CS471
Security & Info Assurance

Welcome!
3/15/2023

CS471
Security & Info Assurance

Course Schedule

Week #	Monday	Wednesday	Reading	Weekly Topic	Due	Assigned
1	01/16/23	01/18/23		Getting started		
2	01/23/23	01/25/23	Chapter 1	Introduction		Assignment 1
3	01/30/23	02/01/23	Chapter 2	Symmetric Encryption	Assignment 1	Assignment 2
4	02/06/23	02/08/23	Chapter 3	Asymmetric Encryption	Assignment 2	Assignment 3
5	02/13/23	02/15/23	Chapter 4	Key Distribution and Authentication	Assignment 3	
6	02/20/23	02/22/23	Chapters 1-4	Review : **Midterm 1**		
7	02/27/23	03/01/23	Chapter 5	Network Access Control		Assignment 4
8	03/06/23	03/08/23	Chapter 6	Transport Level Security	Assignment 4	Assignment 5
9	03/13/23	03/15/23	Chapter 7	Wireless Network Security		
10	03/20/23	03/22/23	Chapter 8	DNS and Email Security	Assignment 5	
11	03/27/23	03/29/23		Spring Break		
12	04/03/23	04/05/23	Chapters 1-8	Review : **Midterm 2**		
13	04/10/23	04/12/23	Chapter 9	IP Security		Assignment 6
14	04/17/23	04/19/23	Chapter 10	Malicious Software	Assignment 6	Assignment 7
15	04/24/23	04/26/23	Chapter 11	IDS		
16	05/01/23	05/03/23	Chapter 12	Firewalls	Assignment 7	
17	05/08/23	05/10/23		Finals Week		
	*No Meeting			Final Exam: **TBD**		

CS471
Security & Info Assurance

The X.800 service categories will be important for the entire semester.

As we examine security, this will be our measure.

- **X.800 Service Categories**
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Non-repudiation

CS471
Security & Info Assurance

Technologies that provide security services:

Confidentiality
- Encryption
- TLS
- SSH

Authentication
- EAP
- EAPOL
- Encryption

Access Control
- Kerberos
- 802.1x
- Firewall

Integrity
- Hashing
- Digital Certificates

Non-Reputability
- Asymmetric Encryption
- Digital Certificates

CS471
Security & Info Assurance

Automatic Authentication and Confidentiality

How can we provide *automatic* authenticity and confidentiality services to applications?

Does this work over ‘any’ network?
– LAN, WAN, CAN

CS471
Security & Info Assurance

Wireless Networks

How is are wireless networks different than wired networks?

How is are wireless networks the same as wired networks?

Does WIFI present any additional security risks?

Can we *provide* security over WIFI?

CS471
Security & Info Assurance

Security Services

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Non-repudiation

What do we expect from ‘wireless network security’?

All of them!

How do we provide wireless network security?

802.11i

CS471
Security & Info Assurance

Wireless Network Mapping

How would we test wireless network security?

What information would we want to know about any wireless network?

What tools exist for this purpose?

CS471
Security & Info Assurance

Examine several Wireless tools from Kali Linux.

Wireless attacks (Active)

- Aircrack-ng
- Wifite
- Fern
- PixieWPS
- Bully

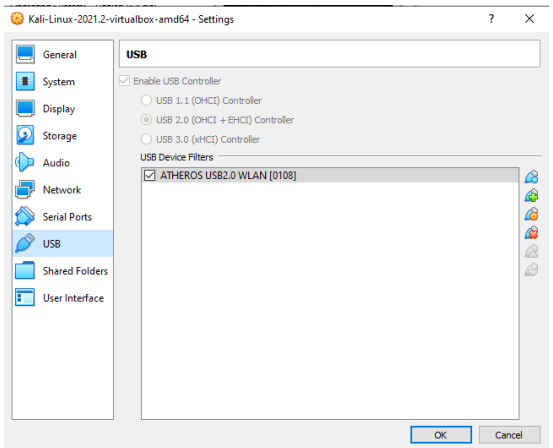
Sniffing and analysis (Passive)

- Wireshark
- Kismet

CS471
Security & Info Assurance

Using wireless tools in Kali requires a wireless device..

- Connect a USB WIFI device to your host system. (Additional Device)
- Set this USB device to pass through from the host to Kali.
  In VirtualBox> Settings> USB> Add> (Select the device)
- Reboot Kali
- Reconnect the USB device
- Kali Linux should now have a new wlan0 device.



Use these commands in Kali for troubleshooting: (as Root)

```
dmesg
ifconfig
iwconfig
```

CS471
Security & Info Assurance

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark is the continuation of a project started by Gerald Combs in 1998.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

Official Docs:
https://www.wireshark.org/docs/

CS471
Security & Info Assurance

Kismet - wireless sniffer and monitor

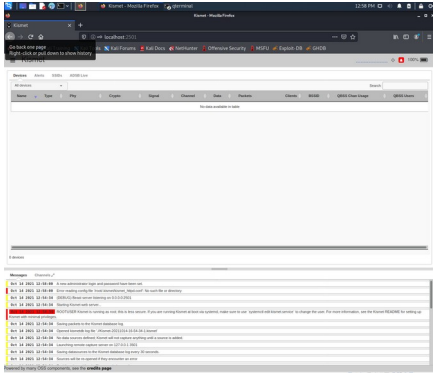
Kismet is a wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework.

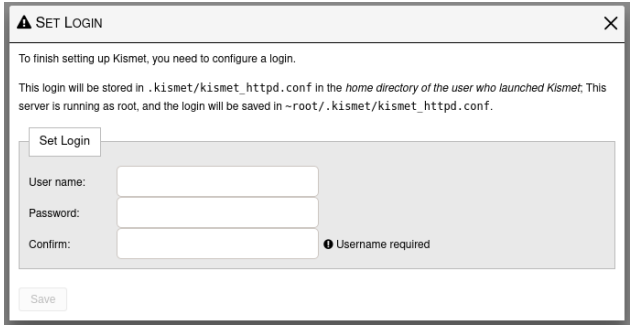
Kismet works with Wi-Fi interfaces, Bluetooth interfaces, some SDR (software defined radio) hardware like the RTLSDR, and other specialized capture hardware.

Kismet works on Linux, OSX, and, to a degree, Windows 10 under the WSL framework. On Linux it works with most Wi-Fi cards, Bluetooth interfaces, and other hardware devices. On OSX it works with the built-in Wi-Fi interfaces, and on Windows 10 it will work with remote captures.

TLDR; Quick Start Guides
https://www.kismetwireless.net/docs/readme/quickstart/
https://www.kismetwireless.net/docs/readme/starting_kismet/

Official Docs:
https://www.kismetwireless.net/docs/





CS471
Security & Info Assurance

Fern Wifi Cracker

Fern Wifi Cracker is a Wireless security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library. The program is able to crack and recover WEP/WPA/WPS keys and also run other network based attacks on wireless or ethernet based networks.

Official Docs:
https://github.com/savio-code/fern-wifi-cracker

CS471
Security & Info Assurance

pixiewps - Offline Wi-Fi Protected Setup bruteforce tool

pixiewps is a tool written in C used to bruteforce offline the WPS PIN method exploiting the low or non-existing entropy of some Access Points, the so-called "pixie-dust attack".

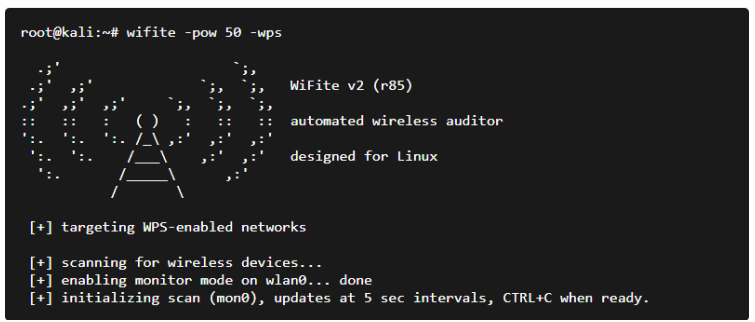
Official Docs:
https://github.com/wiire-a/pixiewps

CS471
Security & Info Assurance

wifite - Python script automates wireless auditing with aircrack-ng

Wifite is a tool to audit WEP or WPA encrypted wireless networks.
It uses aircrack-ng, pyrit, reaver, tshark tools to perform the audit.
This tool is customizable to be automated with only a few arguments and can be trusted to run without supervision.

Official Docs:
https://github.com/kimocoder/wifite2



CS471
Security & Info Assurance

Aircrack-ng: suite of tools to assess WiFi network security.

It focuses on different areas of WiFi security:

- Monitoring: Packet capture and export of data
- Attacking: Replay attacks, deauthentication, fake access points via packet injection
- Testing: Checking WiFi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2)

All tools are command line which allows for heavy scripting. A lot of GUIs have taken advantage of this feature. It works primarily on Linux but also Windows, macOS, FreeBSD, OpenBSD, NetBSD, as well as Solaris and even eComStation 2.

Useful Usage Examples:
https://www.kali.org/tools/aircrack-ng/

Official Docs:
https://www.aircrack-ng.org/

CS471
Security & Info Assurance

Bully

Bully is a new implementation of the WPS brute force attack, written in C. It is conceptually identical to other programs, in that it exploits the (now well known) design flaw in the WPS specification. It has several advantages over the original reaver code. These include fewer dependencies, improved memory and cpu performance, correct handling of endianness, and a more robust set of options.

Useful Usage Examples:
https://www.kali.org/tools/bully/

Official Docs:
https://github.com/kimocoder/bully

CS471
Security & Info Assurance

WIFI Cracking Tools

Do these tools serve any legitimate purpose?

It seems that several of these tools defeat encryption.
– How do these tools do this?

If possible, how could these tools be used to improve security?

CS471
Security & Info Assurance

Assignment 5

Demonstrate network mapping using Nmap, Zenmap, and Wireshark.

Describe how network mapping software affects security. How do network mapping tools, like NMAP, increase or decrease security? How could network mapping attempts be detected and/or stopped?

Due 3/20/23

Questions?

CS471
Security & Info Assurance

Next Week:

Chapter 8: DNS and Email Security

If you are not familiar with DNS, please read the chapter *before* lecture.

CS471
Security & Info Assurance

Thank you!