Question Text	Question Type	Option 1	Option 2
Text of the question (required)	Question Type (default is Multiple Choice)	Text for option 1 (required in all cases except open-ended & draw questions)	Text for option 2 (required in all cases except open-ended & draw questions)
The stage in a computer forensics investigation wherein the data involved is collected. Often the means used is a bit-by-bit copy or a forensic working images of the hard disk or other media in question.	Multiple Choice	Acquisition	Active Files
Data on a computer that is not deleted and is generally accessible and readily visible to the user under normal use.	Multiple Choice	Active Files	Allocated space / sector / block
The logical area on a hard disk or other media assigned to a file by the Operating System (See Unallocated)	Multiple Choice	Allocated space / sector / block	Allocation Block
A contiguous group of sectors, which is the smallest amount of space, assigned to a file by an operating system such as Microsoft Windows.	Multiple Choice	Allocation Block	Application
Commonly known as a Program, or (sometimes) Software. The software used to access and create files or documents. Microsoft Word and Corel WordPerfect are applications that work with word processing documents. Microsoft Excel and Lotus 1-2-3 are applications that work with or spreadsheets.	Multiple Choice	Application	ASCII

_____ uses 8 bits to encode any character, most of them from the English language used in modern-day programming. It is also used in graphic arts to represent clip art or images using characters. The major disadvantage of _____ is that it can represent only 256 different characters as it can use only 8 bits. _____ cannot be used to encode the many types of characters found around the world. Unicode was extended further to UTF-16 and UTF-32 to encode the various types of characters. Therefore, the significant difference between _____ and Unicode is the number of bits used to encode.	Multiple Choice	ASCII	Audit Trail
A chronological record of system activities on a computer or network security system that may keep track of user actions such as logins, file access, and other activities.	Multiple Choice	Audit Trail	Back door
A means of accessing or controlling a computer that bypasses normal authentication, while remaining hidden from the casual user. A backdoor may be a program that has been installed surreptitiously, or may be a hidden function of a legitimate program.	Multiple Choice	Back door	Backdoor Trojan
A generic name for Trojan horse programs that open a backdoor and allow an unauthorized user remote access to a computer.	Multiple Choice	Backdoor Trojan	Backup
A copy of data that is kept as an emergency measure against data loss in a system or media failure, and/or for the purpose of keeping archival data. Backups may be compressed or encrypted, and are usually kept separate from the system containing the active version of the data that is being backed up.	Multiple Choice	Backup	Backup media
A hacker sending unsolicited messages via Bluetooth is a form of?	Multiple Choice	Bluejacking	Bluesnarfing
A buffer overflow occurs when:	Multiple Choice	Data exceeds the storage capacity of a buffer.	A system runs out of RAM.

A Man-in-the-Middle (MitM) attack in which an attacker intercepts communication between two parties without altering it is called:	Multiple Choice	Eavesdropping	Sniffing
What is the primary purpose of a rootkit?	Multiple Choice	Keylogging	Evasion from detection
Which type of vulnerability assessment tool actively attempts to exploit discovered vulnerabilities?	Multiple Choice	Passive scanner	Intrusive scanner
Which attack involves capturing packets from a network and potentially using them for malicious purposes?	Multiple Choice	Spoofing	Sniffing
Which of the following attacks typically involves a third-party service to amplify the attack traffic?	Multiple Choice	Ping flood	SYN flood
Which of the following describes a zero-day exploit?	Multiple Choice	An exploit that impacts zero systems.	An exploit that is discovered and patched within one day.
Which type of malware is typically responsible for holding a user's data hostage until a ransom is paid?	Multiple Choice	Worm	Virus
Phishing attempts that target specific individuals or companies are referred to as:	Multiple Choice	Vishing	Whaling
The stage in a computer forensics investigation wherein the data involved is collected. Often the means used is a bit-by-bit copy or a forensic working images of the hard disk or other media in question.	Fill-in-the-Blank	Acquisition	ACQUISITION
Data on a computer that is not deleted and is generally accessible and readily visible to the user under normal use.	Fill-in-the-Blank	Active Files	ACTIVE FILES
A contiguous group of sectors, which is the smallest amount of space, assigned to a file by an operating system such as Microsoft Windows.	Fill-in-the-Blank	Allocation Block	ALLOCATION BLOCK
Commonly known as a Program, or (sometimes) Software. The software used to access and create files or documents. Microsoft Word and Corel WordPerfect are applications that work with word processing documents. Microsoft Excel and Lotus 1-2-3 are applications that work with or spreadsheets.	Fill-in-the-Blank	Application	APPLICATION

_____ uses 8 bits to encode any character, most of them from the English language used in modern-day programming. It is also used in graphic arts to represent clip art or images using characters. The major disadvantage of _____ is that it can represent only 256 different characters as it can use only 8 bits. _____ cannot be used to encode the many types of characters found around the world. Unicode was extended further to UTF-16 and UTF-32 to encode the various types of characters. Therefore, the significant difference between _____ and Unicode is the number of bits used to encode.	Fill-in-the-Blank	ASCII	ASCII
A chronological record of system activities on a computer or network security system that may keep track of user actions such as logins, file access, and other activities.	Fill-in-the-Blank	Audit Trail	AUDIT TRAIL
A means of accessing or controlling a computer that bypasses normal authentication, while remaining hidden from the casual user. A _____ may be a program that has been installed surreptitiously, or may be a hidden function of a legitimate program.	Fill-in-the-Blank	Back door	BACK DOOR
A generic name for Trojan horse programs that open a backdoor and allow an unauthorized user remote access to a computer.	Fill-in-the-Blank	Backdoor Trojan	BACKDOOR TROJAN
A copy of data that is kept as an emergency measure against data loss in a system or media failure, and/or for the purpose of keeping archival data. Backups may be compressed or encrypted, and are usually kept separate from the system containing the active version of the data that is being backed up.	Fill-in-the-Blank	Backup	BACKUP
The media on which backup data is kept. May be almost any form of media, such as tapes, CD-ROM, DVD, external hard disks, floppy diskettes, magneto-optical disks, WORM disks, Zip disks, Jaz disks, and many others.	Fill-in-the-Blank	Backup media	BACKUP MEDIA
An attack that exhausts system resources rendering a system unusable is known as:	Fill-in-the-Blank	Denial of Service	DENIAL OF SERVICE

A Man-in-the-Middle (MitM) attack in which an attacker intercepts communication between two parties without altering it is called:	Fill-in-the-Blank	Eavesdropping	EAVESDROPPING
What is the primary purpose of a rootkit?	Fill-in-the-Blank	Evasion from detection	EVASION FROM DETECTION
Which type of vulnerability assessment tool actively attempts to exploit discovered vulnerabilities?	Fill-in-the-Blank	Intrusive scanner	INTRUSIVE SCANNER
Which attack involves capturing packets from a network and potentially using them for malicious purposes?	Fill-in-the-Blank	Sniffing	SNIFFING
Phishing attempts that target specific individuals or companies are referred to as:	Fill-in-the-Blank	Spear phishing	SPEAR PHISHING
The media on which backup data is kept. May be almost any form of media, such as tapes, CD-ROM, DVD, external hard disks, floppy diskettes, magneto-optical disks, WORM disks, Zip disks, Jaz disks, and many others.	Multiple Choice	Backup media	Backup Server
A computer on a network that is designed to be used to back up data from other computers on the network. A Backup Server may also be used as a File Server, a Mail Server or as an Application Server.	Multiple Choice	Backup Server	Bit
The smallest unit of data, consisting of a zero or a one, stands for “binary digit.”	Multiple Choice	Bit	Bitstream or bit-by-bit copy
A copy of every consecutive sector on a hard disk or other media, without regard to allocation of data. Sometimes confused with mirroring.	Multiple Choice	Bitstream or bit-by-bit copy	Block
An allocation block, as referred to in the Macintosh Operating System.	Multiple Choice	Block	Buffer
An area of memory used to temporarily hold data. May be written to a buffer file.	Multiple Choice	Buffer	Buffer file
A file written from data in a buffer.	Multiple Choice	Buffer file	Burn
The process of creating a CD-ROM or DVD.	Multiple Choice	Burn	Byte

Eight consecutive bits. The unit in which computer storage and computer memory is measured. The amount of data necessary to make a single character (such as a letter or a number) of data. Part of the words kilobyte (KB), megabyte (MB), gigabyte (GB), terabyte, petabyte.	Multiple Choice	Byte	Cache
French for “hide.” A storage area where frequently accessed data may be kept for rapid access. There are three main types of cache	Multiple Choice	Cache	CD-ROM
Stands for Compact Disk – Read Only Memory. A plastic disk able to hold approximately 650MB to 700MB of data. A common storage medium for data.	Multiple Choice	CD-ROM	Chain of Custody
What attack involves flooding a system with connection requests, using fake IP addresses?	Multiple Choice	TCP SYN flood	ICMP flood
In which type of attack does an attacker exploit a vulnerability without prior knowledge of the vulnerability?	Multiple Choice	Zero-day attack	Replay attack
What is the most common form of social engineering where attackers pretend to be from legitimate organizations, usually over email?	Multiple Choice	Vishing	Phishing
Which type of malware provides a backdoor for unauthorized access to a system?	Multiple Choice	Worm	Trojan
Which type of attack involves sending unauthorized replies to an ARP request?	Multiple Choice	MAC spoofing	DNS poisoning
Which attack involves the hacker predicting the sequence number of TCP packets between the client and server?	Multiple Choice	TCP/IP hijacking	TCP spoofing
An attacker who deceives individuals into providing sensitive data by posing as a trustworthy entity via telephone is using:	Multiple Choice	Impersonation	Phishing
A computer on a network that is designed to be used to back up data from other computers on the network. A Backup Server may also be used as a File Server, a Mail Server or as an Application Server.	Fill-in-the-Blank	Backup Server	BACKUP SERVER
The smallest unit of data, consisting of a zero or a one, stands for “binary digit.”	Fill-in-the-Blank	Bit	BIT
An allocation block, as referred to in the Macintosh Operating System.	Fill-in-the-Blank	Block	BLOCK
An area of memory used to temporarily hold data. May be written to a buffer file.	Fill-in-the-Blank	Buffer	BUFFER

A file written from data in a buffer.	Fill-in-the-Blank	Buffer file	BUFFER FILE
The process of creating a CD-ROM or DVD.	Fill-in-the-Blank	Burn	BURN
Eight consecutive bits. The unit in which computer storage and computer memory is measured. The amount of data necessary to make a single character (such as a letter or a number) of data. Part of the words kilobyte (KB), megabyte (MB), gigabyte (GB), terabyte, petabyte.	Fill-in-the-Blank	Byte	BYTE
French for “hide.” A storage area where frequently accessed data may be kept for rapid access. There are three main types of cache	Fill-in-the-Blank	Cache	CACHE
Stands for Compact Disk – Read Only Memory. A plastic disk able to hold approximately 650MB to 700MB of data. A common storage medium for data.	Fill-in-the-Blank	CD-ROM	CD-ROM
As in other fields, a record of the chronological history of (electronic) evidence.	Fill-in-the-Blank	Chain of Custody	CHAIN OF CUSTODY
What is a short, repeated sequence used in cryptographic attacks called?	Multiple Choice	Cipher	Key
What is a short, repeated sequence used in cryptographic attacks called?	Fill-in-the-Blank	Nonce	NONCE
What is the most common form of social engineering where attackers pretend to be from legitimate organizations, usually over email?	Fill-in-the-Blank	Phishing	PHISHING
Which attack involves the hacker predicting the sequence number of TCP packets between the client and server?	Fill-in-the-Blank	Sequence prediction	SEQUENCE PREDICTION
Which type of malware provides a backdoor for unauthorized access to a system?	Fill-in-the-Blank	Trojan	TROJAN
An attacker who deceives individuals into providing sensitive data by posing as a trustworthy entity via telephone is using:	Fill-in-the-Blank	Vishing	VISHING
In which type of attack does an attacker exploit a vulnerability without prior knowledge of the vulnerability?	Fill-in-the-Blank	Zero-day attack	ZERO-DAY ATTACK
As in other fields, a record of the chronological history of (electronic) evidence.	Multiple Choice	Chain of Custody	Cluster

Also known as allocation blocks, a cluster is a contiguous group of sectors that is the smallest amount of space assigned to a file by an operating system such as Microsoft Windows. Clusters generally range in size from 4 sectors to 64 sectors.	Multiple Choice	Cluster	Compressed file, zipped file
A file that has been encoded using less space than the original file in its uncompressed state. A zipped file may contain more than on compressed file.	Multiple Choice	Compressed file, zipped file	Computer Forensics
electronic imaging, electronic discovery, forensic analysis of discovered information, preparation of information in a manner useful to the client or court, presentation of findings to the client or attorney, such as in written, oral and/or electronic reports, testimony in a court of law, when necessary, by an expert witness, including deposition and jury trial.	Multiple Choice	Computer Forensics	Cookie
In Internet or browser usage, a small file accessed by a web browser and written to the user's computer. A shortened form of the term, "magic cookie," cookies are used for tracking, authenticating, and maintaining information about users, generally to ease interaction between a website and a user. Cookies stored on a user's computer often contain the times and dates that the user accessed a given website.	Multiple Choice	Cookie	Corrupt Data, Corrupt File
A file that is damaged. Damage may have occurred inadvertently during transmission, copying, through operating system error, physical damage to the media on which the data was stored, or though other means.	Multiple Choice	Corrupt Data, Corrupt File	Darkweb
A part of the Deep Web that is used for anonymous and semi-anonymous communication and websites and which generally requires TOR or the equivalent for access.	Multiple Choice	Darkweb	Deduplication ("De-duping")
A process performed on a collection of data from multiple sources, whether from several files, several different locations or computers, or from within a collective email file. The process is designed to yield one unique copy of ant given record, file, or email.	Multiple Choice	Deduplication ("De-duping")	Deep Web

A part of the Internet (about 95% of it) that is not indexed by Google, Bing, or the like and is generally not accessible by web browsers such as Internet Explorer, Edge, and Chrome. Includes databases, internal networks, communities and resources.	Multiple Choice	Deep Web	Default
A setting or value automatically assigned without user intervention.	Multiple Choice	Default	Delete
To cause a file or email to move from an active or live state to an ambient state, usually performed by moving a file to the trash or recycle bin on a computer, or by selecting a file and then pressing the delete [Del] key. Deleted files, while generally not removed from the computer until overwritten, are nonetheless invisible to the user.	Multiple Choice	Delete	Desktop computer
A stand-alone computer that is generally designed to be connected to a keyboard and monitor (although some desktop computers, such as the Macintosh iMac, have the monitor integrated), as distinct from a laptop, and from a Server.	Multiple Choice	Desktop computer	Directory
A hierarchically arranged listing of files stored on a hard disk or other media. The topmost directory is the root directory. Subsequent directories nested within the root directory are called subdirectories. In a GUI, a directory appears as a file folder.	Multiple Choice	Directory	Disk
Which attack involves manipulating a system's logical operations to execute unintended commands?	Multiple Choice	Logic bomb	Buffer overflow
What kind of attack exploits the differences between the application layer and transport layer's view of data?	Multiple Choice	Injection attack	Desynchronization attack
An attacker is exploiting the time gap between the trigger of a condition and its mitigation. This is known as a:	Multiple Choice	Logic bomb	Race condition
Which attack occurs when an attacker "piggybacks" behind an authorized person to gain physical access to a restricted area?	Multiple Choice	Phishing	Tailgating
What type of attack takes place when the attacker tricks the victim into running a malicious file, believing it's a video or image file?	Multiple Choice	Masquerading	Trojan horse
Which malware primarily logs a user's keystrokes?	Multiple Choice	Ransomware	Spyware

A technique where an attacker manipulates the inputs of a web application to retrieve arbitrary data from the database is known as?	Multiple Choice	CSRF	Buffer overflow
Also known as allocation blocks, a cluster is a contiguous group of sectors that is the smallest amount of space assigned to a file by an operating system such as Microsoft Windows. Clusters generally range in size from 4 sectors to 64 sectors.	Fill-in-the-Blank	Cluster	CLUSTER
electronic imaging, electronic discovery, forensic analysis of discovered information, preparation of information in a manner useful to the client or court, presentation of findings to the client or attorney, such as in written, oral and/or electronic reports, testimony in a court of law, when necessary, by an expert witness, including deposition and jury trial.	Fill-in-the-Blank	Computer Forensics	COMPUTER FORENSICS
In Internet or browser usage, a small file accessed by a web browser and written to the user's computer. A shortened form of the term, "magic cookie," cookies are used for tracking, authenticating, and maintaining information about users, generally to ease interaction between a website and a user. Cookies stored on a user's computer often contain the times and dates that the user accessed a given website.	Fill-in-the-Blank	Cookie	COOKIE
A part of the Deep Web that is used for anonymous and semi-anonymous communication and websites and which generally requires TOR or the equivalent for access.	Fill-in-the-Blank	Darkweb	DARKWEB
A part of the Internet (about 95% of it) that is not indexed by Google, Bing, or the like and is generally not accessible by web browsers such as Internet Explorer, Edge, and Chrome. Includes databases, internal networks, communities and resources.	Fill-in-the-Blank	Deep Web	DEEP WEB
A setting or value automatically assigned without user intervention.	Fill-in-the-Blank	Default	DEFAULT

To cause a file or email to move from an active or live state to an ambient state, usually performed by moving a file to the trash or recycle bin on a computer, or by selecting a file and then pressing the delete [Del] key. Deleted files, while generally not removed from the computer until overwritten, are nonetheless invisible to the user.	Fill-in-the-Blank	Delete	DELETE
A hierarchically arranged listing of files stored on a hard disk or other media. The topmost directory is the root directory. Subsequent directories nested within the root directory are called subdirectories. In a GUI, a directory appears as a file folder.	Fill-in-the-Blank	Directory	DIRECTORY
What type of attack involves intercepting and altering communications between two parties without detection?	Fill-in-the-Blank	Man-in-the-Middle	MAN-IN-THE-MIDDLE
An attacker is exploiting the time gap between the trigger of a condition and its mitigation. This is known as a:	Fill-in-the-Blank	Race condition	RACE CONDITION
A technique where an attacker manipulates the inputs of a web application to retrieve arbitrary data from the database is known as?	Fill-in-the-Blank	SQL injection	SQL INJECTION
Which attack occurs when an attacker "piggybacks" behind an authorized person to gain physical access to a restricted area?	Fill-in-the-Blank	Tailgating	TAILGATING
Which type of attack is described as the automated discovery of weak passwords in a system?	Multiple Choice	Brute Force Attack	Dictionary Attack
Generally a hard disk. Floppy diskettes are often referred to as disks.	Multiple Choice	Disk	Disk cache
RAM used to speed up access to stored data. May be part of a computer's RAM, or may be RAM integrated into the disk drive itself.	Multiple Choice	Disk cache	Disk Mirroring
Data copied to another hard disk or to another area on the same hard disk in order to have a complete, identical copy of the original.	Multiple Choice	Disk Mirroring	Dot

A period that is used as part of a filename, or as part of a Web address. It is pronounced “dot.” For instance, a file named “glossary.doc” would be spoken as “glossary dot doc.” Similarly, a web address, such as www.yahoo.com would be spoken as “W-W-W dot yahoo dot com.”	Multiple Choice	Dot	Download
The transfer of data between two computers, generally over a network. One may download a file from the Internet, for instance. Commonly used as a misnomer for “copy.” For instance, a common mistake is to say that one downloaded a file from a diskette, when a file is copied (not downloaded) from a diskette.	Multiple Choice	Download	E-mail
Electronic mail. Messages transmitted over a computer network or networks, directed to a given user, either individually or in bulk. Email may be stored in a largely text format, or in an encrypted form. Microsoft Outlook stores email messages in an encrypted file; most other email programs store messages primarily as text.	Multiple Choice	E-mail	Encryption
A process to render a file unreadable to unauthorized persons or devices.	Multiple Choice	Encryption	Exabyte
1024 Petabytes	Multiple Choice	Exabyte	Extension, File Extension
Part of a file’s name, usually follows a “dot,” or period in a file name. Some operating systems, such a Microsoft Windows, depend on the extension to know what program is used to open the given file. Microsoft word documents, for instance have “.doc” as their extension.	Multiple Choice	Extension, File Extension	File Attribute
Properties associated with a file that are kept with the file directory listing. Such attributes include the date and time the file was last accessed, created, or modified,	Multiple Choice	File Attribute	File Server
An attack where an unauthorized user attempts to become a part of a network by pretending to be a trusted device is:	Multiple Choice	ARP poisoning	MAC spoofing
In which attack is the attacker intercepting a public key exchange and then providing the client and server with a fraudulent key?	Multiple Choice	Replay Attack	Man-in-the-Middle

Which malware uses encryption to lock user data and demand a payment to decrypt it?	Multiple Choice	Worm	Ransomware
An attacker uses previously captured network traffic in an attempt to resend or replay it. This describes which type of attack?	Multiple Choice	ARP poisoning	Replay attack
An attacker sends a ping to a broadcast address to have all devices reply to the ping, overwhelming the system. What is this attack called?	Multiple Choice	Ping of Death	Smurf attack
Which malware typically does not need user intervention to propagate and spread?	Multiple Choice	Virus	Worm
Which vulnerability scan takes place from outside an organization's network?	Multiple Choice	Internal scan	Passive scan
An attack where an attacker tricks users into revealing information by posing as a legitimate website is known as:	Multiple Choice	Phishing	Spoofing
Which of the following best describes a scenario where an employee unintentionally installs malware by opening an email attachment?	Multiple Choice	Insider Threat	Logic Bomb
Which type of attack is described as the automated discovery of weak passwords in a system?	Fill-in-the-Blank	Brute Force Attack	BRUTE FORCE ATTACK
Generally a hard disk. Floppy diskettes are often referred to as disks.	Fill-in-the-Blank	Disk	DISK
RAM used to speed up access to stored data. May be part of a computer's RAM, or may be RAM integrated into the disk drive itself.	Fill-in-the-Blank	Disk cache	DISK CACHE
Data copied to another hard disk or to another area on the same hard disk in order to have a complete, identical copy of the original.	Fill-in-the-Blank	Disk Mirroring	DISK MIRRORING
A period that is used as part of a filename, or as part of a Web address. It is pronounced "dot." For instance, a file named "glossary.doc" would be spoken as "glossary dot doc." Similarly, a web address, such as www.yahoo.com would be spoken as "W-W-W dot yahoo dot com."	Fill-in-the-Blank	Dot	DOT

The transfer of data between two computers, generally over a network. One may download a file from the Internet, for instance. Commonly used as a misnomer for “copy.” For instance, a common mistake is to say that one downloaded a file from a diskette, when a file is copied (not downloaded) from a diskette.	Fill-in-the-Blank	Download	DOWNLOAD
Which of the following best describes a scenario where an employee unintentionally installs malware by opening an email attachment?	Fill-in-the-Blank	Drive-by Download	DRIVE-BY DOWNLOAD
Electronic mail. Messages transmitted over a computer network or networks, directed to a given user, either individually or in bulk. Email may be stored in a largely text format, or in an encrypted form. Microsoft Outlook stores email messages in an encrypted file; most other email programs store messages primarily as text.	Fill-in-the-Blank	E-mail	E-MAIL
A process to render a file unreadable to unauthorized persons or devices.	Fill-in-the-Blank	Encryption	ENCRYPTION
1024 Petabytes	Fill-in-the-Blank	Exabyte	EXABYTE
Which vulnerability scan takes place from outside an organization's network?	Fill-in-the-Blank	External scan	EXTERNAL SCAN
Properties associated with a file that are kept with the file directory listing. Such attributes include the date and time the file was last accessed, created, or modified,	Fill-in-the-Blank	File Attribute	FILE ATTRIBUTE
A computer on a network that is used to store files from and for multiple users on the network. A file server may also be used as an Application Server, a Backup Server, or as a Mail Server. May be used as a backup for the computers on the network.	Fill-in-the-Blank	File Server	FILE SERVER
An attack where an unauthorized user attempts to become a part of a network by pretending to be a trusted device is:	Fill-in-the-Blank	MAC spoofing	MAC SPOOFING
An attack where an attacker tricks users into revealing information by posing as a legitimate website is known as:	Fill-in-the-Blank	Pharming	PHARMING
Which malware uses encryption to lock user data and demand a payment to decrypt it?	Fill-in-the-Blank	Ransomware	RANSOMWARE

An attacker sends a ping to a broadcast address to have all devices reply to the ping, overwhelming the system. What is this attack called?	Fill-in-the-Blank	Smurf attack	SMURF ATTACK
Which malware typically does not need user intervention to propagate and spread?	Fill-in-the-Blank	Worm	WORM
A computer on a network that is used to store files from and for multiple users on the network. A file server may also be used as an Application Server, a Backup Server, or as a Mail Server. May be used as a backup for the computers on the network.	Multiple Choice	File Server	File signature
Information contained within a file that identifies its type, even though the file's extension may have been altered.	Multiple Choice	File signature	File slack
Information at the end of a cluster that has not been completely filled, or overwritten by a file. The file may end before the end of the cluster, hence the cluster may contain data from a previous file	Multiple Choice	File slack	Filename
The name of a file. Sometimes refers to the name of a file minus its extension.	Multiple Choice	Filename	Floppy diskette, floppy
A square-shaped enclosure holding a rotating flexible plastic magnetically coated disk used for data storage. At this writing, the 8" and 5.25" variety of floppy diskette is obsolete, and the 3.5" variety is approaching obsolescence. The most common floppy diskettes hold 1.44 MB of data.	Multiple Choice	Floppy diskette, floppy	Folder
in a GUI, a folder is the representation of a directory and may contain files and other, nested folders.	Multiple Choice	Folder	Forensic image
A forensically sound and complete copy of a hard drive or other digital media, generally intended for use as evidence. Such copies include unallocated space, slack space, and boot record. A forensic image is often accompanied by a calculated Hash signature to validate that the image is an exact duplicate of the original.	Multiple Choice	Forensic image	GIF
A common format for storage of digital images. An acronym for Graphic Interchange Format. Pronounced "Jiff." GIFs have the file extension "gif"	Multiple Choice	GIF	Gigabyte (GB)

1024 megabytes (MB), or 1,048,576 KB, or 1,073,741,824 bytes. Often considered (incorrectly) to be one billion bytes.	Multiple Choice	Gigabyte (GB)	GUI
Graphical User Interface. An image and icon-based interface designed to make manipulation of computer data easy. Common GUIs are Microsoft Windows and the Macintosh OS.	Multiple Choice	GUI	Hard disk
Currently the primary storage medium for data on most computers, Consists of a sealed chassis containing a rapidly spinning metal-coated platter, or stack of platters that are magnetically encoded as data is written to them by enclosed magnetic read/write heads.	Multiple Choice	Hard disk	Hash, hash value
A hash is a number generated from a string of text. A hash value may be generated for a single file, or for an entire hard disk. A matching hash virtually guarantees that a copy is identical to the original. It does not absolutely guarantee this.	Multiple Choice	Hash, hash value	HTML
What term describes software that displays unwanted advertising?	Multiple Choice	Worm	Adware
Which attack involves reflecting traffic off of third-party systems to amplify the attack?	Multiple Choice	Ping flood	Amplification attack
Which attack exploits vulnerabilities in a DNS server to divert traffic from legitimate servers to fake ones?	Multiple Choice	ARP poisoning	DNS spoofing
What is the term for hidden malicious functionality triggered by a specific condition?	Multiple Choice	Spyware	Logic bomb
Which of the following is NOT a type of social engineering attack?	Multiple Choice	Tailgating	Vishing
Which attack involves subverting the trust relationship between user and website by forging the website's SSL certificate?	Multiple Choice	ARP poisoning	CSRF
Which type of malware remains active in the RAM and does not write any files to the disk?	Multiple Choice	Ransomware	Rootkit
Which attack involves overwhelming a system by rapidly establishing a large number of connections?	Multiple Choice	Buffer overflow	DNS amplification
Which attack involves subverting the trust relationship between user and website by forging the website's SSL certificate?	Fill-in-the-Blank	Certificate spoofing	CERTIFICATE SPOOFING

Which attack exploits vulnerabilities in a DNS server to divert traffic from legitimate servers to fake ones?	Fill-in-the-Blank	DNS spoofing	DNS SPOOFING
Information contained within a file that identifies its type, even though the file's extension may have been altered.	Fill-in-the-Blank	File signature	FILE SIGNATURE
Information at the end of a cluster that has not been completely filled, or overwritten by a file. The file may end before the end of the cluster, hence the cluster may contain data from a previous file	Fill-in-the-Blank	File slack	FILE SLACK
Which type of malware remains active in the RAM and does not write any files to the disk?	Fill-in-the-Blank	Fileless malware	FILELESS MALWARE
The name of a file. Sometimes refers to the name of a file minus its extension.	Fill-in-the-Blank	Filename	FILENAME
in a GUI, a folder is the representation of a directory and may contain files and other, nested folders.	Fill-in-the-Blank	Folder	FOLDER
A forensically sound and complete copy of a hard drive or other digital media, generally intended for use as evidence. Such copies include unallocated space, slack space, and boot record. A forensic image is often accompanied by a calculated Hash signature to validate that the image is an exact duplicate of the original.	Fill-in-the-Blank	Forensic image	FORENSIC IMAGE
A common format for storage of digital images. An acronym for Graphic Interchange Format. Pronounced "Jiff." GIFs have the file extension "gif"	Fill-in-the-Blank	GIF	GIF
1024 megabytes (MB), or 1,048,576 KB, or 1,073,741,824 bytes. Often considered (incorrectly) to be one billion bytes.	Fill-in-the-Blank	Gigabyte (GB)	GIGABYTE (GB)
Graphical User Interface. An image and icon-based interface designed to make manipulation of computer data easy. Common GUIs are Microsoft Windows and the Macintosh OS.	Fill-in-the-Blank	GUI	GUI
Currently the primary storage medium for data on most computers, Consists of a sealed chassis containing a rapidly spinning metal-coated platter, or stack of platters that are magnetically encoded as data is written to them by enclosed magnetic read/write heads.	Fill-in-the-Blank	Hard disk	HARD DISK

What refers to software or hardware used to capture keystrokes?	Fill-in-the-Blank	Keylogger	KEYLOGGER
What is the term for hidden malicious functionality triggered by a specific condition?	Fill-in-the-Blank	Logic bomb	LOGIC BOMB
Which type of attack involves an attacker sending messages on a network to impersonate a different machine?	Multiple Choice	ARP poisoning	Replay attack
An authoring language, written in text that is used to create documents for access on the World Wide Web. Such documents may be web pages, or otherwise enhanced documents or email messages. Stands fro Hypertext Markup Language.	Multiple Choice	HTML	Instant Messaging
Abbreviated as IM. A text-based electronic communication in real time. It is similar to a telephone call in its immediacy; it is different in that it is generally text-based.	Multiple Choice	Instant Messaging	IP Address (IPv4)
An electronic identifier for a specific computer or device on the World Wide Web or other (internal or external) electronic network using the TCP/IP protocol. An IP address is a series of four numbers separated by periods (“dots”), Each number is a value from 0 to 255. An example could be 192.168.55.207 “IP” stands for “Internet Protocol.” This identifier support 340 trillion addresses.	Multiple Choice	IP Address (IPv4)	IP Address (IPv6)
An electronic identifier for a specific computer or device on the World Wide Web or other (internal or external) electronic network using the TCP/IP protocol. An _____ address is a series of eight groups of four hexadecimal digits with each groups being separated by colons.	Multiple Choice	IP Address (IPv6)	ISP
A provider of access to or connection to the Internet. Some large _____'s include Earthlink, Yahoo, Roadrunner, SBC Global.	Multiple Choice	ISP	JPEG
A common format for storage of digital images. An acronym for Joint Photographic Experts Group. Pronounced “jay-peg.” JPEGs have the file extension, “jpg”	Multiple Choice	JPEG	Jumplists

Lists of recently modified documents in certain programs in Windows from Windows 7 onward. May be used to help determine a history of use of certain files that may be expanded beyond the standard file date attributes.	Multiple Choice	Jumplists	Keylogger
A program or device designed to keep a record of the keys types on a computer. May be used for monitoring, or espionage, such as to collect passwords. Some keyloggers may be accessed remotely.	Multiple Choice	Keylogger	Keyword search
A common technique used in computer forensic and electronic discovery, a keyword search is usually performed to find and identify every instance on a computer or other media of a given word or phrase, even if said word or phrase occurs in unallocated space or in deleted files.	Multiple Choice	Keyword search	Kilobyte (KB)
1024 bytes. Used to measure both storage and memory. Often considered (incorrectly) to be one thousand bytes.	Multiple Choice	Kilobyte (KB)	LNK files
Windows creates LNK files when a user opens a local or remote file, and references both the original file along with date and time attributes about a file that has been opened.	Multiple Choice	LNK files	Log files, or logfile
In which attack does an attacker insert themselves between the client and server to capture sensitive information?	Multiple Choice	Man-in-the-Browser	DDoS
Which malware is intentionally installed by an authorized user and can be used to access systems remotely?	Multiple Choice	RAT (Remote Access Trojan)	Worm
Which attack exploits JavaScript vulnerabilities in web browsers to execute unauthorized actions?	Multiple Choice	SQL injection	Cross-Site Scripting (XSS)
An attacker who is trying to guess a password using a system-generated list of possibilities is performing a:	Multiple Choice	Brute force attack	Dictionary attack
Which of the following is NOT a primary characteristic of a worm?	Multiple Choice	Replicates itself	Requires a host file to spread
An attacker who intercepts a session to take over or hijack the session is performing a:	Multiple Choice	Replay attack	Session hijacking

Which of the following attacks primarily exploits human behavior to gain unauthorized access?	Multiple Choice	Buffer overflow	Spear phishing
A form of malware that replicates itself and infects the boot sector of storage devices is known as:	Multiple Choice	Worm	Spyware
What type of malware provides unauthorized remote access to a victim's system?	Multiple Choice	Trojan	Worm
Which attack aims to render a website or service inoperable by overwhelming it with traffic?	Multiple Choice	SYN flood	Phishing
Which type of attack involves an attacker sending messages on a network to impersonate a different machine?	Fill-in-the-Blank	ARP poisoning	ARP POISONING
A form of malware that replicates itself and infects the boot sector of storage devices is known as:	Fill-in-the-Blank	Boot sector virus	BOOT SECTOR VIRUS
An attacker who is trying to guess a password using a system-generated list of possibilities is performing a:	Fill-in-the-Blank	Dictionary attack	DICTIONARY ATTACK
An authoring language, written in text that is used to create documents for access on the World Wide Web. Such documents may be web pages, or otherwise enhanced documents or email messages. Stands fro Hypertext Markup Language.	Fill-in-the-Blank	HTML	HTML
Abbreviated as IM. A text-based electronic communication in real time. It is similar to a telephone call in its immediacy; it is different in that it is generally text-based.	Fill-in-the-Blank	Instant Messaging	INSTANT MESSAGING
A provider of access to or connection to the Internet. Some large _____'s include Earthlink, Yahoo, Roadrunner, SBC Global.	Fill-in-the-Blank	ISP	ISP
A common format for storage of digital images. An acronym for Joint Photographic Experts Group. Pronounced “jay-peg.” JPEGs have the file extension, “jpg”	Fill-in-the-Blank	JPEG	JPEG
Lists of recently modified documents in certain programs in Windows from Windows 7 onward. May be used to help determine a history of use of certain files that may be expanded beyond the standard file date attributes.	Fill-in-the-Blank	Jumplists	JUMPLISTS

A common technique used in computer forensic and electronic discovery, a keyword search is usually performed to find and identify every instance on a computer or other media of a given word or phrase, even if said word or phrase occurs in unallocated space or in deleted files.	Fill-in-the-Blank	Keyword search	KEYWORD SEARCH
1024 bytes. Used to measure both storage and memory. Often considered (incorrectly) to be one thousand bytes.	Fill-in-the-Blank	Kilobyte (KB)	KILOBYTE (KB)
Windows creates LNK files when a user opens a local or remote file, and references both the original file along with date and time attributes about a file that has been opened.	Fill-in-the-Blank	LNK files	LNK FILES
Which vulnerability might be exploited by an attacker sending input data that is too large for a program to handle?	Multiple Choice	Buffer overflow	SQL injection
In which attack does the attacker exploit relationships between web application users to steal cookies?	Multiple Choice	Cross-site scripting (XSS)	SQL injection
A record kept by many applications and operating systems of various activities by saving to a file – the logfile.	Multiple Choice	Log files, or logfile	MAC dates
File attributes in the Windows operating system. Thee MAC dates are the date a file was last Modifies, Last Accessed, and Created.	Multiple Choice	MAC dates	Mail Server
A server on a network that processes incoming and outgoing electronic communications, especially email. A _____ generally has security policies in place to allow only authenticated users access to given email communication. The _____ may store a copy of users' data in various forms, or may not store copies of users' data. A _____ may be utilized for multiple functions, including as a File Server, Application Server, or Backup Server.	Multiple Choice	Mail Server	Master File Table, or MFT

In an NTFS file structure (used in most versions of Windows from 1993-2014 (so far). The MFT contains substantial metadata about all files in a given volume, including file physical locations, MAC dates (times), file permissions, file size, the file's parent directory, entry modification time, and at times, the entire content of small files.	Multiple Choice	Master File Table, or MFT	Megabyte (MB)
1024 Kilobytes (KB), or 1,048,576 bytes. Often considered (incorrectly) to be one million bytes.	Multiple Choice	Megabyte (MB)	Memory Cache
Also known as RAM cache, it is high-speed memory designed to store frequently accessed or recently accessed data for quick use. On the Macintosh, RAM cache may also be disk cache.	Multiple Choice	Memory Cache	Native format, native environment
The original configuration or program in which a file or other data was produced.	Multiple Choice	Native format, native environment	Network
A group of computers electronically linked so as to be able to share files or other resources, or for electronic communication. The World Wide Web is a particularly large network.	Multiple Choice	Network	NTFS
NEW Technology FIle System. An operating system developed by Microsoft and released in 1993 with Windows NT 3.1. It has subsequently been used in versions of Windows through Windows 8.1. Previous versions of Windows had been dependent on the DOS operating system.	Multiple Choice	NTFS	Operating System, OS
The suite of programs that allow a computer to operate. The OS controls signals from and to input devices (such as mouse, keyboard, microphone), peripherals (such as hard disks, CD-ROM drives, and printers), output devices (such as monitors and speakers) and performs the basic functions needed for a computer to operate. Common operating systems include Windows XP, Macintosh OS X, and Linux.	Multiple Choice	Operating System, OS	Partition
A logical delineation on a disk drive such that a single drive acts as two, smaller disk drives.	Multiple Choice	Partition	PDF

Which attack involves the attacker making a copy of a system's authentication token to use it later?	Multiple Choice	Pass the hash	Replay attack
An Adobe Acrobat document. A common format for graphic and text files that is not easily altered. Stands for Portable Document Format.	Multiple Choice	PDF	Petabyte
Which attack leverages a botnet to flood a system with requests, making it unavailable to its users?	Multiple Choice	DoS	DDoS
Which attack involves an attacker redirecting a user's web traffic to a malicious site by poisoning the local DNS cache?	Multiple Choice	Man-in-the-Middle	DNS poisoning
Which of the following types of malware can hide its presence or the presence of other malware?	Multiple Choice	Spyware	Rootkit
Which vulnerability might be exploited if user input isn't properly sanitized before being processed by a database?	Multiple Choice	Cross-site scripting	SQL injection
Which attack involves the attacker creating thousands of sessions with a target, but never completing the three-way handshake?	Multiple Choice	Ping flood	SYN flood
Which of the following attempts to make a machine or network resource unavailable by flooding it with illegitimate requests?	Multiple Choice	Man-in-the-Middle	CSRF
Which type of malware disguises its malicious activity by appearing as a legitimate software?	Multiple Choice	Spyware	Adware
Which type of social engineering attack is highly targeted, often using detailed research on the victim?	Multiple Choice	Baiting	Vishing
Which vulnerability might be exploited by an attacker sending input data that is too large for a program to handle?	Fill-in-the-Blank	Buffer overflow	BUFFER OVERFLOW
Which attack leverages a botnet to flood a system with requests, making it unavailable to its users?	Fill-in-the-Blank	DDoS	DDOS
Which attack involves an attacker redirecting a user's web traffic to a malicious site by poisoning the local DNS cache?	Fill-in-the-Blank	DNS poisoning	DNS POISONING
File attributes in the Windows operating system. Thee MAC dates are the date a file was last Modifies, Last Accessed, and Created.	Fill-in-the-Blank	MAC dates	MAC DATES

A server on a network that processes incoming and outgoing electronic communications, especially email. A _____ generally has security policies in place to allow only authenticated users access to given email communication. The _____ may store a copy of users' data in various forms, or may not store copies of users' data. A _____ may be utilized for multiple functions, including as a File Server, Application Server, or Backup Server.	Fill-in-the-Blank	Mail Server	MAIL SERVER
1024 Kilobytes (KB), or 1,048,576 bytes. Often considered (incorrectly) to be one million bytes.	Fill-in-the-Blank	Megabyte (MB)	MEGABYTE (MB)
Also known as RAM cache, it is high-speed memory designed to store frequently accessed or recently accessed data for quick use. On the Macintosh, RAM cache may also be disk cache.	Fill-in-the-Blank	Memory Cache	MEMORY CACHE
A group of computers electronically linked so as to be able to share files or other resources, or for electronic communication. The World Wide Web is a particularly large network.	Fill-in-the-Blank	Network	NETWORK
NEW Technology FIle System. An operating system developed by Microsoft and released in 1993 with Windows NT 3.1. It has subsequently been used in versions of Windows through Windows 8.1. Previous versions of Windows had been dependent on the DOS operating system.	Fill-in-the-Blank	NTFS	NTFS
A logical delineation on a disk drive such that a single drive acts as two, smaller disk drives.	Fill-in-the-Blank	Partition	PARTITION
Which attack involves the attacker making a copy of a system's authentication token to use it later?	Fill-in-the-Blank	Pass the hash	PASS THE HASH
An Adobe Acrobat document. A common format for graphic and text files that is not easily altered. Stands for Portable Document Format.	Fill-in-the-Blank	PDF	PDF
Which type of social engineering attack is highly targeted, often using detailed research on the victim?	Fill-in-the-Blank	Spear phishing	SPEAR PHISHING

Which attack involves the attacker creating thousands of sessions with a target, but never completing the three-way handshake?	Fill-in-the-Blank	SYN flood	SYN FLOOD
1024 Terabytes, or 1,125,899,906,900,000 bytes – a bit more than a quadrillion bytes	Multiple Choice	Petabyte	Program
Also known as an Application, or (sometimes) Software. The software used to access and create files or documents. Microsoft Word and Corel WordPerfect are applications that work with word processing documents. Microsoft Excel and Lotus 1-2-3 are applications that work with or spreadsheets.	Multiple Choice	Program	Protocol
An agreed-upon standard format for communicating, connecting, or transferring data between two computers or devices. There are many communications protocols, such as TCP (Transmission Control Protocol).	Multiple Choice	Protocol	RAM
Random Access Memory. Computer chips that store digital data in electronic form.	Multiple Choice	RAM	Registry Hives
The Windows registry is made up of sub files called “hives.” Individual Windows User settings and some history of usage are kept in the various hives and may be updated as the computer is used.	Multiple Choice	Registry Hives	SAM Hive
“Security Account Manager” that stores Users’ passwords	Multiple Choice	SAM Hive	Sector
The basic and smallest unit of data storage on a hard disk or other electronic media. Generally consists of one contiguous area able to hold 512 bytes of data.	Multiple Choice	Sector	Server
A computer on a network that shares data with other computers on the network.	Multiple Choice	Server	Shadow Volume
Also known as Shadow Copy, Volume Snapshot Service, Volume Shadow Copy Service, or VSS, is included with Microsoft Windows and makes automated backup copies of some files and operating system components from time to time on NTFS-based computers.	Multiple Choice	Shadow Volume	Software
Anything that can be stored electronically. Includes programs, files, and data.	Multiple Choice	Software	Software Hive
Which of the following attacks takes advantage of the communication between web applications?	Multiple Choice	Watering hole attack	CSRF

Which of the following attacks uses ICMP packets to flood a target, rendering it unresponsive?	Multiple Choice	Ping of Death	ICMP flood
An attacker who captures a token to later authenticate as a genuine user is attempting a:	Multiple Choice	Pass the token attack	Replay attack
An attacker who tricks a user into running a malicious script on a webpage is using which technique?	Multiple Choice	Drive-by download	XSS
Which type of malware primarily displays unwanted advertisements to the user?	Multiple Choice	Ransomware	Spyware
Which type of attack leverages a botnet to reflect attacks off third-party servers to mask the source of the attack and amplify its impact?	Multiple Choice	Reflected attack	SYN flood
Which type of malware is typically installed without the user's knowledge and gathers information about the user?	Multiple Choice	Adware	Worm
Which type of attack often involves fake antennas to intercept cellular traffic?	Multiple Choice	Phishing	Man-in-the-Middle
Which type of malware primarily displays unwanted advertisements to the user?	Fill-in-the-Blank	Adware	ADWARE
Which type of attack leverages a botnet to reflect attacks off third-party servers to mask the source of the attack and amplify its impact?	Fill-in-the-Blank	Amplification attack	AMPLIFICATION ATTACK
Which of the following attacks takes advantage of the communication between web applications?	Fill-in-the-Blank	CSRF	CSRF
Which of the following attacks uses ICMP packets to flood a target, rendering it unresponsive?	Fill-in-the-Blank	ICMP flood	ICMP FLOOD
Which type of attack often involves fake antennas to intercept cellular traffic?	Fill-in-the-Blank	IMSI catcher	IMSI CATCHER
What type of attack involves changing the MAC address of an attacker's network interface card to impersonate another device on the network?	Fill-in-the-Blank	MAC	MAC
1024 Terabytes, or 1,125,899,906,900,000 bytes – a bit more than a quadrillion bytes	Fill-in-the-Blank	Petabyte	PETABYTE

Also known as an Application, or (sometimes) Software. The software used to access and create files or documents. Microsoft Word and Corel WordPerfect are applications that work with word processing documents. Microsoft Excel and Lotus 1-2-3 are applications that work with or spreadsheets.	Fill-in-the-Blank	Program	PROGRAM
An agreed-upon standard format for communicating, connecting, or transferring data between two computers or devices. There are many communications protocols, such as TCP (Transmission Control Protocol).	Fill-in-the-Blank	Protocol	PROTOCOL
Random Access Memory. Computer chips that store digital data in electronic form.	Fill-in-the-Blank	RAM	RAM
The Windows registry is made up of sub files called “hives.” Individual Windows User settings and some history of usage are kept in the various hives and may be updated as the computer is used.	Fill-in-the-Blank	Registry Hives	REGISTRY HIVES
An attacker who captures a token to later authenticate as a genuine user is attempting a:	Fill-in-the-Blank	Replay attack	REPLAY ATTACK
“Security Account Manager” that stores Users’ passwords	Fill-in-the-Blank	SAM Hive	SAM HIVE
The basic and smallest unit of data storage on a hard disk or other electronic media. Generally consists of one contiguous area able to hold 512 bytes of data.	Fill-in-the-Blank	Sector	SECTOR
A computer on a network that shares data with other computers on the network.	Fill-in-the-Blank	Server	SERVER
Also known as Shadow Copy, Volume Snapshot Service, Volume Shadow Copy Service, or VSS, is included with Microsoft Windows and makes automated backup copies of some files and operating system components from time to time on NTFS-based computers.	Fill-in-the-Blank	Shadow Volume	SHADOW VOLUME
Anything that can be stored electronically. Includes programs, files, and data.	Fill-in-the-Blank	Software	SOFTWARE
Which type of malware is typically installed without the user’s knowledge and gathers information about the user?	Fill-in-the-Blank	Spyware	SPYWARE
An attacker who tricks a user into running a malicious script on a webpage is using which technique?	Fill-in-the-Blank	XSS	XSS

What attack involves the attacker setting up a fake Wi-Fi access point to intercept data?	Multiple Choice	Evil twin	Rogue AP
A collection of software tools used by an attacker to hide the actions or presence of other types of malicious software is known as:	Multiple Choice	Rootkit	Trojan horse
Which attack can be prevented by disabling ICMP on your router?	Multiple Choice	Smurf attack	CSRF
Contains software and Windows settings	Multiple Choice	Software Hive	Spoliation
Intentional, negligent, or accidental destruction or alteration of evidence.	Multiple Choice	Spoliation	Standalone
A computer that is not connected to a network.	Multiple Choice	Standalone	Steganography
A means of writing hidden messages such that only the intended recipient knows of its existence. An modern example may be the replacing a few pixels of a digital image with a digital message. The slight change in the image may be unnoticeable to a person who does not know where in the image to look. Older forms of Steganography, which means “covered writing” in Greek, date back more than 2.000 years.	Multiple Choice	Steganography	System Hive
Contains information about the Windows system setup, mounted devices, alternative configurations for hardware drivers and services.	Multiple Choice	System Hive	TCP/IP
A suite of communications protocols used to allow communication between computers on a network, such as on the Internet. Stands fro Transmission Control Protocol / Internet Protocol.	Multiple Choice	TCP/IP	Terabyte
1024 Gigabytes, or 1,099,511,627,800 bytes – a bit more than one trillion bytes.	Multiple Choice	Terabyte	Thumbnail
Generally stands for a small, low-resolution image that takes the place of an original full-resolution image. Thumbnails do not generally contain metadata with GPS location or date of original creation of the source image.	Multiple Choice	Thumbnail	TOR
Stands for “The Onion Router. TOR is US Government-created (through the US Naval Research Lab) software designed to allow anonymous or semi-anonymous communication.	Multiple Choice	TOR	Unallocated

The area on a hard disk or other media that is not (or is no longer) assigned to a file by the Operating System. May contain intact deleted files, remnants thereof, or other data.	Multiple Choice	Unallocated	User
Which type of vulnerability scan uses the database of known vulnerability signatures to identify threats?	Multiple Choice	Passive scan	Active scan
An attacker who sends unsolicited messages to Bluetooth-enabled devices is conducting a:	Multiple Choice	Bluesnarfing attack	Bluejacking attack
An attacker intercepting unencrypted traffic between a user's computer and the network is using:	Multiple Choice	ARP poisoning	Wiretapping
An attacker who targets vulnerabilities in a system before the vendor has time to address them is exploiting:	Multiple Choice	Misconfigurations	Zero-day vulnerabilities
Which of the following is the most effective method to prevent SQL injection attacks?	Multiple Choice	Network firewalls	User training and awareness
Which of the following describes an attacker who manipulates a person inside the targeted organization to install malware?	Multiple Choice	Impersonation	Insider threat
An attacker gaining unauthorized access to a system by taking advantage of its default configuration settings is exploiting:	Multiple Choice	Zero-day vulnerabilities	Known vulnerabilities
Which type of vulnerability scan uses the database of known vulnerability signatures to identify threats?	Fill-in-the-Blank	Active scan	ACTIVE SCAN
An attacker who sends unsolicited messages to Bluetooth-enabled devices is conducting a:	Fill-in-the-Blank	Bluejacking attack	BLUEJACKING ATTACK
What attack involves the attacker setting up a fake Wi-Fi access point to intercept data?	Fill-in-the-Blank	Evil twin	EVIL TWIN
Which of the following is the most effective method to prevent SQL injection attacks?	Fill-in-the-Blank	Input validation	INPUT VALIDATION
An attacker gaining unauthorized access to a system by taking advantage of its default configuration settings is exploiting:	Fill-in-the-Blank	Misconfigurations	MISCONFIGURATIONS
A collection of software tools used by an attacker to hide the actions or presence of other types of malicious software is known as:	Fill-in-the-Blank	Rootkit	ROOTKIT

Contains software and Windows settings	Fill-in-the-Blank	Software Hive	SOFTWARE HIVE
Intentional, negligent, or accidental destruction or alteration of evidence.	Fill-in-the-Blank	Spoliation	SPOLIATION
A computer that is not connected to a network.	Fill-in-the-Blank	Standalone	STANDALONE
A means of writing hidden messages such that only the intended recipient knows of its existence. An modern example may be the replacing a few pixels of a digital image with a digital message. The slight change in the image may be unnoticeable to a person who does not know where in the image to look. Older forms of Steganography, which means “covered writing” in Greek, date back more than 2.000 years.	Fill-in-the-Blank	Steganography	STEGANOGRAPHY
Contains information about the Windows system setup, mounted devices, alternative configurations for hardware drivers and services.	Fill-in-the-Blank	System Hive	SYSTEM HIVE
A suite of communications protocols used to allow communication between computers on a network, such as on the Internet. Stands fro Transmission Control Protocol / Internet Protocol.	Fill-in-the-Blank	TCP/IP	TCP/IP
1024 Gigabytes, or 1,099,511,627,800 bytes – a bit more than one trillion bytes.	Fill-in-the-Blank	Terabyte	TERABYTE
Generally stands for a small, low-resolution image that takes the place of an original full-resolution image. Thumbnails do not generally contain metadata with GPS location or date of original creation of the source image.	Fill-in-the-Blank	Thumbnail	THUMBNAIL
Stands for “The Onion Router. TOR is US Government-created (through the US Naval Research Lab) software designed to allow anonymous or semi-anonymous communication.	Fill-in-the-Blank	TOR	TOR
The area on a hard disk or other media that is not (or is no longer) assigned to a file by the Operating System. May contain intact deleted files, remnants thereof, or other data.	Fill-in-the-Blank	Unallocated	UNALLOCATED
Which type of malware requires the user to spread the malware without the knowledge or intent?	Fill-in-the-Blank	Virus	VIRUS

An attacker intercepting unencrypted traffic between a user's computer and the network is using:	Fill-in-the-Blank	Wiretapping	WIRETAPPING
In which type of attack does an attacker target the vulnerabilities in a published public API?	Multiple Choice	API attack	SQL Injection
Which attack involves tricking the user into downloading and executing malicious code by pretending it is useful software?	Multiple Choice	Baiting	Vishing
The process of attempting to identify OS and software version numbers in order to find known vulnerabilities is called:	Multiple Choice	Fingerprinting	Spoofing
Which attack involves the attacker substituting their own IP address for a trusted IP address?	Multiple Choice	IP spoofing	DNS spoofing
What is the term for testing an organization's security measures by attempting to exploit vulnerabilities without prior knowledge of the environment?	Multiple Choice	Red teaming	Vulnerability assessment
A common term for the person using a computer, also referred to as an End _____.	Multiple Choice	User	Web Browser
Often simply referred to as “browser.” A program used to find and display web pages. Popular browsers as of this writing are Microsoft Internet Explorer) often abbreviated as “Explorer,” Netscape Navigator, Mozilla Firefox, and Apple Safari.	Multiple Choice	Web Browser	Windows Registry
Microsoft Windows (“Windows”) keeps a large amount of information regarding the User’s Windows use and configuration in a part of the operating system called the Windows Registry. Included in the information kept in the Windows Registry is information such as that kept in Jump Lists and LNK files, and other data found in the Registry Hives.	Multiple Choice	Windows Registry	Windows Swap File
Also known as the Page file, or Pagesys file. A virtual memory file used by Microsoft Windows as a kind of scratch pad during most operations. The Swap file is usually quite large and often contains records of operations or remnants of files not found elsewhere.	Multiple Choice	Windows Swap File	World Wide Web

A system of servers connected through the Internet that support HTML documents.	Multiple Choice	World Wide Web	Yottabyte
1024 zettabytes.	Multiple Choice	Yottabyte	Zettabyte
1024 exabytes.	Multiple Choice	Zettabyte	Burn
The act of sending emails or other messages that appear to come from a trusted source but are malicious in nature is known as:	Multiple Choice	Baiting	Tailgating
An attack in which the attacker takes control of a session between two machines and masquerades as one of them is known as:	Multiple Choice	Replay attack	Session splicing
In which type of attack does an attacker target the vulnerabilities in a published public API?	Fill-in-the-Blank	API attack	API ATTACK
Which attack involves tricking the user into downloading and executing malicious code by pretending it is useful software?	Fill-in-the-Blank	Baiting	BAITING
The process of attempting to identify OS and software version numbers in order to find known vulnerabilities is called:	Fill-in-the-Blank	Fingerprinting	FINGERPRINTING
Which attack involves the attacker substituting their own IP address for a trusted IP address?	Fill-in-the-Blank	IP spoofing	IP SPOOFING
What is the term for testing an organization's security measures by attempting to exploit vulnerabilities without prior knowledge of the environment?	Fill-in-the-Blank	Red teaming	RED TEAMING
An attack in which the attacker takes control of a session between two machines and masquerades as one of them is known as:	Fill-in-the-Blank	Session hijacking	SESSION HIJACKING
A common term for the person using a computer, also referred to as an End _____.	Fill-in-the-Blank	User	USER
Often simply referred to as “browser.” A program used to find and display web pages. Popular browsers as of this writing are Microsoft Internet Explorer) often abbreviated as “Explorer,” Netscape Navigator, Mozilla Firefox, and Apple Safari.	Fill-in-the-Blank	Web Browser	WEB BROWSER

Microsoft Windows (“Windows”) keeps a large amount of information regarding the User’s Windows use and configuration in a part of the operating system called the Windows Registry. Included in the information kept in the Windows Registry is information such as that kept in Jump Lists and LNK files, and other data found in the Registry Hives.	Fill-in-the-Blank	Windows Registry	WINDOWS REGISTRY
Also known as the Page file, or Pagesys file. A virtual memory file used by Microsoft Windows as a kind of scratch pad during most operations. The Swap file is usually quite large and often contains records of operations or remnants of files not found elsewhere.	Fill-in-the-Blank	Windows Swap File	WINDOWS SWAP FILE
A system of servers connected through the Internet that support HTML documents.	Fill-in-the-Blank	World Wide Web	WORLD WIDE WEB
1024 zettabytes.	Fill-in-the-Blank	Yottabyte	YOTTABYTE
1024 exabytes.	Fill-in-the-Blank	Zettabyte	ZETTABYTE

Option 3	Option 4	Option 5	Correct Answer	Time in seconds	Image Link
Text for option 3 (optional)	Text for option 4 (optional)	Text for option 5 (optional)	The correct option choice (between 1-5). Leave blank for "Open-Ended", "Poll", "Draw" and "Fill-in-the-Blank".	Time in seconds (optional, default value is 30 seconds)	Link of the image (optional)
Allocated space / sector / block	Allocation Block	Application	1		
Allocation Block	Application	ASCII	1		
Application	ASCII	Audit Trail	1		
ASCII	Audit Trail	Back door	1		
Audit Trail	Back door	Backdoor Trojan	1		

Back door	Backdoor Trojan	Backup	1		
Backdoor Trojan	Backup	Backup media	1		
Backup	Backup media	Backup Server	1		
Backup media	Backup Server	Bit	1		
Backup Server	Bit	Bitstream or bit-by-bit copy	1		
Spoofing	Snarfing		1		
The bandwidth of a network is exceeded.	A disk drive is full.		1		

Spoofing	Replay attack		1		
Encryption	Networking		2		
Non-intrusive scanner	Network mapper		2		
Smurf Attack	DDoS Attack		2		
Amplification attack	Botnet attack		3		
An exploit for which no official patch has been released.	An exploit that only affects outdated systems.		3		
Ransomware	Spyware		3		
Spear phishing	Tailgating		3		

Bit	Bitstream or bit-by-bit copy	Block	1		
Bitstream or bit-by-bit copy	Block	Buffer	1		
Block	Buffer	Buffer file	1		
Buffer	Buffer file	Burn	1		
Buffer file	Burn	Byte	1		
Burn	Byte	Cache	1		
Byte	Cache	CD-ROM	1		
Cache	CD-ROM	Chain of Custody	1		

CD-ROM	Chain of Custody	Cluster	1		
Chain of Custody	Cluster	Compressed file, zipped file	1		
Cluster	Compressed file, zipped file	Computer Forensics	1		
UDP flood	Ping flood		1		
Drive-by attack	Insider threat		1		
Tailgating	Impersonation		2		
Virus	Spyware		2		
ARP poisoning	DHCP spoofing		3		
Sequence prediction	Replay attack		3		
Vishing	Baiting		3		

Nonce	Vector		3		
Compressed file, zipped file	Computer Forensics	Cookie	1		

Computer Forensics	Cookie	Corrupt Data, Corrupt File	1		
Cookie	Corrupt Data, Corrupt File	Darkweb	1		
Corrupt Data, Corrupt File	Darkweb	Deduplication (“De-duping”)	1		
Darkweb	Deduplication (“De-duping”)	Deep Web	1		
Deduplication (“De-duping”)	Deep Web	Default	1		
Deep Web	Default	Delete	1		
Default	Delete	Desktop computer	1		

Delete	Desktop computer	Directory	1		
Desktop computer	Directory	Disk	1		
Directory	Disk	Disk cache	1		
Disk	Disk cache	Disk Mirroring	1		
Disk cache	Disk Mirroring	Dot	1		
Race condition	Watering hole		1		
Amplification attack	Reflection attack		2		
Buffer overflow	Replay attack		2		
Baiting	Vishing		2		
Fileless malware	RAT		2		
Keylogger	Worm		3		

SQL injection	XSS		3		

Rainbow Table Attack	Birthday Attack		1		
Disk Mirroring	Dot	Download	1		
Dot	Download	E-mail	1		
Download	E-mail	Encryption	1		

E-mail	Encryption	Exabyte	1		
Encryption	Exabyte	Extension, File Extension	1		
Exabyte	Extension, File Extension	File Attribute	1		
Extension, File Extension	File Attribute	File Server	1		
File Attribute	File Server	File signature	1		
File Server	File signature	File slack	1		
File signature	File slack	Filename	1		
IP spoofing	DHCP snooping		2		
Distributed Reflection	ARP poisoning		2		

Spyware	Trojan		2		
Man-in-the-Middle	TCP SYN flood		2		
ICMP flood	Ping flood		2		
Spyware	Adware		2		
External scan	Intrusive scan		3		
Pharming	Spear Phishing		3		
RAT	Drive-by Download		4		

File slack	Filename	Floppy diskette, floppy	1		
Filename	Floppy diskette, floppy	Folder	1		
Floppy diskette, floppy	Folder	Forensic image	1		
Folder	Forensic image	GIF	1		
Forensic image	GIF	Gigabyte (GB)	1		
GIF	Gigabyte (GB)	GUI	1		
Gigabyte (GB)	GUI	Hard disk	1		
GUI	Hard disk	Hash, hash value	1		

Hard disk	Hash, hash value	HTML	1		
Hash, hash value	HTML	Instant Messaging	1		
HTML	Instant Messaging	IP Address (IPv4)	1		
Instant Messaging	IP Address (IPv4)	IP Address (IPv6)	1		
Spyware	Virus		2		
SYN flood	Smurf attack		2		
Man-in-the-Middle	DDoS		2		
Rootkit	Worm		2		
Brute force	Baiting		3		
Certificate spoofing	XML injection		3		
Fileless malware	Trojan		3		
SYN flood	Watering hole		3		

MAC spoofing	DNS poisoning		1		
IP Address (IPv4)	IP Address (IPv6)	ISP	1		
IP Address (IPv6)	ISP	JPEG	1		
ISP	JPEG	Jumplists	1		
JPEG	Jumplists	Keylogger	1		
Jumplists	Keylogger	Keyword search	1		
Keylogger	Keyword search	Kilobyte (KB)	1		

Keyword search	Kilobyte (KB)	LNK files	1		
Kilobyte (KB)	LNK files	Log files, or logfile	1		
LNK files	Log files, or logfile	MAC dates	1		
Log files, or logfile	MAC dates	Mail Server	1		
MAC dates	Mail Server	Master File Table, or MFT	1		
Drive-by download	Watering hole		1		
Logic bomb	Virus		1		
CSRF	XML injection		2		
Rainbow table attack	Birthday attack		2		
Can propagate without human intervention	Exploits software vulnerabilities		2		
CSRF	Man-in-the-Middle attack		2		

Race condition	Denial of Service		2		
Boot sector virus	Rootkit		3		
Spyware	Backdoor		4		
Man-in-the-Middle	Denial of Service (DoS)		4		

Session hijacking	ARP poisoning		1		
Cross-site request forgery (CSRF)	Buffer overflow		1		
Mail Server	Master File Table, or MFT	Megabyte (MB)	1		
Master File Table, or MFT	Megabyte (MB)	Memory Cache	1		
Megabyte (MB)	Memory Cache	Native format, native environment	1		

Memory Cache	Native format, native environment	Network	1		
Native format, native environment	Network	NTFS	1		
Network	NTFS	Operating System, OS	1		
NTFS	Operating System, OS	Partition	1		
Operating System, OS	Partition	PDF	1		
Partition	PDF	Petabyte	1		
PDF	Petabyte	Program	1		
Petabyte	Program	Protocol	1		

Dictionary attack	CSRF		1		
Program	Protocol	RAM	1		
Smurf attack	Session hijacking		2		
Replay attack	Session hijacking		2		
Ransomware	Worm		2		
Buffer overflow	ARP poisoning		2		
Smurf attack	ICMP flood		2		
Denial of Service (DoS)	Replay attack		3		
Trojan	Worm		3		
Phishing	Spear phishing		4		

Protocol	RAM	Registry Hives	1		
RAM	Registry Hives	SAM Hive	1		
Registry Hives	SAM Hive	Sector	1		
SAM Hive	Sector	Server	1		
Sector	Server	Shadow Volume	1		
Server	Shadow Volume	Software	1		
Shadow Volume	Software	Software Hive	1		
Software	Software Hive	Spoliation	1		
Software Hive	Spoliation	Standalone	1		
Spoliation	Standalone	Steganography	1		
SQL Injection	Man-in-the-Middle		2		

SYN flood	Smurf attack		2		
Phishing attack	Man-in-the-Middle attack		2		
CSRF	DNS spoofing		2		
Adware	Rootkit		3		
Amplification attack	Smurf attack		3		
Spyware	Ransomware		3		
Evil Twin	IMSI catcher		4		

Man-in-the-Middle	Session hijacking		1		
Logic bomb	Worm		1		
SQL injection	Replay attack		1		
Standalone	Steganography	System Hive	1		
Steganography	System Hive	TCP/IP	1		
System Hive	TCP/IP	Terabyte	1		
TCP/IP	Terabyte	Thumbnail	1		
Terabyte	Thumbnail	TOR	1		
Thumbnail	TOR	Unallocated	1		
TOR	Unallocated	User	1		
Unallocated	User	Web Browser	1		
User	Web Browser	Windows Registry	1		

Web Browser	Windows Registry	Windows Swap File	1		
Credentialed scan	Non-credentialed scan		2		
War driving	Wardialing		2		
MAC spoofing	DNS spoofing		2		
Legacy systems	Open source software		2		
Input validation	Regular software updates		3		
Phishing	Baiting		4		
Unpatched software	Misconfigurations		4		

Buffer overflow	Man-in-the-middle		1		
Spear phishing	Watering hole attack		1		
Phishing	Port scanning		1		
ARP poisoning	Session hijacking		1		
White box testing	Static code analysis		1		
Windows Registry	Windows Swap File	World Wide Web	1		
Windows Swap File	World Wide Web	Yottabyte	1		
World Wide Web	Yottabyte	Zettabyte	1		
Yottabyte	Zettabyte	Burn	1		

Zettabyte	Burn	Byte	1		
Burn	Byte	Cache	1		
Byte	Cache	CD-ROM	1		
Phishing	Spoofing		3		
Session hijacking	Man-in-the-middle		3		
