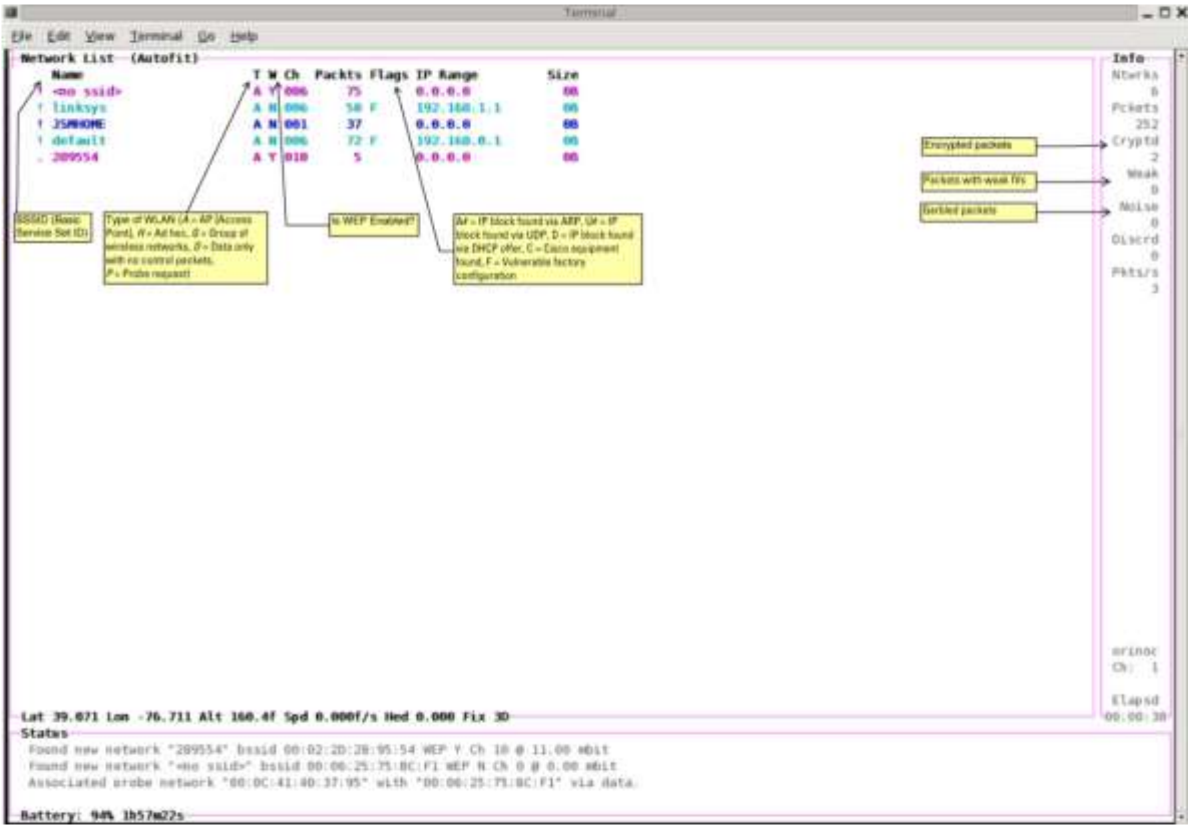
Monitor mode

Monitor mode, or RFMON (Radio Frequency MONitor) mode, allows a computer with a wireless network interface controller (WNIC) to monitor all traffic received from the wireless network. Unlike promiscuous mode, which is also used for packet sniffing, monitor mode allows packets to be captured without having to associate with an access point ad hoc network first. Monitor mode only applies to wireless networks, while promiscuous mode can be used on both wired and wireless networks. Monitor mode is one of the seven modes that 802.11 wireless cards can operate in: Master (acting as an access point), Managed (client, also known as station), Ad hoc, Mesh, Repeater, Promiscuous, and Monitor mode.

Software such as KisMAC or Kismet, in combination with packet analysers that can read pcap files, provide a user interface for passive wireless network monitoring. In many cases, monitor mode support is not properly implemented by the vendor. Linux's interfaces for 802.11 drivers support monitor mode and many drivers offer that support. FreeBSD, NetBSD, OpenBSD, and DragonFly BSD also provide an interface for 802.11 drivers that supports monitor mode and many drivers for those operating systems support monitor mode as well.

Kismet

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also run on Microsoft Windows, although, aside from external drones (see *Figure 2*), there's only one supported wireless hardware available as packet source. Distributed under the GNU General Public License, Kismet is free software.



Terminal
File
Edit
View
Terminal
Go
Help
SSSID (Basic Service Set ID)
Type of WLAN (A = AP (Access Point), H = Ad hoc, G = Group of wireless networks, D = Data only with no control packets, P = Probe request)
Is WEP Enabled?
A4 = IP block found via ARP, U4 = IP block found via UDP, D = IP block found via DHCP offer, C = Cisco equipment found, F = Vulnerable factory configuration
Encrypted packets
Packets with weak IVs
Garbled packets

```
Network List  (Autofit)
     Name                     T W Ch  Packts Flags IP Range        Size
   ! <no ssid>                A Y 006    75        0.0.0.0           0B
   ! linksys                  A N 006    58 F      192.168.1.1       0B
   ! 3SMHOME                  A N 001    37        0.0.0.0           0B
   ! default                  A N 006    72 F      192.168.0.1       0B
   . 289554                   A Y 010     5        0.0.0.0           0B

Info
Ntwrks
     6
Pckets
   252
Cryptd
     2
  Weak
     0
 Noise
     0
Discrd
     0
Pkts/s
     3

orinoc
Ch:  1
Elapsd
00:00:38

Lat 39.071 Lon -76.711 Alt 160.4f Spd 0.000f/s Hed 0.000 Fix 3D
Status
 Found new network "289554" bssid 00:02:2D:28:95:54 WEP Y Ch 10 @ 11.00 mbit
 Found new network "<no ssid>" bssid 00:06:25:75:BC:F1 WEP N Ch 0 @ 0.00 mbit
 Associated probe network "00:0C:41:40:37:95" with "00:06:25:75:BC:F1" via data.

Battery: 94% 1h57m22s
```

Figure 2: An explanation of the headings displayed in Kismet.

Kismet in tandem with wireshark can be used to capture and analyse wireless packets. Major attributes that need to be located and further analysed are: wireless packets, basic system ID, Frame Sequence number, WEP etc. Packets captured by Kismet can be saved into pcap files, which are then analysed by some analyser tools by opening those files in an offline mode.

NetStumbler

NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP. A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system. No updated version has been developed since 2005.

The program is commonly used for:

i. Wardriving: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).
ii. Verifying network configurations
iii. Finding locations with poor coverage in a WLAN
iv. Detecting causes of wireless interference
v. Detecting unauthorized ("rogue") access points
vi. Aiming directional antennas for long-haul WLAN links. (A directional antenna or beam antenna is an antenna which radiates or receives greater power in specific directions allowing for increased performance and reduced interference from unwanted sources.)

Pcap

In the field of computer network administration, pcap (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement pcap in the libpcap library; Windows uses a port of libpcap known asWinPcap.

Monitoring software may use libpcap and/or WinPcap to capture packets travelling over a network and, in newer versions, to transmit packets on a network at the link layer, as well as to get a list of network interfaces for possible use with libpcap or WinPcap.

Airodump and aircrack

Airodump-ng is a Packet sniffer, it Places air traffic into PCAP or IVS files and shows information about networks. Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and Windows.

VIDEO LECTURE

WEPWedgie

WEPWedgie is a open source toolkit for determining 802.11 WEP keystreams and injecting traffic with known keystreams. The toolkit also includes logic for firewall rule mapping, pingscanning, and portscanning via the injection channel and a cellular modem

13.4 WIRELESS SECURITY

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Short for Wired Equivalent Privacy (or Wireless Encryption Protocol), WEP is part of the IEEE 802.11 wireless networking standard and was designed to provide the same level of security as that of a wired LAN. Because wireless networks broadcast messages using radio, they are susceptible to eavesdropping. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. WEP was the encryption scheme considered to be the initial standard for first generation wireless networking devices. However, it has been found that WEP is not as secure as once believed.

13.4.1 Attacks

Wireless systems encounter attacks which are in some cases similar to network attacks. However, the attacks which are typically specific to wireless systems are:

a) Probing and surveillance.
b) Denial of Service.
c) Impersonation or MAC Spoofing.
d) Man in the middle.

Probing and surveillance

Probing or sniffing can be of two types:

a) Active
b) Passive

Attackers can indulge in active probing where they send probe requests and continuously wait for a probe response. The response will contain SSID information and many other information from nodes or access points in the range. Certain access points are cloaked, i.e. they are configured not to respond with a probe request. In such cases the attacker might not get any active response hence will not be able to probe or sniff into these access points.

In passive probing the attacker keeps on listening on all available (or listenable) channels for all the packets that are sent or received. While doing this the attacker doesn’t have to send a single packet into the transmission channel. But, cloaked Access Points with no wireless activities during the period of the probe would not be detected. Because there is no probes the cloaked Access Points will not send any packets into the channel, thus, the attacker will never be able to sniff into those Access Points.

NetStumbler is a good example of a tool that can help in active probing is. Kismet is a software tool that facilitates passive probing. The Data gathered during probing can be saved into pcap format (see previous section) for future analysis while in offline mode. On a non-encrypted stream in the network, the attacker could immediately find or probe into a traffic stream and can easily acquire vital information MAC address, IP address range, and gateway etc from the traffic.

In case of encrypted streams like Wireless Encryption Protocol (WEP), then WEP crackers which are available with the attacker can be used. For example, airodump can be used to gather all the encrypted packets transmitted and aircrack (see previous section) is then used to try to crack the WEP key. If there is no sufficient traffic on the network, certain tools for packet injection like WEPWedgie (see previous section) can be used to insert random traffic into the WEP encrypted network. This will fetch responses from the network; these response packets can be collected and given for WEP key cracking.

Denial of Service

DoS type attacks at every wireless layers can be easily carried out in a wireless network. Noise I the channel can be induced by emitting a very strong Radio Frequency interference on the channel in which the wireless network is operating on this will cause interference to all wireless networks that are operating on that channel or nearby channels. Certain DoS attacks can utilize packet injection, the attackers will flood the network connected clients with lots of disassociate or authentication packets.

Impersonation(spoofing)

Another attack is called as impersonation, where the attackers change their MAC address in the transmission packets with an address that he had found while probing. This is typically used by criminals to send derogatory mails like intimidation etc. A MAC address might belong to an authorized client in the network. This is usually done to defeat the MAC filtering capabilities of access points where only a list of authorized MAC addresses are allowed to use the wireless network. As earlier described, even if the wireless network is WEP encrypted, the MAC address of the sending and receiving party is still viewable by a wireless sniffing tool. MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. However, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy. MAC address can be changed in linux using ifconfig command. In windows we can do this using registry.

Man in the middle

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the hacker’s soft AP (disconnects the user from the modem so they have to connect again using their password which one can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

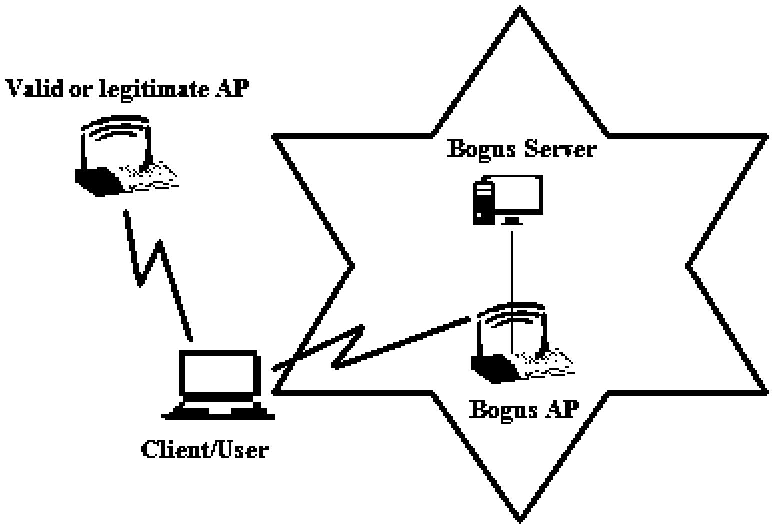


Figure 3: A typical man in middle in wireless systems

13.5 WIRELESS ATTACKS DETECTION TECHNIQUES

Now that we have a good idea of various attacks in a wireless system, we should now look into certain ways that can be employed to detect certain attacks. These detection techniques can be categorized in following three basic forms:

a. Wireless Access point monitoring
b. Wireless client/node monitoring
c. Wireless traffic monitoring

13.5.1 Wireless Access Point Monitoring

In this the wireless network keeps a list of authorized access points and hardware using the net with information like respective SSID, MAC address and other channel information recorded earlier. The monitoring agent/component would continuously listen to wireless frames like beacons, frame probes; responses and authentications etc. sent out by every Access Points and compare these with the previously recorded information. The monitoring device must listen to every possible channel and record all packets for this technique to be effective. To detect Man-in-the-middle attack, such a monitoring component needs to detect that whether there is a sudden introduction of an AP on another channel previously not present. Though the SSID, MAC address might be spoofed (see previous section) by the attacker in the process of setting up the rouge AP, the channel information in which the genuine AP was operating from has been changed which provides an alert on a possible MitM attack.

13.5.2 Wireless Client/Node Monitoring

The access point monitoring is much simpler, in the wireless client monitoring a list of allowed clients' needs to be maintained. This adds up to lot of administrative overheads, however, some of the clients' aspects can be recorded and monitored. Like, list of blacklisted clients can be maintained and any movements from these nodes can generate alerts for analysis. Also, all wireless clients with an unauthorized MAC address (MAC address ranges which have not been allocated out yet) are automatically denied access and an alert send off. Also, clients sending probes with typical nicknames can also be recorded and alert generated. One more area where monitoring might be applied is WEP (encrypted) traffic is being used to send/receive, no station should be reusing the same WEP Initialization Vector (used to generate keys) over and over again within a very short period of time (WepWedgie and other cracking tools use this).

For wireless clients that are legitimate, there is a sequence number field within the IEEE 802.11 header which can be tracked for abrupt changes. Certain times when impersonation attacks are being carried out, the attacker will be able to read the MAC / IP address of the victim, but it will not be able to continue with the sequence number used previously by the victim, thus by monitoring the sequence number in these client generated packets impersonation attacks can be easily detected.

13.5.3 General Wireless Traffic Monitoring

To detect DoS attacks, Wireless traffic can be monitored for attempts to flood the network using deauthentication, de-association, authentication, association, erroneous authentication. Frequency and Signal-To-Noise Ratio monitoring could help signal an oncoming RF based DOS attack on your wireless network. Failures in authentication as well as association can also be monitored and reported.

13.6 WIRELESS INTRUSION DETECTION SYSTEMS

Let us look at few examples of open-source wireless Intrusion Detection Systems that are available for usage.

13.6.1 Snort-wireless

Snort's open-source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyse it against a rule set defined by the user. The program will then perform a specific action based on what has been identified. Snort-wireless is a wireless intrusion detection system adapted from the snort IDS engine. One can write snort-wireless rules for detecting wireless traffic like one would detect for IP layer attacks.

13.6.2 WIDZ

WIDZ version 1 is a proof-of-concept IDS system for 802.11 that guards an AP(s) and Monitors local frequencies for potentially malevolent activity. It detects scans, association floods, and bogus/Rogue AP's. It can easily be integrated with SNORT or RealSecure.

13.6.3 Bro

Originally written by Vern Paxson, Bro is an open source Unix based network monitoring framework. Often compared to a Network Intrusion Detection Systems(NIDS), Bro can be used to build a NIDS but is much more. Bro can also be used for collecting network measurements, conducting forensic investigations, traffic baselining and more. Bro has been compared to tcpdump, Snort, netflow, and Perl (or any other scripting language) all in one. It is released under the BSD license.

Bro can be conceptualized in two layers

Bro Event Engine; which analyses live or recorded network traffic or trace files to generate neutral events.

Bro uses an engine (written in C++) to generate events when "something" happens. This can be triggered by the Bro process, such as just after initialization or just before termination of the Bro process, as well as by something taking place on the network (or trace file) being analysed, such as Bro witnessing an HTTP request or a new TCP connection. Bro uses common ports and dynamic protocol detection (involving signatures as well as behavioural analysis) to make a best guess at interpreting network protocols. Events are policy neutral in that they are not good or bad but simply signals to script land that something happened.

Bro Policy Scripts; which analyse events to create action policies.

Events are handled from within Bro policy scripts (written in the Turing complete Bro scripting language). By default Bro simply logs information about events to files (Bro also supports logging events in binary output), however it can be configured to take other actions such as sending an email, raising an alert, executing a system command, updating an internal metric and even calling another Bro script. The default behaviour produces net flow-like output (conn log) as well as application event information. Bro scripts are able to read in data from external files, such as blacklists, for use within Bro policy scripts.

13.7 SUMMARY

1. Wireless networks have entered in a paramount way in the day to day life of people as well as enterprises. The wireless have added convenience of mobility and thus introduced risks on the traditional networks.
2. The IEEE 802.11 protocol and associated technologies are the basis of present day wireless networking.
3. Various ways of sniffing into wireless frames are by using capabilities of monitor mode.

4. WEP is an old IEEE 802.11 standard from 1999, which was outdated in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2.
5. Attacks which are typically specific to wireless systems are Probing and surveillance, Denial of Service, Impersonation or MAC Spoofing, Man in the middle.
6. Wireless attack detection techniques can be categorized in following three basic forms; Wireless Access point monitoring, Wireless client/node monitoring, Wireless traffic monitoring.
7. Few examples of open source wireless Intrusion Detection Systems that are available for usage are Snort-wireless, WIDZ, RealSecure.

13.8 CHECK YOUR PROGRESS

1. Fill in the blanks.

a) Main components in the 802.11 are ___________________________________.
b) Various ways of sniffing into wireless frames are using capabilities of ______________.
c) ___________ is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).
d) WEP stands for ________________.
e) WPA stands for __________________.
f) Examples of wireless intrusion detection systems are: _________________________.
g) Two ways of DoS attack in wireless systems are __________________, _________________.

2. State True or False

a) Monitor mode is one way of capturing packets and applies to both wired and wireless networks.
b) pcap (packet capture) consists of an application programming interface (API) for capturing network traffic.
c) WEP enabled node is highly secured.
d) WPA stands for Wireless Protection and authentication.
e) Active probing is where an attacker sends probe requests and continuously wait for a probe response from an access point.
f) Impersonation is to use captured MAC address while communicating.
g) Wireless Access Point Monitoring helps in detecting spoofing and man in the middle attacks.
h) In Wireless Client/Node Monitoring the administrator continuously sends probe packets to clients connected to an access point.

13.9 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks.

a) Station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS).
b) Monitor mode.
c) Wardriving.
d) Wired Equivalent Privacy.
e) Wi-Fi Protected Access.
f) Snort-wireless, WIDZ, RealSecure.
g) Inducing strong RF noise, continuously injecting lot of authentication packets.

2. State True or False.

a) (F)
b) (T)
c) (F)
d) (F)
e) (T)
f) (T)
g) (T)
h) (F)

13.10 FURTHER READING

a) Debra Littlejohn Shinder, Michael Cross, Scene of the Cybercrime, syngress
b) Computer Forensics: Investigating Wireless Networks and Devices By EC-Council
c) Mark Ciampa, CWSP Guide to Wireless Security
d) Linda Volonino, Reynaldo Anzaldua; Computer Forensics For Dummies, Wiley Publishing, Inc.
e) How 802.11 Wireless Works: Wireless - TechNet – Microsoft, https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx
f) Intrusion Detection Systems: An Overview of RealSecure, https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-overview-realsecure-342
g) Understanding Wireless Attacks and Detection – SANS, https://www.sans.org/.../understanding-wireless-attacks-detection-1633

References, Article Source & Contributors

[1] Aircrack-ng - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Aircrack-ng
[2] Kismet (software) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Kismet_(software)
[3] Monitor mode - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Monitor_mode
[4] NetStumbler - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/NetStumbler

[5] Network forensics - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Network_forensics

[6] pcap - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Pcap

[7] The Differences Between WEP and WPA - Webopedia.com, www.webopedia.com › Did You Know › Computer_Science

[8] WEPWedgie - Best Open Source, www.findbestopensource.com/product/wepwedgie

[9] widzv1-0.zip ≈ Packet Storm, https://packetstormsecurity.com/files/30700/widzv1-0.zip.html

[10] Wireless security - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Wireless_security

[11] Bro (software) - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Bro_(software)

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan, Bhubaneswar

This MOOC has been prepared with the support of

C·O·L

CEMCA