SET - 1

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date: 22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:

Multiple choice questions:

1) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

2) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

3) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

4) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

5) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

6) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

7) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

8) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

9) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

10) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence
c) Admissibility of Evidence d) Discovery of Evidence

SET - 1

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY Date: 22-02-19
Time: 20 mins Max.Marks:10

==========

Answer all the following:

Multiple choice questions:

1) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

2) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

3) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

4) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

5) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

6) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

7) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

8) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

9) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

10) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence
c) Admissibility of Evidence d) Discovery of Evidence

Fill in the blanks:

11) _____ is the crime that involves a computer and a network.

12) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

13) The two components of security in mobile computing are _____ and _____

14) Computer Forensics is known as _____ approach to network and computer security.

15) The best defense against any type of sniffing is _____

State True or False (T or F):

16) Mishing attacks are attempted using mobile phone technology [ ]

17) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

18) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

19) Polymorphic virus modifies itself to avoid detection [ ]

20) To locate live systems ping sweep is used [ ]

Fill in the blanks:

11) _____ is the crime that involves a computer and a network.

12) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

13) The two components of security in mobile computing are _____ and _____

14) Computer Forensics is known as _____ approach to network and computer security.

15) The best defense against any type of sniffing is _____

State True or False (T or F):

16) Mishing attacks are attempted using mobile phone technology [ ]

17) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

18) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

19) Polymorphic virus modifies itself to avoid detection [ ]

20) To locate live systems ping sweep is used [ ]

SET - 2

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IVB.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date: 22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

2) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

3) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

4) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

5) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

6) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence
c) Admissibility of Evidence d) Discovery of Evidence

7) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

8) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

9) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

10) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

SET - 2

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IVB.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date: 22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

2) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

3) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

4) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

5) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

6) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence
c) Admissibility of Evidence d) Discovery of Evidence

7) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

8) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

9) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

10) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

Fill in the blanks:

11) The two components of security in mobile computing are _____ and _____

12) Computer Forensics is known as _____ approach to network and computer security.

13) The best defense against any type of sniffing is _____

14) _____ is the crime that involves a computer and a network.

15) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

State True or False (T or F):

16) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

17) Polymorphic virus modifies itself to avoid detection [ ]

18) To locate live systems ping sweep is used [ ]

19) Mishing attacks are attempted using mobile phone technology [ ]

20) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

Fill in the blanks:

11) The two components of security in mobile computing are _____ and _____

12) Computer Forensics is known as _____ approach to network and computer security.

13) The best defense against any type of sniffing is _____

14) _____ is the crime that involves a computer and a network.

15) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

State True or False (T or F):

16) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

17) Polymorphic virus modifies itself to avoid detection [ ]

18) To locate live systems ping sweep is used [ ]

19) Mishing attacks are attempted using mobile phone technology [ ]

20) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

SET - 3

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date:22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence c) Admissibility of Evidence
d) Discovery of Evidence

2) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

3) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

4) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

5) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

6) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

7) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

8) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

9) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

10) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

SET - 3

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date:22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence c) Admissibility of Evidence
d) Discovery of Evidence

2) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

3) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

4) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

5) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

6) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing luxury goods and services
c)transferring money/funds d)all of the above

7) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

8) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

9) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

10) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

Fill in the blanks:

11) The best defense against any type of sniffing is _____

12) Computer Forensics is known as _____ approach to network and computer security.

13) The two components of security in mobile computing are _____ and _____

14) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

15) _____ is the crime that involves a computer and a network.

State True or False (T or F):

16) To locate live systems ping sweep is used [ ]

17) Polymorphic virus modifies itself to avoid detection [ ]

18) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

19) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

20) Mishing attacks are attempted using mobile phone technology [ ]

Fill in the blanks:

11) The best defense against any type of sniffing is _____

12) Computer Forensics is known as _____ approach to network and computer security.

13) The two components of security in mobile computing are _____ and _____

14) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.

15) _____ is the crime that involves a computer and a network.

State True or False (T or F):

16) To locate live systems ping sweep is used [ ]

17) Polymorphic virus modifies itself to avoid detection [ ]

18) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

19) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]

20) Mishing attacks are attempted using mobile phone technology [ ]

SET - 4

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date: 22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence c) Admissibility of Evidence
d) Discovery of Evidence

2) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

3) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

4) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

5) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

6) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

7) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

8) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

9) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

10) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing laxury goods and services
c)transferring money/funds d)all of the above

SET - 4

G.PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY (AT)
IV B.Tech II Semester 1st Mid Examination - Objective
Branch: Computer Science and Engineering

Sub: CYBER SECURITY **Date: 22-02-19**
Time: 20 mins **Max.Marks:10**

==========

Answer all the following:
Multiple choice questions:

1) What is the most significant legal issue in computer forensics? [ ]
a) Preserving Evidence b) Seizing Evidence c) Admissibility of Evidence
d) Discovery of Evidence

2) Bluetooth hacking tools [ ]
a) car whisperer b) Trojan horse c) trapdoor d) all of the above

3) Keyloggers are a form of _____. [ ]
a)spyware b) Shoulder surfing c) Trojan d) Social engineering

4) The security of RAS system involves [ ]
a) server b) client c) data transmission d) all of the above

5) What type of password attack would be most successful against the password T63k#s23A? [ ]
a) Dictionary b) Hybrid c) Password guessing d)Brute force

6) NIST stands for [ ]
a)National industry of standards and technology
b)National international of standards and technology
c)National internet of standards and technology
d)National institute of standards and technology

7) The first phase of hacking an IT system is compromise of which foundation of security? [ ]
a) Availability b) Confidentiality c) Integrity d) Authentication

8) IMEI stands for [ ]
a)International mobile equipmental identity
b)International mobile equipments identity
c)International mobile equipment identity
d)International mobile equipmention identity

9) To hide information side a picture, what technology is used? [ ]
a)Root kits b)Bitmapping c)Steganography d)Image Rendering

10) The most profitable uses of the information gained through a vishing attack include [ ]
a)Identity theft b)purchasing laxury goods and services
c)transferring money/funds d)all of the above

Fill in the blanks:

11) The best defense against any type of sniffing is _____
12) _____ is the crime that involves a computer and a network.
13) Computer Forensics is known as _____ approach to network and computer security.
14) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
15) The two components of security in mobile computing are _____ and _____

State True or False (T or F):

16) To locate live systems ping sweep is used [ ]
17) Mishing attacks are attempted using mobile phone technology [ ]
18) Polymorphic virus modifies itself to avoid detection [ ]
19) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]
20) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]

Fill in the blanks:

11) The best defense against any type of sniffing is _____
12) _____ is the crime that involves a computer and a network.
13) Computer Forensics is known as _____ approach to network and computer security.
14) _____ is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
15) The two components of security in mobile computing are _____ and _____

State True or False (T or F):

16) To locate live systems ping sweep is used [ ]
17) Mishing attacks are attempted using mobile phone technology [ ]
18) Polymorphic virus modifies itself to avoid detection [ ]
19) Blue jacking is sending unsolicited messages over Bluetooth-enabled devices such as mobile phones, PDA 's or computer with in 15m radius [ ]
20) The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country [ ]