

## Exam Report: 13.2.5 Practice Questions

Date: 5/26/2020 6:29:15 pm

Candidate: Garsteck, Matthew

Time Spent: 1:07

Login: mGarsteck

## Overall Performance

Your Score: 25%



Passing Score: 80%

View results by: ☐ Objective Analysis ☒ Individual Responses

## Individual Responses

## ▼ Question 1:

**Incorrect**

Which of the following Bluetooth configuration and discovery tools can be used to check which services are made available by a specific device and can work when the device is not discoverable, but is still nearby?

☐ hciconfig☒ sdptool☒ l2ping☐ hcitool**Explanation**

The sdptool tool provides the interface for performing Service Discovery Protocol (SDP) queries on Bluetooth devices. The sdptool can be used to check which services are made available by a specific device and can work when the device is not discoverable, but is still nearby.

The hciconfig tool is used to view and manage Linux Bluetooth devices. When run without any options, hciconfig displays the name and basic information about all the Bluetooth devices installed in the system. hcix (where x is a number) is the name of a Bluetooth device installed in the system. HCI is an acronym for Host Controller Interface.

The hcitool tool is used to configure Bluetooth connections and send some special commands to the Bluetooth devices. If no command is given or if the option -h is used, hcitool prints some usage information and exits.

The l2ping tool sends an L2CAP echo request to a Bluetooth MAC address. It can only be run by the root user and is used to check to see if the Bluetooth device is up.

**References**

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_DISCOVERY\_TOOLS\_01\_EH1]

## ▼ Question 2:

**Incorrect**

A user is having trouble connecting to a newly purchased Bluetooth device. An administrator troubleshoots the device using a Linux computer with BlueZ installed. The administrator sends an echo request to the device's Bluetooth MAC address to determine whether the device responds. Which of the following commands was used?

☒ l2ping☒ hciconfig☐ hcitool☐ sdptool

## Explanation

The l2ping command sends an L2CAP echo request to a Bluetooth MAC address given in dotted hex notation. This command can only be run by the root user and is used to check to see if the Bluetooth device is up.

The hciconfig command is used to view and manage Linux Bluetooth devices. When run without any options, hciconfig displays the name and basic information about all the Bluetooth devices installed in the system. hcix (where x is a number) is the name of a Bluetooth device installed in the system.

The hcitool command is used to configure Bluetooth connections and send some special commands to the Bluetooth devices.

The sdptool command provides the interface for performing Service Discovery Protocol (SDP) queries on Bluetooth devices. The sdptool command can be used to check which services are made available by a specific device and can work when the device is not discoverable, but is still nearby.


## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_DISCOVERY\_TOOLS\_02\_EH1]

### ▼ Question 3: Correct

Which of the following Bluetooth discovery tool commands will show the Bluetooth MAC address, clock offset, and class of each discovered device?

- ☐ hcitool scan
- ☐ hciconfig hci0 up
-  ☒ hcitool inq
- ☐ l2ping scan

## Explanation

The hcitool inq command searches for remote devices. For each discovered device, the clock offset and class are shown.

The hciconfig hci0 up command opens and initializes the hci0 Bluetooth device discovered by the hciconfig command.

The l2ping scan command returns an error. l2ping xx:xx:xx:xx:xx:xx sends an L2CAP echo request to the Bluetooth MAC address given in dotted hex notation.

The hcitool scan command searches for remote devices. For each discovered device, the device's MAC address and name are displayed.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_DISCOVERY\_TOOLS\_03\_EH1]

### ▼ Question 4: Incorrect

Which of the following Bluetooth discovery tools will produce the output shown below?

```
Service Name: Headset Audio Gateway
Service RecHandle: 0x10002
Service Class ID List:
  "Headset Audio Gateway" (0x1112)
  "Generic Audio" (0x1203)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
  Channel: 1
Language Base Attr List:
  code_IS0639: 0x656e
  encoding:    0x6a
  base_offset: 0x100
```

```
Profile Descriptor List:  
  "Headset" (0x1108)  
    Version: 0x0102
```

- ☐ hcitool
- ☒ l2ping
- ☐ hciconfig

➡ ☐ sdptool

## Explanation

The sdptool tool performs Service Discovery Protocol (SDP) queries on Bluetooth devices and will show all available services on the device.

The hciconfig tool is used to view and manage Linux Bluetooth devices.

The hcitool tool is used to configure Bluetooth connections and send special commands to a Bluetooth device.

The l2ping tool sends an L2CAP echo request to a Bluetooth MAC address given in dotted hex notation.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_DISCOVERY\_TOOLS\_04\_EH1]

### ▼ Question 5: Incorrect

Which of the following types of Bluetooth hacking is a denial-of-service attack?

- ➡ ☐ Bluesmacking
- ☐ Bluebugging
- ☒ Bluesnarfing
- ☐ Bluejacking

## Explanation

A Bluesmack attack is a denial-of-service attack where the L2CAP layer of the Bluetooth protocol stack is used to transfer an oversized packet causing the L2CAP layer to crash, denying Bluetooth services to the user.

Bluejacking is the act of sending unwanted data to Bluetooth devices that are enabled and discoverable. Bluejacking hackers don't gain control of the device and can't steal data from the device. The messages they send are usually more annoying than malicious.

Bluesnarfing exploits the Object Exchange (OBEX) protocol to gain access to a device. If that device is a smartphone, the attacker can access the address book, call, and text information and other data.

A Bluebugging attack exploits a Bluetooth device to install a backdoor that bypasses normal authentication, giving full access to the device. Bluebugging has been used to initiate and forward phone calls from a smartphone, send text messages, steal sensitive data, track victims, and even change network provider settings.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_HACKING\_01\_EH1]

### ▼ Question 6: Incorrect

Which of the following best describes Bluetooth MAC spoofing?

- ☒ An attacker performs a denial of service attack where the L2CAP layer of the Bluetooth protocol stack is used to transfer an oversized packet, causing the L2CAP layer to crash.

- ☒ An attacker changes the Bluetooth address of his own device to match the address of a target device so that the data meant for the victim device reaches the attacker's device first.
- ☐ An attacker exploits a Bluetooth device by installing a backdoor that bypasses normal authentication, giving the attacker full access.
- ☐ An attacker sends unwanted data, such as annoying messages, to Bluetooth devices that are enabled and discoverable.

## Explanation

Bluetooth MAC spoofing occurs when an attacker changes the Bluetooth address of his own device to match a target device's address. In this attack, the data meant for the victim device reaches the attacker's device first.

A Bluesmacking attack is a denial-of-service attack. The L2CAP layer of the Bluetooth protocol stack is used to transfer an oversized packet. This causes the L2CAP layer to crash, denying the user Bluetooth services.

A Bluebugging attack exploits a Bluetooth device to install a backdoor that bypasses normal authentication, giving full access to the device. Bluebugging has been used to initiate and forward phone calls from a smartphone, send text messages, steal sensitive data, track victims, and even change network provider settings.

Bluejacking is the act of sending unwanted data to Bluetooth devices that are enabled and discoverable. Bluejacking hackers don't gain control of the device and can't steal data from the device. The messages they send are usually more annoying than malicious.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_HACKING\_02\_EH1]

### Question 7:

Incorrect

Jim, a smartphone user, receives a bill from his provider that contains fees for calling international numbers he is sure he hasn't called. Which of the following forms of Bluetooth hacking was most likely used to attack his phone?

- ☐ Bluesmacking
- ☒ Bluebugging
- ☐ Bluejacking
- ☐ Bluesniffing

## Explanation

A Bluebugging attack exploits a Bluetooth device to install a backdoor that bypasses normal authentication, giving full access to the device, including the ability to initiate phone calls.

A Bluesmacking attack is a denial-of-service attack. His phone remains operational.

A Bluejacking attack sends unwanted data to Bluetooth devices, but does not give access to the phone.

A Bluesniffing attack finds discoverable Bluetooth devices, but is only used to locate the device.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_HACKING\_03\_EH1]

### Question 8:

Incorrect

Which of the following Bluetooth hacking tools is a complete framework to perform man-in-the-middle attacks on Bluetooth smart devices?

- ☐ BluetoothView
- ☒ Btlejuice
- ☐

- ☐ Bluediving
- ☒ ~~BTScanner~~

## Explanation

Btlejuice is a complete framework to perform man-in-the-middle attacks on Bluetooth smart devices. It is composed of an interception core, an interception proxy, and a dedicated web interface. The core and proxy components are run on two independent computers, each with a Bluetooth adapter. Using the two adapters, btlejuice can send and receive Bluetooth communications to perform the man-in-the-middle attack.

BluetoothView is a small utility that lists discoverable Bluetooth devices with information such as the device name, Bluetooth address, major device type, and minor device type. It runs in the background and monitors the activity of Bluetooth devices. It can also send a notification when a new Bluetooth device is detected.

BTScanner is another Linux-based Bluetooth sniffing tool that provides the same functions as BluetoothView.

Bluediving is a Bluetooth penetration suite that runs on Linux. It can implement several attacks, including bluebug, bluesnarf, and bluesmack. It also performs Bluetooth address spoofing.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking  
[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_HACK\_TOOLS\_01\_EH1]

### ▼ Question 9: Correct

Which of the following best describes the Bluediving hacking tool?

- ➔ ☒ A penetration suite that runs on Linux that can implement several attacks, including bluebug, bluesnarf, and bluesmack, and also performs Bluetooth address spoofing.
- ☐ A small utility that lists discoverable Bluetooth devices with information such as the device name, Bluetooth address, major device type, and minor device type.
- ☐ An Android phone application that can be used to view the files on another Bluetooth-connected Android phone.
- ☐ A complete framework to perform man-in-the-middle attacks on Bluetooth smart devices that is composed of an interception core, an interception proxy, and a dedicated web interface.

## Explanation

Bluediving is a Bluetooth penetration suite that runs on Linux. It can implement several attacks, including bluebug, bluesnarf, and bluesmack. It also performs Bluetooth address spoofing.

BluetoothView is a small utility that lists discoverable Bluetooth devices with information such as the device name, Bluetooth address, major device type, and minor device type. It runs in the background and monitors the activity of Bluetooth devices. It can also send a notification when a new Bluetooth device is detected.

Btlejuice is a complete framework to perform man-in-the-middle attacks on Bluetooth smart devices. It is composed of an interception core, an interception proxy, and a dedicated web interface. The core and proxy components are run on two independent computers, each with a Bluetooth adapter. Using the two adapters, btlejuice can send and receive Bluetooth communications to perform a man-in-the-middle attack.

Super Bluetooth Hack is an Android phone application that can be used to view the files on another Bluetooth-connected Android phone.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking  
[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_HACK\_TOOLS\_02\_EH1]

### ▼ Question 10: Incorrect

Which of the following Bluetooth threats has increased due to the availability of software that can be used to activate Bluetooth cameras and microphones?

- ☐ Smartphone worms that replicate by exploiting Bluetooth connections.
- ☐ Phone calls made through compromised smartphones to numbers that charge fees.
- ➡ ☐ The creation of Bluetooth bugging and eavesdropping devices.
- ☒ The leaking of calendars and address books through the Bluetooth protocol.

## Explanation

The creation of Bluetooth bugging and eavesdropping devices has become easier due to availability of software that can be used to activate Bluetooth cameras and microphones.

Smartphone worms are not replicated by software used to activate Bluetooth cameras and microphones.

Phone calls made through compromised smartphones to numbers that charge fees are not implemented through software used to activate Bluetooth cameras and microphones.

The leakage of calendars and address books through the Bluetooth protocol is not implemented through software used to activate Bluetooth cameras and microphones.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_BT\_THREATS\_01\_EH1]

### ▼ Question 11:

Incorrect

Which of the following Bluetooth attack countermeasures would help prevent other devices from finding your Bluetooth device that is in continuous operation?

- ☐ Ensure the Bluetooth device is operating in a lower security mode.
- ☐ Raise the power setting on Bluetooth devices.
- ☒ Use a regular pattern when pairing your device.
- ➡ ☐ Use hidden mode when your Bluetooth device is enabled.

## Explanation

While Bluetooth is enabled on your device, you can use hidden mode. Hidden mode prevents other devices from finding your device.

Ensure each Bluetooth device is operating in a higher security mode.

- The Bluetooth specification details four security modes.
- Mode 1 is unsecure, but has been phased out in later versions.
- Each successive security mode is more secure.
- Mode 4 requires encryption and the use of Diffie-Hellman techniques for key exchange and key generation.
- Later versions of Bluetooth require mode 4.

Using non-regular patterns when pairing makes the PIN harder to guess.

Lowering the power setting on Bluetooth devices will decrease Bluetooth range and reduces the possibility of an outsider attack.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUETOOTH\_HACKING\_COUNTERMEASURES\_01\_EH1]

### ▼ Question 12:

Correct

Ann has a corner office that looks out on a patio that is frequently occupied by tourists. She likes the convenience of her Bluetooth headset paired to her smartphone, but is concerned that her conversations could be intercepted by an attacker sitting on the patio. Which of the following countermeasures would be the most effective for protecting her conversations?

- ➡ ☒ Lower the Bluetooth power setting on the smartphone and headset.

- ☐ Add a Bluetooth firewall to the smartphone.
- ☐ Use a non-regular pattern when pairing the headset.
- ☐ Disable the headset when it is not being used.

## Explanation

Lowering the Bluetooth power settings will decrease the Bluetooth range, making it harder to intercept from a distance.

A non-regular pairing pattern makes the PIN keys harder to guess, but doesn't affect the Bluetooth signal.

Disabling the headset when not in use will limit its exposure, but will not affect Bluetooth vulnerabilities while the headset is operating.

A Bluetooth firewall guards against hacking the smartphone, but doesn't prevent the signal from being intercepted.

## References

TestOut Ethical Hacker Pro - 13.2 Bluetooth Hacking

[e\_blue\_tooth\_hacking\_eh1.exam.xml Q\_BLUEETOOTH\_HACKING\_COUNTERMEASURES\_02\_EH1]