CNT 6519, Fall 2019 Assigned: 11/15/2019
S. Lang Assignment #6 (**incomplete**) Due: 12/2/2019 on UCF's WebCourses (by 9 pm, EST)

Objectives: To learn about wireless network penetration testing (pen-testing), with authorization, using open source hacking/pen-testing tools running on a Linux platform (e.g., Kali Linux), and forensic investigation.

Notes: First, this version of the assignment is incomplete, missing Question 2, Part 2. Also, there are two versions of Question 3. One requires access to equipment with Bluetooth; the other (Q3 alternative) does not need Bluetooth and deals with forensic investigation of an alleged hacking incident. Choose either version (but not both) for your work. Both have parts for extra-credit.

Notes:

(1) Equipment: You need to have administrative privilege, or be given consent to administrative privilege, to a computer/laptop (the pen-tester or attacker machine), a Wifi router (access point) running the WPA/WPA2-PSK security protocol, and another Windows machine as the target/victim machine, all connected in a wireless LAN environment.

(2) Tools: You need to run Linux on the pen-tester machine (such as Kali Linux). Specific tools of Kali Linux to be used include (but not limited to): Aircrack-ng suite, Metaspolit, nmap, etc. You may download Kali Linux and make a bootable USB drive to run Kali Linux on your computer/laptop (see instructions at https://docs.kali.org/downloading/kali-linux-live-usb-install for details). Alternatively, you may install Virtualbox on your computer/laptop (https://www.virtualbox.org/manual/ch01.html) and run Kali Linux as a virtual machine (https://www.blackmoreops.com/2014/04/08/detailed-guide-installing-kali-linux-on-virtualbox/). In the case of running Kali Linux as a virtual machine, since Kali Linux may not be able to see your host machine's wireless interface card, you will/may need to add a Wifi adapter USB dongle in order for the VM to have wireless connection (see https://www.youtube.com/watch?v=K1ETBeRQBs4 for details on purchasing a Kali Linux compatible Wifi USB adapter, setting up Wireless connection, in the VM). In sum, the pen-tester machine could be: an Intel-based machine booted into Kali Linux, Kali Linux running as a virtual machine on a host computer/laptop, or a Linux machine that have installed the necessary tools (aircrack-ng, metasploit, etc.) for the assignment. In all cases, your pen-tester/attacker machine needs to have wireless access while running Linux.

(3) As always, be sure to include adequate explanations and details in your answers to each of the questions (or, otherwise, points will be deducted if there is insufficient/inadequate amount of explanation/details in your submitted work).

1. (8 pts.) In this question the attacker/pen-tester machine attempts to capture WPA/WPA2 4-way handshake packets between an AP and a victim/target machine by first de-authenticating the victim from the AP, then conducting a brute-force dictionary attack of the packet capture file to crack the pre-shared key of the WLAN. The main tools used are part of the aircrack-ng suite (preinstalled in Kali Linux), using the examples described at https://www.aircrack-ng.org/doku.php?id=deauthentication#usage_examples and https://www.aircrack-ng.org/doku.php?id=cracking_wpa as a guide. You need to follow the below steps and describe your work/results (including screenshots) **using your words** in each of the steps:
Note: To balance documentations of your work and, at the same time, protecting your privacy, please **do not include** model/serial numbers in your answers or screenshots, and, for MAC addresses (6 bytes), report only the first 2 bytes and blank out (redact) the last 4 bytes (out of the 6 bytes); for SSIDs, blank out (redact) all leading characters except for the last character of the SSID.

(a) Describe briefly the equipment you use for this question, including: the pen-tester and target machines (e.g., a Dell laptop running Kali Linux VM in Virtualbox, and a Dell desktop PC, respectively) and the AP (e.g., an IEEE 802.11n Wireless router/DSL modem made by Zyxel). **Additionally, include a statement whether you have administrative privileges, or are given the consent, to conduct penetration testing using the equipment described here.**

(b) In Kali Linux, open a terminal and use the command "ifconfig –a" to make sure your pen-tester/attacker machine sees the wireless interface wlan0 is up. Produce a screenshot showing the wlan0 interface and the current time when you did this work (using the "date" command to show current date/time).

(c) Logon to your wireless router/access point and change its current password/phrase to something different but equally strong (with adequate length and combinations of characters). Report what you did (but do not report your AP's old password/phrase), when you made the change (e.g., 05:10 pm on 11/18/2018), and the new password/phrase. After completing Question 1, **be sure to restore** the AP's password/phrase to its original.

(d) After you changed the AP's password/phrase, reconnect your target/victim machine to the AP using the new password/phrase. **Do not reconnect** your pen-tester/attacker machine to the AP using the new password/phrase. In Kali Linux, open a terminal, run the below commands, respectively, to: put the pen-tester machine's wireless interface in monitor mode; and identify the AP and connected target/victim device. Report what you did, when you did this, and relevant screenshots (Be sure to blank out/redact) portions of the MAC addresses, SSIDs, etc., as noted above, in your screenshots):

airmon-ng start wlan0 (to put the pen-tester's wireless adapter in monitor mode)
airodump-ng wlan0mon (to identify your AP's MAC address, the channel number used, and the target device's MAC address)

(e) Once you identified your AP's channel (e.g., 11), run the below command to capture wireless packets on that channel and write/save them to a file. Report your work, time, and relevant screenshot(s):

airodump-ng -c 11 --bssid xx:xx:xx:xx:xx:xx -w out wlan0mon (to start capturing wireless packets on channel 11 (replace 11 with your AP's channel), AP's MAC address of 6 bytes separated by the colon ":" symbol (replace XX's with your AP's MAC address), save packets to the file "out" in the current directory (e.g., under /root); there will be several files saved starting their names with "out".

(f) Open a new terminal in Kali (while keeping the terminal of the previous part intact), run the below aireplay-ng command to de-authenticate the target/victim machine, and wait for the command airodump-ng of the previous part captures the WPA/WPA2 4-way handshake packets between the AP and the target/victim machine:

aireplay-ng -0 1 -a xx:xx:xx:xx:xx:xx -c yy:yy:yy:yy:yy:yy wlan0mon
-0 means de-authentication
1 is the number of de-authentications to send (you can send multiple if you wish)
-a xx:xx:xx:xx:xx:xx is to specify the AP's MAC address
-c yy:yy:yy:yy:yy:yy is to specify the client (target/victim)'s MAC address

Describe your work (procedure and steps), results, and relevant screenshot(s).

Wait for the airodump-ng terminal of Part (e) to show WPA Handshake has been captured (a message displayed in its upper right corner). Take a screenshot, then type CTRL-C to terminate airodump-ng(started in Step (e). Use the command "ls –l" to list the capture file(s) in the current directory. Describe your work, results, and relevant screenshot(s).

(g) Create a "dictionary" (wordlist) consisting of the current password/phrase for the AP, for example, using the command "echo zzzzz > dictionary" replacing zzzzz with your AP's password/phrase will create a file named "dictionary" in the current dictionary consisting of a single word "zzzz". Use the command "cat dictionary" to type out the file's content. Describe your work, results, and relevant screenshot(s). Please note that in practice, the dictionary/wordlist would consist of many words that are presumably popular choices for a password/phrase, and that those AP's using such common passwords/phrases will be potential hacking victims.

(h) Use the aircrack-ng command shown below to crack the AP's password/phrase:

```
aircrack-ng -w dictionary out*.cap
```

Describe your work, results, and relevant screenshot(s).

(i) After successfully completing the above work, logon to your AP and restore the AP's password/phrase to its original.

2. (16 pts., **Part 2 incomplete**) This question continues from Question 1, assuming the pen-tester machine (Kali Linux) is connected to the AP, and there is a target/victim Windows machine also connected to the same wireless network (running WPA/WPA2-PSK security after the pen-tester has successfully obtained the PSK). Answer the below questions and **describe your work, results, and relevant screenshot(s) for each of the steps**.
Note: To balance documentations of your work and, at the same time, protecting your privacy, please **do not include** model/serial numbers in your answers or screenshots, and, for MAC addresses (6 bytes), report only the first 2 bytes and blank out the last 4 bytes (out of the 6 bytes); for SSIDs, blank out all leading characters except for the last character of the SSID. Regarding IP addresses you need to **include/show all local IP addresses** (e.g., 10.x.x.x or 192.168.x.x) in your answers including screenshots but please blank out all IPv6 addresses and, for global IPv4 addresses, blank out the first 3 decimal numbers but keep the last decimal number (e.g., the DNS servers on the target Windows system include: 192.168.0.1 (show a local address) and x.x.x.226 (show the last decimal number of a global IP address).
Part 1. ARP Spoofing:

(a) Same as in Question 1(a), describe your equipment and include a statement authorizing your use of the equipment for pen-testing.

(b) Open a command window on the target Windows system and type the command "ipconfig /all" (without the quotes) to report the wireless LAN network connection, including: wireless adapter's MAC address, (local) IPv4 address, default gateway, etc. Also, type the command "arp -a" and report the current content of the system's ARP table.
Note: Address Resolution Protocol (ARP, https://en.wikipedia.org/wiki/Address_Resolution_Protocol) is the protocol used to map IPv4 addresses to MAC addresses on the local subnet.

(c) Open a terminal in Kali Linux, type the command "iwconfig" to report its wireless connection, and type the command "arp –a" to report the current content of the system's ARP table. In particular, the ARP table should show **the AP's MAC address.**

In Parts (d) – (h) below you will demonstrate how to use ARP poisoning/spoofing "to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead." Also, "ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic." (https://en.wikipedia.org/wiki/ARP_spoofing). Specifically, you will demonstrate how the attacker captures the web pages opened by the victim after its ARP table is poisoned.

(d) Zenmap, which is a graphical front-end to nmap and a tool for network exploration and security auditing (port scanning), is preinstalled in Kali Linux. To start zenmap, select it under the main menu Applications>Information Gathering. Alternatively, open a new terminal and type zenmap followed by <Enter> to start it. In zenmap, enter appropriate local subnet (for example, 192.168.0.1/24, based on the interface wlan0's IP address and the network mask in the command ifconfig's output) as the target and select "Quick scan plus" in Profiles' list, then click the "Scan" button. Report the actual nmap command syntax used for this scan, and the purpose of each of the flags/switches used in the command (by consulting nmap's man(ual) pages typing the command "man nmap" in a terminal, using space-bar to advance a page, <Enter> to advance a single line, and "q" to quit the man page). Additionally, report the scan's output when done. In particular, identify a target that is a Windows system from the output (which will be used as the target/victim for this question). After completing this part, close/terminate zenmap.

(e) On the same Kali Linux terminal of Part (c), first type the command "echo 1 > /proc/sys/net/ipv4/ip_forward" (without the quotes) to enable IP forwarding. Then, type the below command to "spoof/poison" the target Windows system's ARP table:

arpspoof –i wlan0 –t x.x.x.x y.y.y.y

(where x.x.x.x is the target/victim's IP address, y.y.y.y is the AP's IP address)

The above command will cause the Kali terminal to continuously outputting ARP redirect messages. Leave this terminal intact.

Similarly, open another (new) terminal in Kali and type the below command:

arpspoof –i wlan0 –t x.x.x.x –r y.y.y.y

(where x.x.x.x is the target/victim's IP address, y.y.y.y is the AP's IP address)

Also, leave this terminal intact.

Go to the target Windows system, type that command "arp –a" to report the current content of its ARP table, and note any differences in the AP's MAC address compared to the earlier results reported in Part (b).

(f) Open another (new) terminal in Kali Linux while keeping both terminals of the previous part intact. Type the below tcpdump command (all on one line) to capture any http traffic to/from the target Windows system and save to a file named "tcpdump.pcap" in the current directory:

tcpdump –i wlan0 –s 1500 –w tcpdump.pcap "host x.x.x.x and tcp port http"

(where x.x.x.x is the target/victim's IP address)

Keep this terminal intact.

(g) While tcpdump of Part (f) is running, go to the target Windows system, open a web browser (Chrome, Firefox, etc.) and logon to the below site to generate some http traffic:

http://www.cs.ucf.edu/courses/cgs5131/fall2007

After the page is loaded, close the browser.

(h) Return to Kali's terminal running the tcpdump command of Part (f), type CTRL-c to terminate tcpdump. Use the command "ls –l" to identify a file named "tcpdump.pcap" has been created. Use Wireshark (in Kali or in a Windows system) to open the captured pcap file and identify the HTML page of the website accessed in Part (g).

Part 2. Client-Side Attack: Exploit of a Windows System using Metasploit:
The Metasploit Project is a security project which delivers information about security vulnerabilities and helps penetration testing and intrusion detection. "The open source project– known as the Metasploit Framework, is used by security professionals to execute exploit code against a remote target machine–for penetration testing." (http://www.concise-courses.com/security/top-ten-pentesting-tools/)

There are three terms used in penetration testing you need to understand (https://www.rapid7.com/resources/penetration-testing/):

- A vulnerability is a security hole in a piece of software, hardware or operating system that provides a potential angle to attack the system. A vulnerability can be as simple as weak passwords or as complex as buffer overflows or SQL injection vulnerabilities.
- An exploit is a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system.
- A payload is the piece of software that lets you control a computer system after it's been exploited. The payload is typically attached to and delivered by the exploit.

(To be cont'd)

3. (6 pts.) A Bluetooth attack includes understanding the technology behind your target as well as scanning and reconnaissance analysis; it concludes with attack and exploitation. First, review the below figure depicting a Bluetooth host (e.g., laptop) and its controller hardware (Joshua Wright and Johnny Cache, "Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions," McGraw-Hill, 2015):

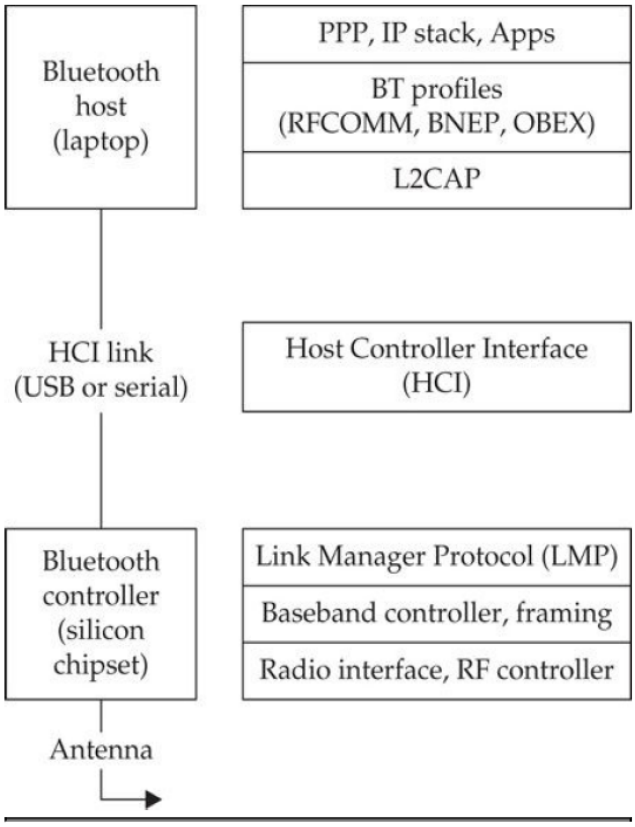

Figure 7-2 Bluetooth host and controller interaction

In addition to the structured Bluetooth stack layers, the Bluetooth Special Interest Group (SIG)—the organization responsible for defining the Bluetooth specification—specifies multiple application-layer profiles. These profiles define additional functionality and security mechanisms for various Bluetooth uses. Implemented on the host, these profiles

can be manipulated freely without specialized hardware. Available profiles include the Service Discovery Protocol (SDP), Advanced Audio Distribution Profile (A2DP), Headset Profile (HSP), Object Exchange Profile (OBEX), and Personal Area Network Profile (PANP).

The purpose of this question is to demonstrate the use of several Bluetooth tools available in Kali Linux. The list of tools/commands and their brief descriptions are as follows:

- hciconfig: The command hciconfig is used to configure Bluetooth devices.
- hcitool: The command hcitool can be used for Bluetooth device discovery and basic enumeration.
- hcidump: The command hcidump reads raw HCI data coming from and going to a Bluetooth device (which can be specified with the option -i, default is the first available one) and prints to screen commands, events and data in a human-readable form. Optionally, the dump can be written to a file rather than parsed, and the dump file can be parsed in a subsequent moment.
- sdptool: The Service Discovery Protocol (SDP) is a protocol defined by the Bluetooth SIG for identifying or publishing services available through a Bluetooth device. From an attack perspective, SDP allows you to identify the potential targets on a host, revealing support for various Bluetooth profiles as well as the configuration details needed to connect to the service. The command sdptool provides the interface for performing SDP queries on Bluetooth devices, and administering a local SDP database.

Equipment: A laptop running Kali Linux with access to a Bluetooth adapter (as the pen-tester machine), and a smart phone with built-in Bluetooth (as the target/victim machine). Note: if you run Kali Linux in a VM then you most probably need to add a Bluetooth USB dongle (~$10) for Kali VM to use.

Follow the below steps and describe your work/results (including screenshots) using your words in each of the steps.
Note: To balance documentations of your work and, at the same time, protecting your privacy, please do not include model/serial numbers in your answers or screenshots, and, for MAC addresses (6 bytes), report only the first 2 bytes and blank out (redact) the last 4 bytes (out of the 6 bytes).

(a) Describe briefly the equipment you use for this question, including: the pen-tester and target machines (e.g., a Dell laptop running Kali Linux VM in Virtualbox, and an Apple iPhone, respectively). Additionally, include a statement whether you have the administrative privilege, or are given the consent, to conduct penetration testing using the equipment described here.

(b) (Configure Bluetooth devices) Open a terminal in Kali Linux. Use the command “hciconfig” to identify the local Bluetooth device (e.g., hci0). Run the command “hciconfig hci0 up” to open/enable the device (if it was down initially), then run the command “hciconfig” to make sure the device is up.

(c) (Active device discovery) Enable your smart phone’s Bluetooth, then in Kali Linux’s terminal run the command “hcitool scan --all --flush” to identify the smart phone’s Bluetooth device, including its address (BD_ADDR), the device name, device class, manufacturer, etc. Note: Since your smart phone’s Bluetooth may be in “discovery mode” only briefly, when you run the above hcitool command again later, you may get no output at all. There are commercial tools (hardware and software) that can help with passive device discovery, such as the Ubertooth ($120) available at http://greatscottgadgets.com/ubertoothone.

(d) (Service Enumeration) In Kali Linux's terminal use the command "sdptool browse xx:xx:xx:xx:xx:xx" where the 6-byte address xx:xx:xx:xx:xx:xx is the smart phone Bluetooth's BD_ADDR from Part (c), to browse all available services on the device specified by the Bluetooth BD_ADDR. Note: A great source for Bluetooth profile information is the Wikipedia article on "List of Bluetooth Profiles" at https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

(e) (Extra-Credit, 2 pts.) (Manipulating Service and Device Class Information) In Kali Linux's terminal use the command "hciconfig hci0 class" to find out the local Bluetooth device's class information. As the root user, you can change the service and device class information to manipulate the system's identity. For example, we can change the service and device class information to 0xf00704 (major device class: wearable device; minor device class: wristwatch), by running the command "sudo hciconfig hci0 class 0xf00704 piscan name NotWristWatch". Afterward, run the command "hciconfig hci0 class" again and report the changes. Go to your smart phone and report the phone's Bluetooth device scan results. Note: Details of Bluetooth service, major, and minor classes, are documented by the
Bluetooth SIG and available at https://www.bluetooth.com/specifications/assigned-numbers/baseband.

(f) (Extra-Credit, 2 pts.) (Testing Connection Access) In Kali Linux's terminal run the command "sudo hcidump -t -i hci0" then leave the terminal open/intact. Open a new Kali Linux terminal, run the command "sudo hcitool cc xx:xx:xx:xx:xx:xx" where xx:xx:xx:xx:xx:xx is the smart phone Bluetooth's BD_ADDR, to attempt to create a connection to the phone. Watch the output presented in the first terminal (which is running hcidump) and report the results. You most probably will see the remote device (phone) rejecting the attempted connection.

3. (Alternative)

(6 pts.) This question is concerned with investigation of an allegedly hacked Windows system (which is not directly related to "wireless" network per se although many investigation techniques and tools used here are the same as those used in any network intrusion investigation).

Background: A Windows XP system appeared to be compromised because the owner (victim) claimed that he had seen several times a window popping up and disappearing by itself on his computer screen, and had occasionally seen a webcam image. The owner wrote down the title of the webcam image, "WebCamImageSave", and reported the incident. An incident response specialist came on 10/15/2013 around 02:00 hours local time and quickly ran an Incident Response (IR) script to collect system information, including: the three event log files (AppEvent.Evt, SecEvent.Evt, SysEvent.Evt) of the XP system, a memory (RAM) dump, open handles, network connections, process list, autoruns, and a directory listing of files under the system folder c:\windows\system32. In addition, the IR specialist identified an executable file named "WebCamImageSave.exe" located under the folder c:\windows\system32 and exported it. The MD5 hashes of the event logs and the memory dump file were also computed. More specifically, by running tools from http://www.SysInternals.com (PsTools, autorunsc.exe, handle.exe, tcpvcon.exe), Windows commands (netstat.exe, fciv.exe), and DumpIt.exe (http://qpdownload.com/dumpit/), a total of 14 files were created by the IR specialist: one executable file, 3 event files (of .evt type), one memory dump file, 8 log files (of .txt type), and an MD5 hash file, see the below list:

(1) WebCamImageSave.exe (a suspicious executable file)
(2) AppEvent.Evt
(3) SecEvent.Evt
(4) SysEvent.Evt

(5) UCF-9C75581A172-20131015-050520.raw (the memory dump, 196,544 KB)
(6) autorunsc.txt (of executable files start automatically when Windows boots up)
(7) DirList.txt (a directory listing of files/folders under c:\windows\system32, sorted by the files' last modification time)
(8) handle.txt (of open handles, i.e., files, processes, Windows Registry keys)
(9) netstat.txt (of open network connections)
(10) PsInfo.txt (system information)
(11) pslist.txt (of running processes)
(12) PsService.txt (of running services)
(13) tcpvcon.txt (of open TCP connections)
(14) MD5hashes.txt (MD5 hashes of the event logs and memory dump file)

A zip file "hw6-files.zip" containing the above 14 files is prepared for the assignment. The zip file's size is 76,879,843 bytes, and its MD5 hash is D5C8C241EC00D02E2D5A32F76F42001B.

Answer each of the following questions, <u>including a brief explanation</u> of how you derive your answer:

(a) What is the version of the compromised Windows XP system? (Hint: Look it up in PsInfo.txt)
(b) What is the IP address of the local (i.e., the compromised) system? (Hint: Look it up in netstat.txt)
(c) Are there any suspicious open handles?
(d) What is or are the source IP address(es) of the attack?
(e) What is the evidence of the compromise? (Hint: Review autorunsc.txt, netstat.txt and tcpvcon.txt)
(f) (Extra-Credit, 2 pts.) What is the nature of the executable file "WebCamImageSave.exe" and any additional executable file(s), and their roles in the reported intrusion incident?
(g) (Extra-Credit, 2 pts.) What procedures do you recommend to remove the malware, and to further secure the hacked Windows system?

Note: (FYI Only) Memory forensic tools such as Volatility (http://www.volatilityfoundation.org/) or Redline (https://www.fireeye.com/services/freeware/redline.html), would be useful for examining the captured RAM dump and extracting more details of potential hacking evidence.