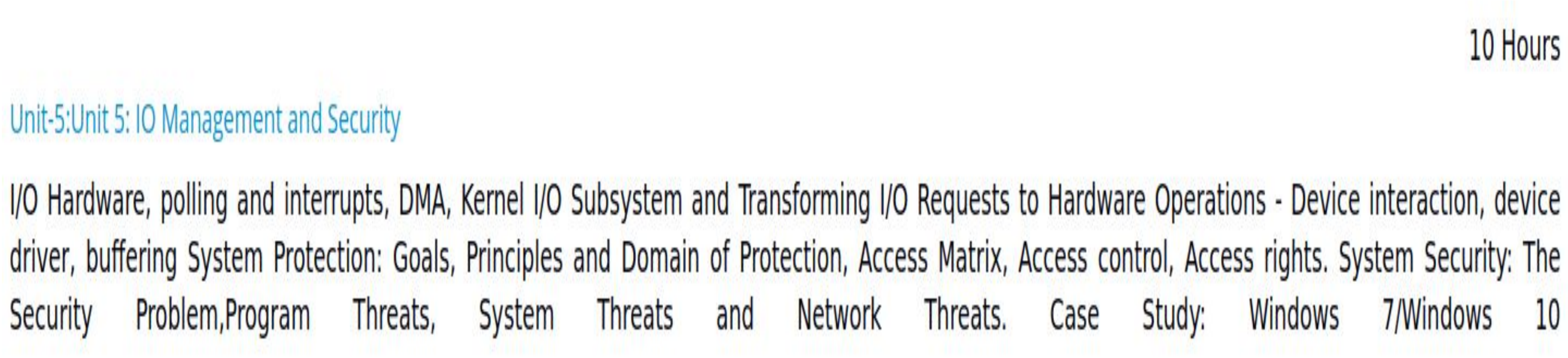
OPERATING SYSTEMS

UE18CS302_Unit 5_Revision_Class_#2

Nitin V Pujari
Faculty, Computer Science
Dean - IQAC, PES University

Course Syllabus - Unit 5



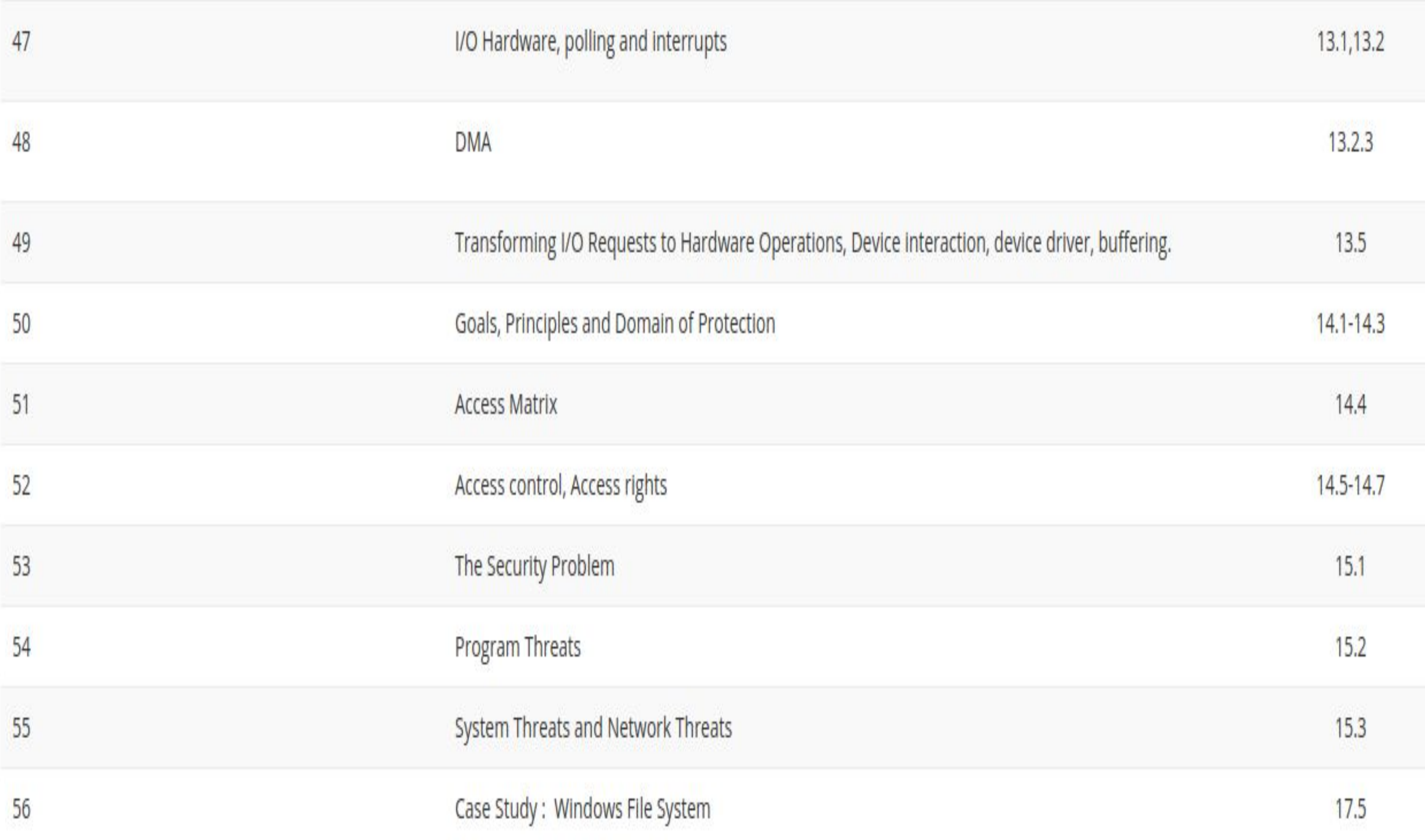
10 Hours

Unit-5:Unit 5: IO Management and Security

I/O Hardware, polling and interrupts, DMA, Kernel I/O Subsystem and Transforming I/O Requests to Hardware Operations - Device interaction, device driver, buffering System Protection: Goals, Principles and Domain of Protection, Access Matrix, Access control, Access rights. System Security: The Security Problem,Program Threats, System Threats and Network Threats. Case Study: Windows 7/Windows 10

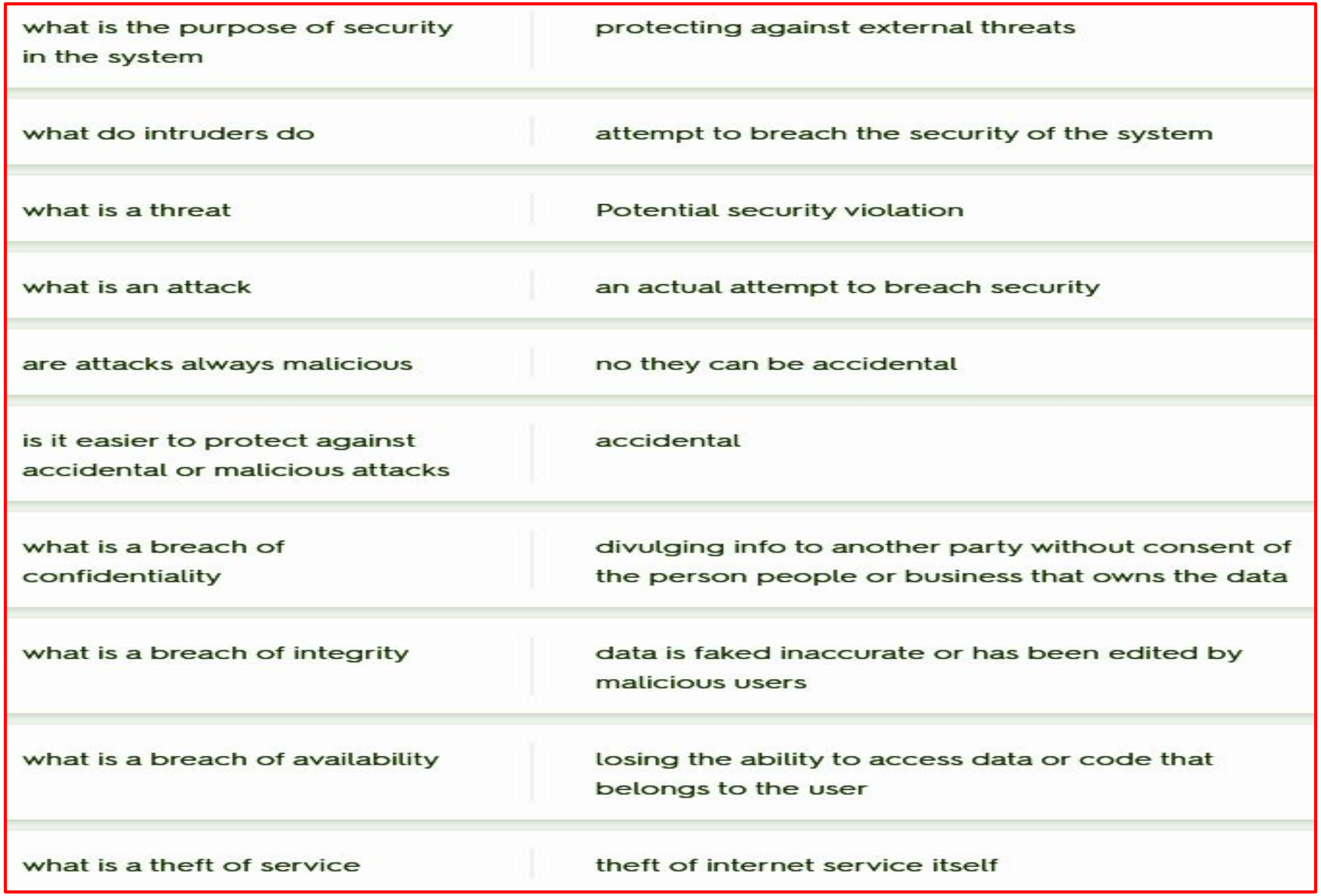
OPERATING SYSTEMS

Course Outline



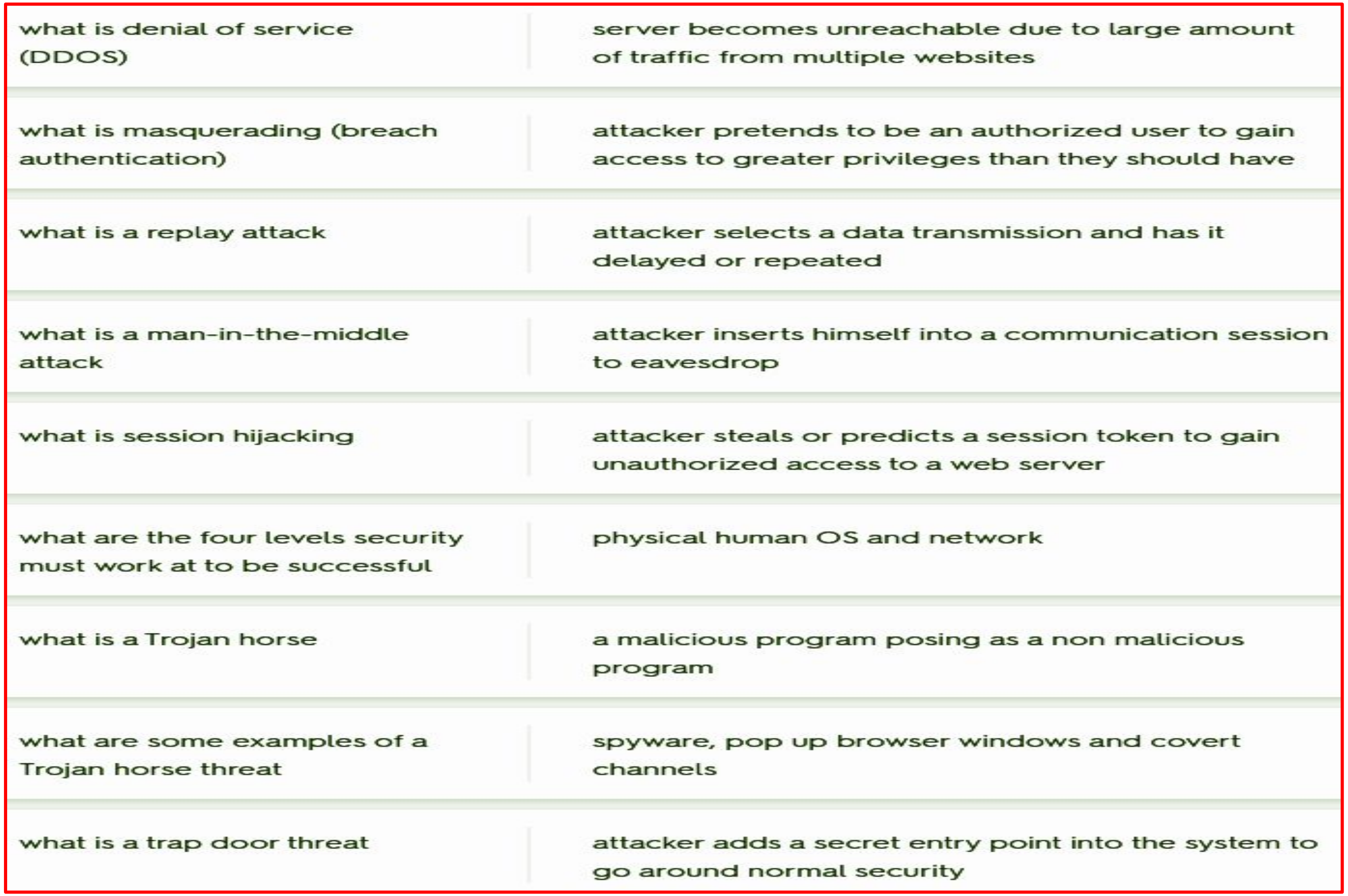
47	I/O Hardware, polling and interrupts	13.1,13.2
48	DMA	13.2.3
49	Transforming I/O Requests to Hardware Operations, Device interaction, device driver, buffering.	13.5
50	Goals, Principles and Domain of Protection	14.1-14.3
51	Access Matrix	14.4
52	Access control, Access rights	14.5-14.7
53	The Security Problem	15.1
54	Program Threats	15.2
55	System Threats and Network Threats	15.3
56	Case Study : Windows File System	17.5

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



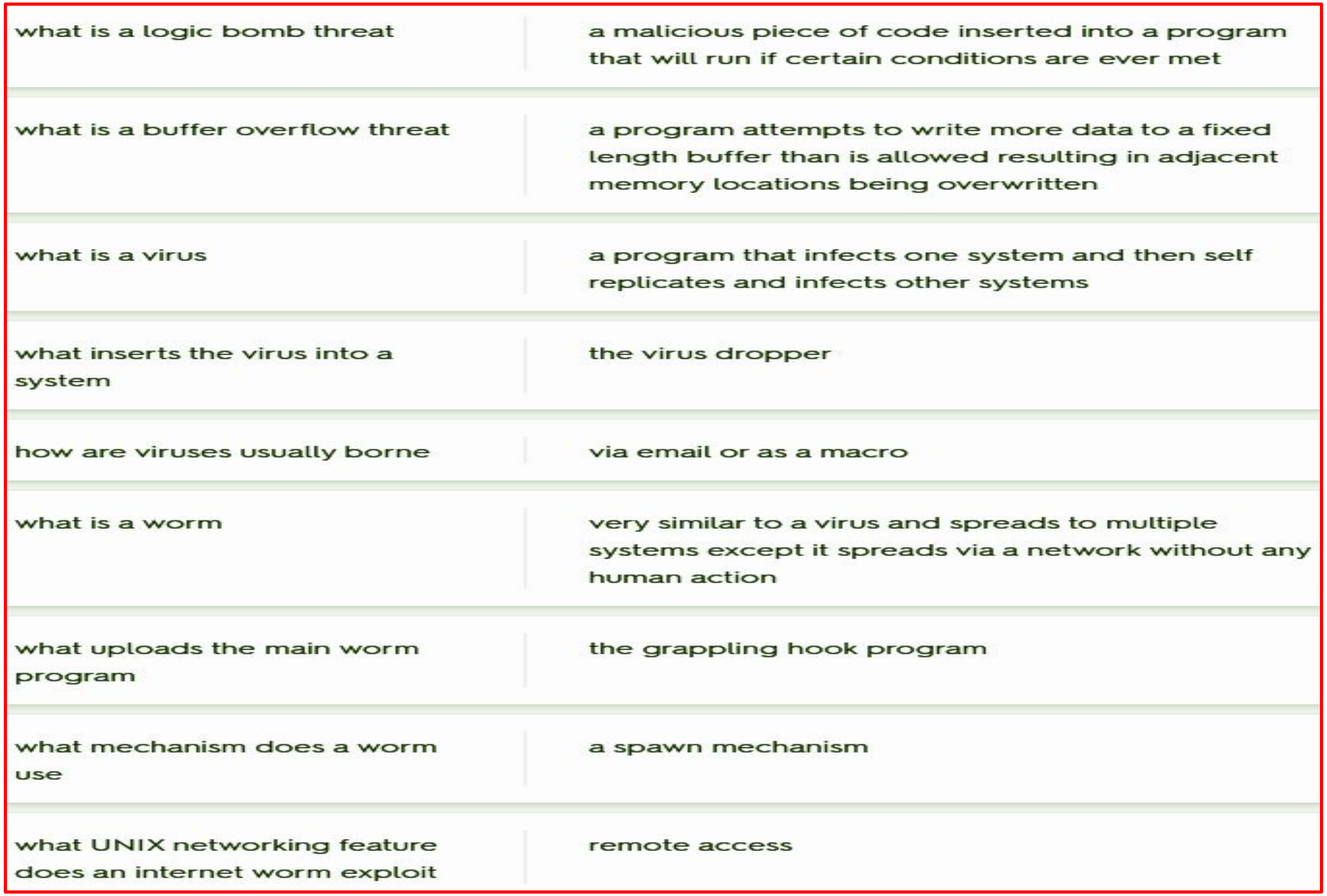
what is the purpose of security in the system	protecting against external threats
what do intruders do	attempt to breach the security of the system
what is a threat	Potential security violation
what is an attack	an actual attempt to breach security
are attacks always malicious	no they can be accidental
is it easier to protect against accidental or malicious attacks	accidental
what is a breach of confidentiality	divulging info to another party without consent of the person people or business that owns the data
what is a breach of integrity	data is faked inaccurate or has been edited by malicious users
what is a breach of availability	losing the ability to access data or code that belongs to the user
what is a theft of service	theft of internet service itself

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



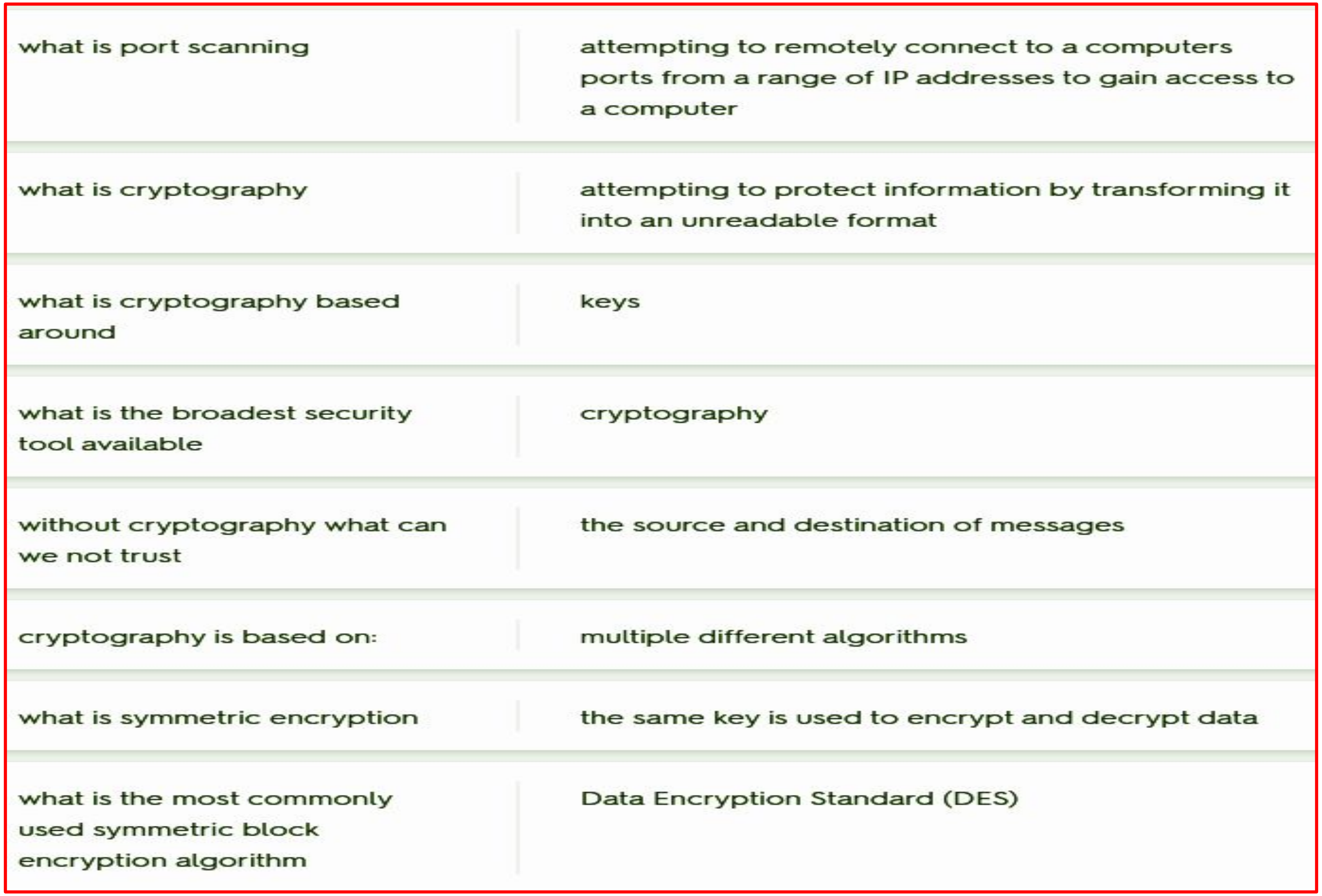
what is denial of service (DDOS)	server becomes unreachable due to large amount of traffic from multiple websites
what is masquerading (breach authentication)	attacker pretends to be an authorized user to gain access to greater privileges than they should have
what is a replay attack	attacker selects a data transmission and has it delayed or repeated
what is a man-in-the-middle attack	attacker inserts himself into a communication session to eavesdrop
what is session hijacking	attacker steals or predicts a session token to gain unauthorized access to a web server
what are the four levels security must work at to be successful	physical human OS and network
what is a Trojan horse	a malicious program posing as a non malicious program
what are some examples of a Trojan horse threat	spyware, pop up browser windows and covert channels
what is a trap door threat	attacker adds a secret entry point into the system to go around normal security

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



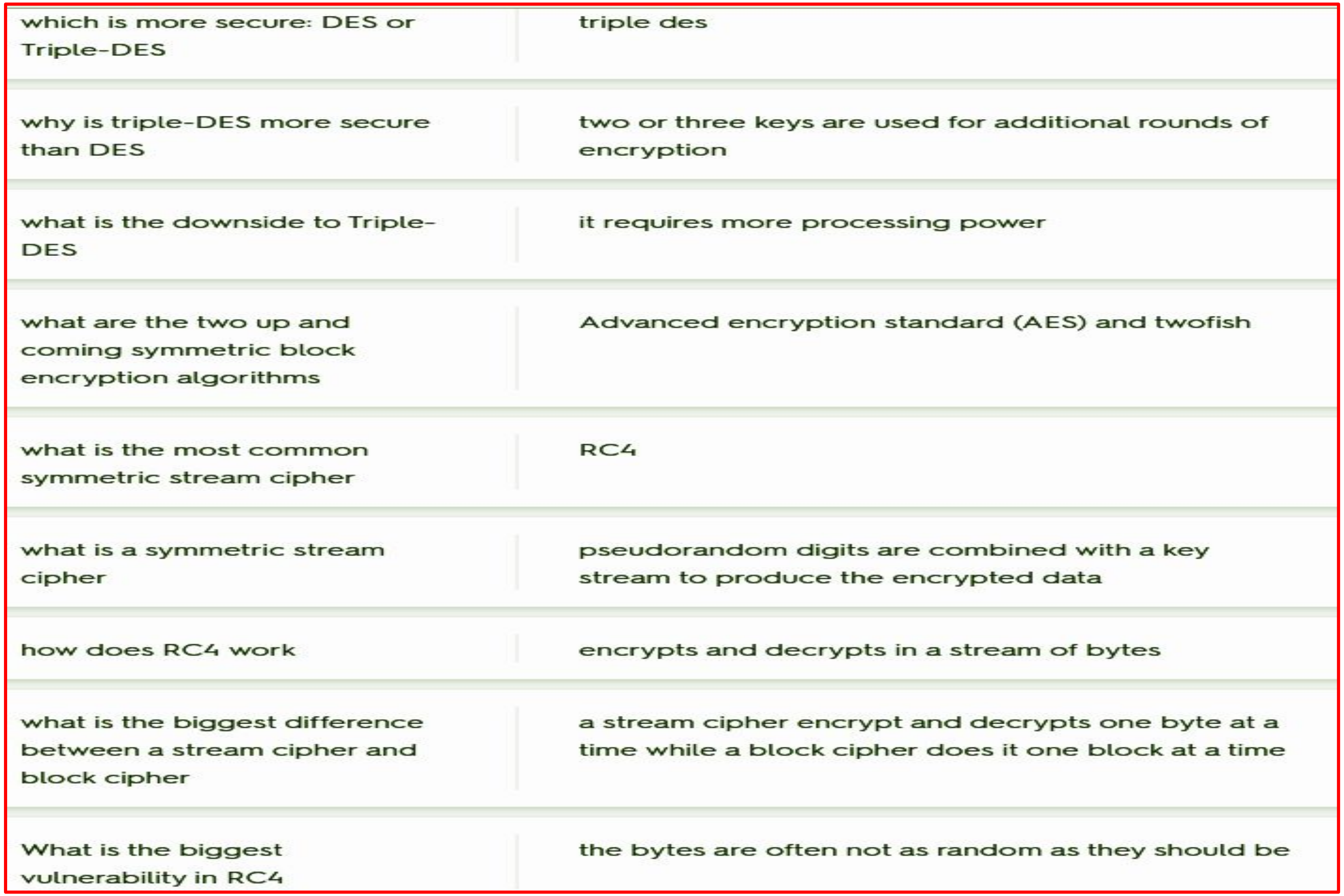
what is a logic bomb threat	a malicious piece of code inserted into a program that will run if certain conditions are ever met
what is a buffer overflow threat	a program attempts to write more data to a fixed length buffer than is allowed resulting in adjacent memory locations being overwritten
what is a virus	a program that infects one system and then self replicates and infects other systems
what inserts the virus into a system	the virus dropper
how are viruses usually borne	via email or as a macro
what is a worm	very similar to a virus and spreads to multiple systems except it spreads via a network without any human action
what uploads the main worm program	the grappling hook program
what mechanism does a worm use	a spawn mechanism
what UNIX networking feature does an internet worm exploit	remote access

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



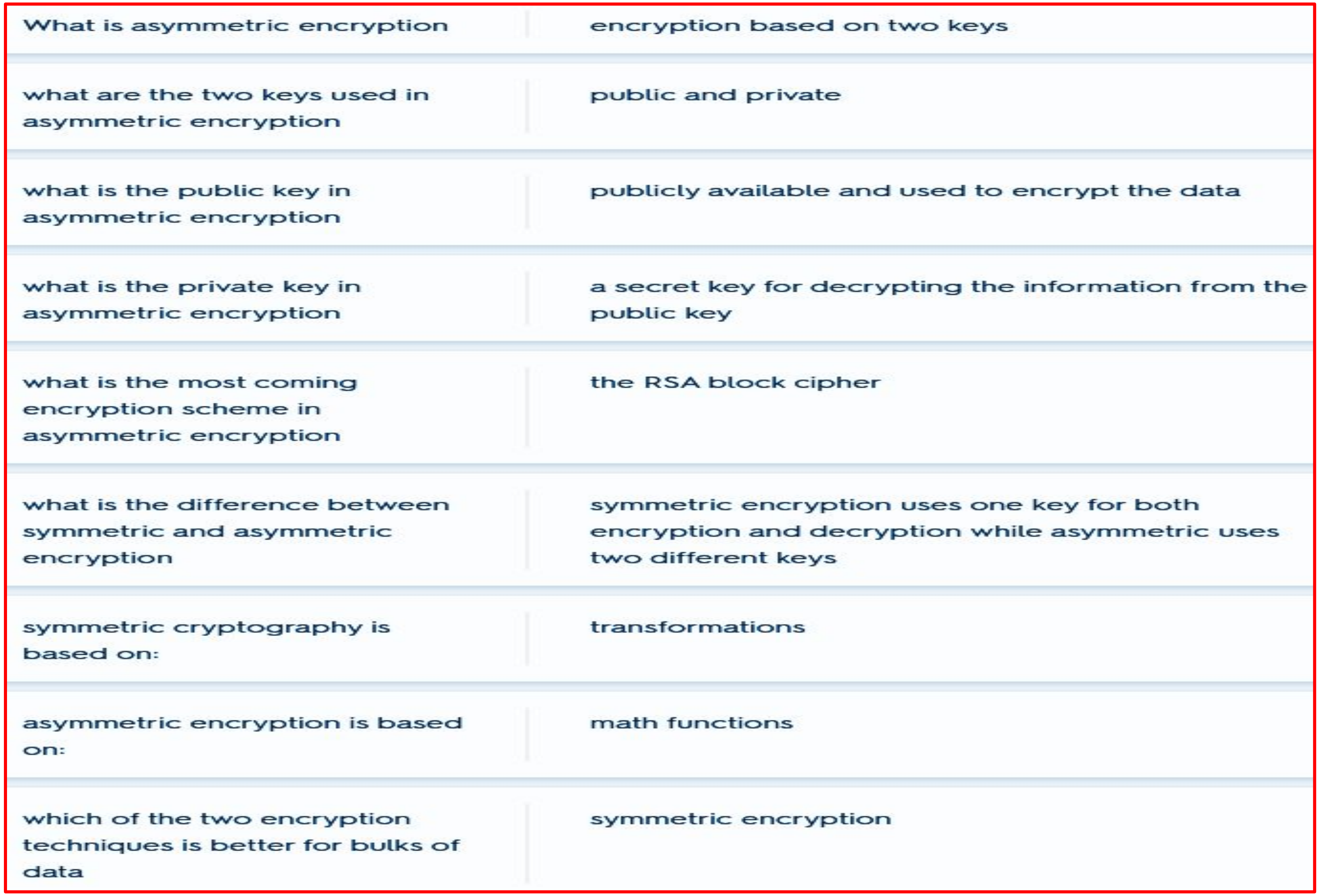
what is port scanning	attempting to remotely connect to a computers ports from a range of IP addresses to gain access to a computer
what is cryptography	attempting to protect information by transforming it into an unreadable format
what is cryptography based around	keys
what is the broadest security tool available	cryptography
without cryptography what can we not trust	the source and destination of messages
cryptography is based on:	multiple different algorithms
what is symmetric encryption	the same key is used to encrypt and decrypt data
what is the most commonly used symmetric block encryption algorithm	Data Encryption Standard (DES)

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



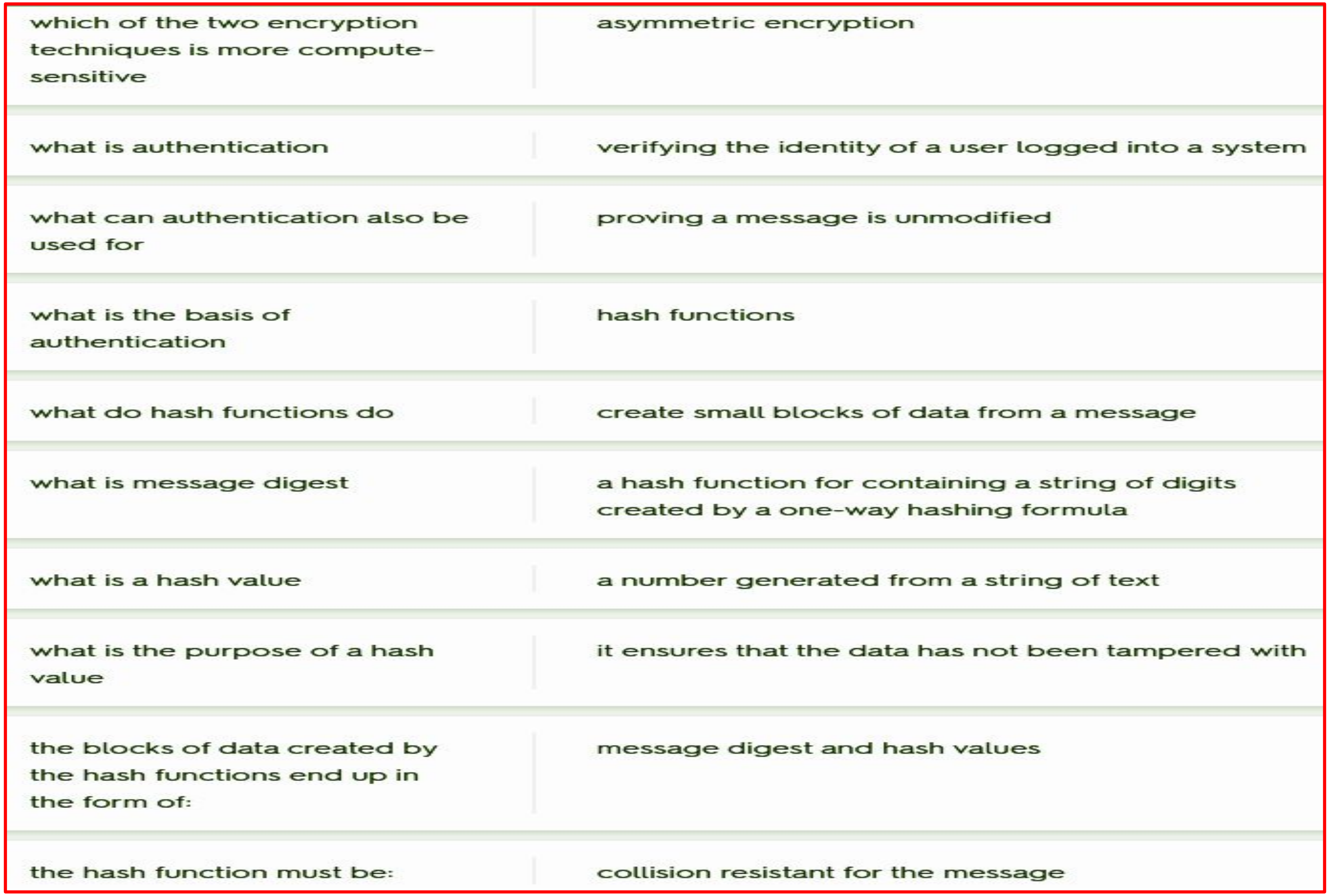
which is more secure: DES or Triple-DES	triple des
why is triple-DES more secure than DES	two or three keys are used for additional rounds of encryption
what is the downside to Triple-DES	it requires more processing power
what are the two up and coming symmetric block encryption algorithms	Advanced encryption standard (AES) and twofish
what is the most common symmetric stream cipher	RC4
what is a symmetric stream cipher	pseudorandom digits are combined with a key stream to produce the encrypted data
how does RC4 work	encrypts and decrypts in a stream of bytes
what is the biggest difference between a stream cipher and block cipher	a stream cipher encrypt and decrypts one byte at a time while a block cipher does it one block at a time
What is the biggest vulnerability in RC4	the bytes are often not as random as they should be

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



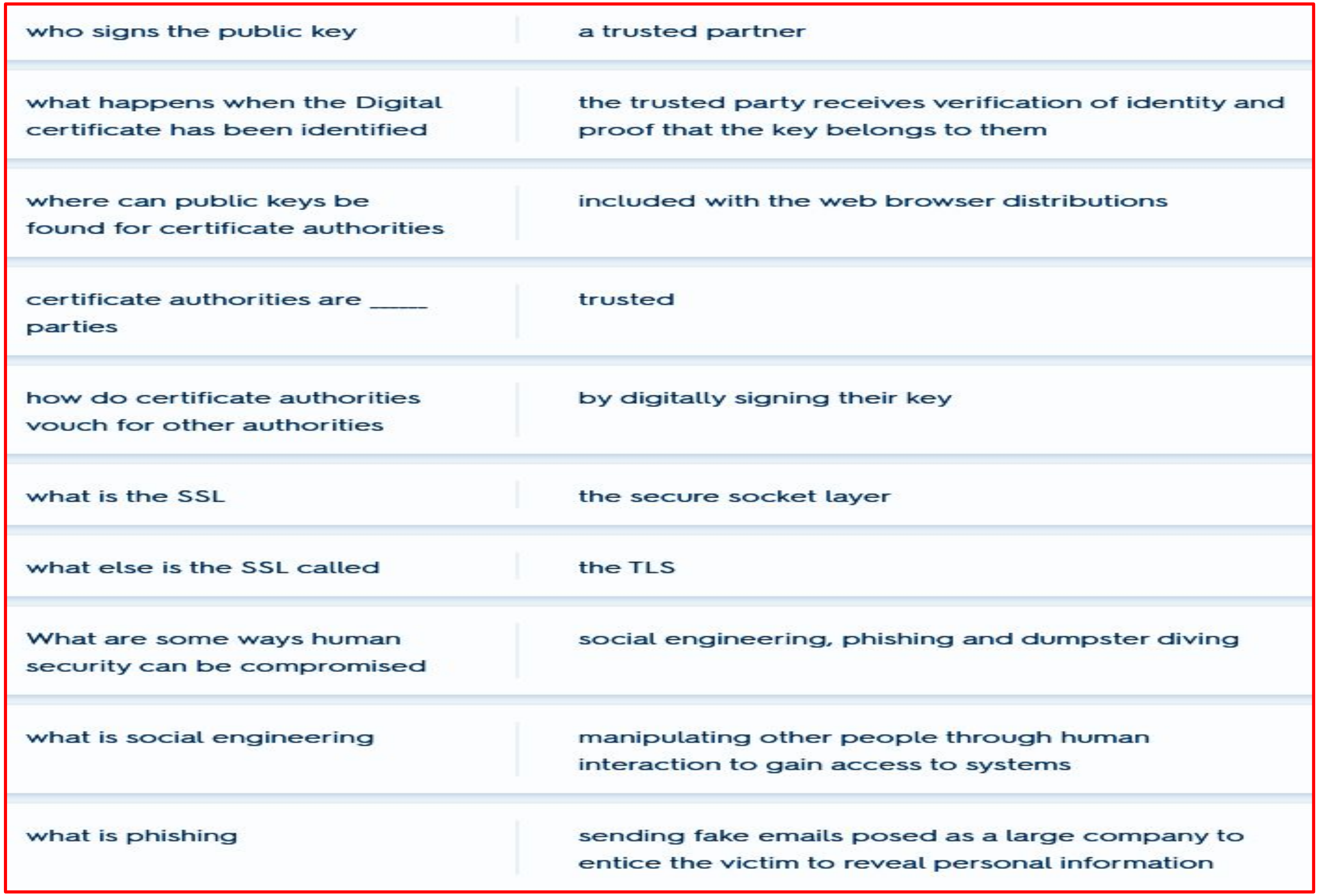
What is asymmetric encryption	encryption based on two keys
what are the two keys used in asymmetric encryption	public and private
what is the public key in asymmetric encryption	publicly available and used to encrypt the data
what is the private key in asymmetric encryption	a secret key for decrypting the information from the public key
what is the most coming encryption scheme in asymmetric encryption	the RSA block cipher
what is the difference between symmetric and asymmetric encryption	symmetric encryption uses one key for both encryption and decryption while asymmetric uses two different keys
symmetric cryptography is based on:	transformations
asymmetric encryption is based on:	math functions
which of the two encryption techniques is better for bulks of data	symmetric encryption

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



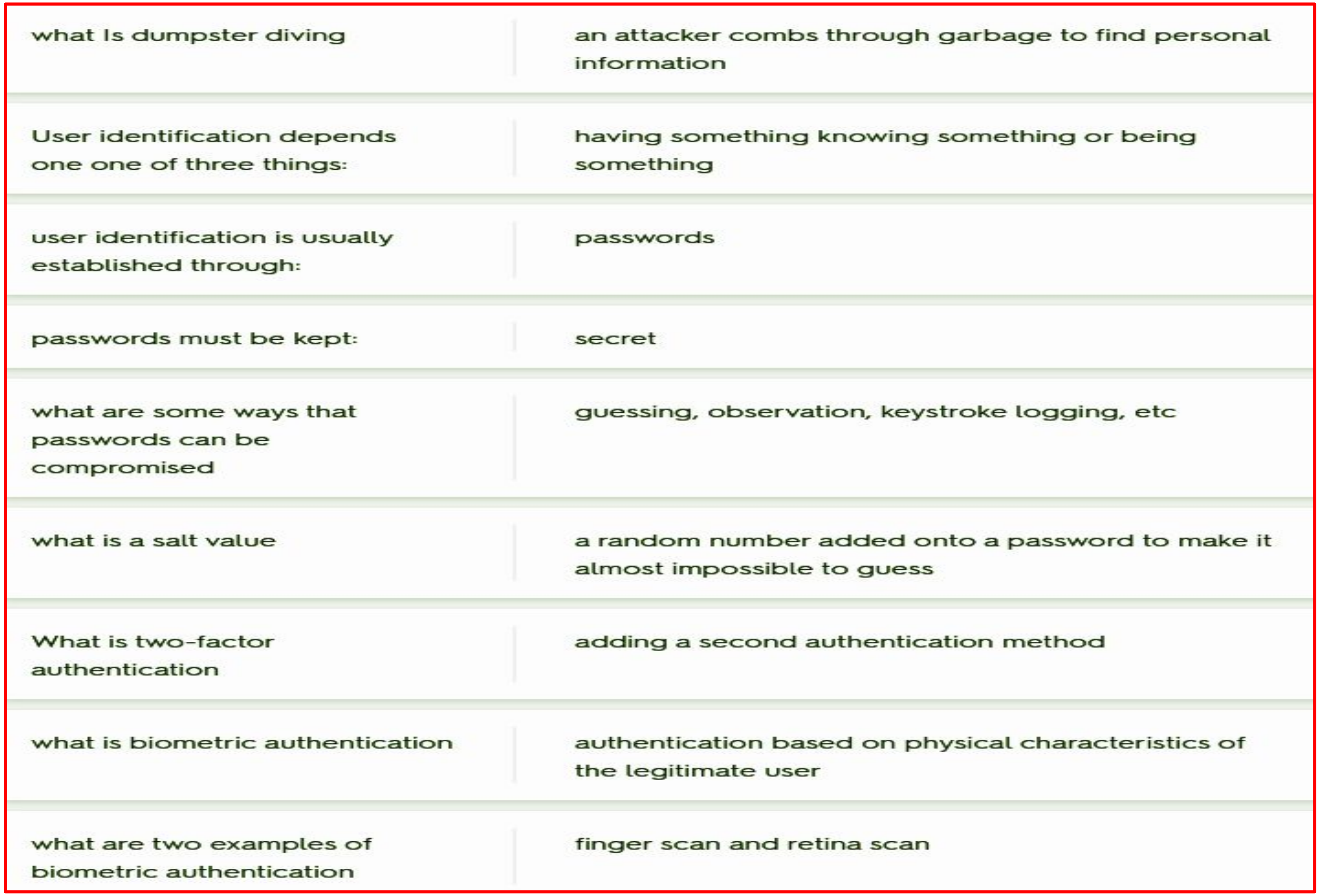
which of the two encryption techniques is more compute-sensitive	asymmetric encryption
what is authentication	verifying the identity of a user logged into a system
what can authentication also be used for	proving a message is unmodified
what is the basis of authentication	hash functions
what do hash functions do	create small blocks of data from a message
what is message digest	a hash function for containing a string of digits created by a one-way hashing formula
what is a hash value	a number generated from a string of text
what is the purpose of a hash value	it ensures that the data has not been tampered with
the blocks of data created by the hash functions end up in the form of:	message digest and hash values
the hash function must be:	collision resistant for the message

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



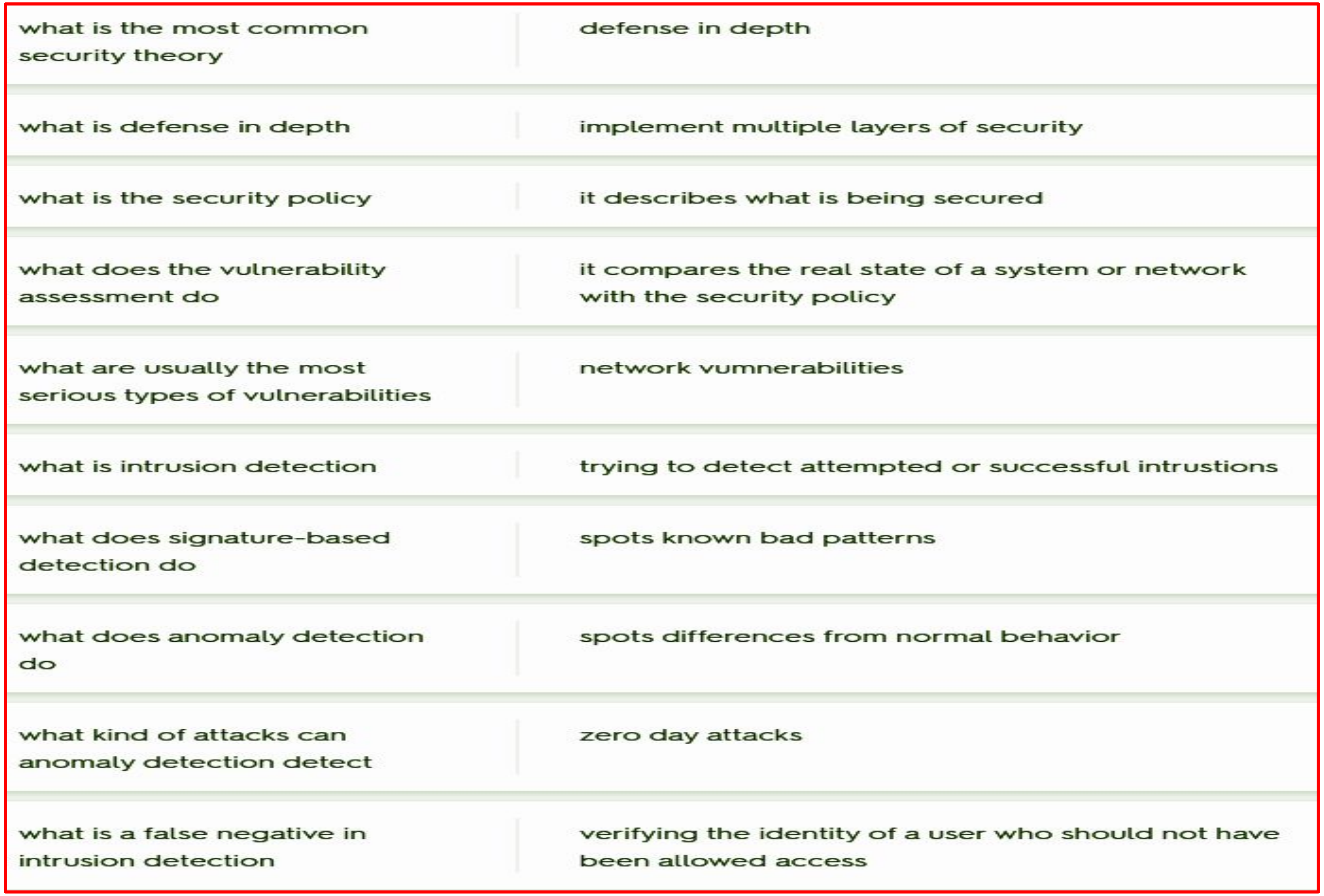
who signs the public key	a trusted partner
what happens when the Digital certificate has been identified	the trusted party receives verification of identity and proof that the key belongs to them
where can public keys be found for certificate authorities	included with the web browser distributions
certificate authorities are ____ parties	trusted
how do certificate authorities vouch for other authorities	by digitally signing their key
what is the SSL	the secure socket layer
what else is the SSL called	the TLS
What are some ways human security can be compromised	social engineering, phishing and dumpster diving
what is social engineering	manipulating other people through human interaction to gain access to systems
what is phishing	sending fake emails posed as a large company to entice the victim to reveal personal information

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



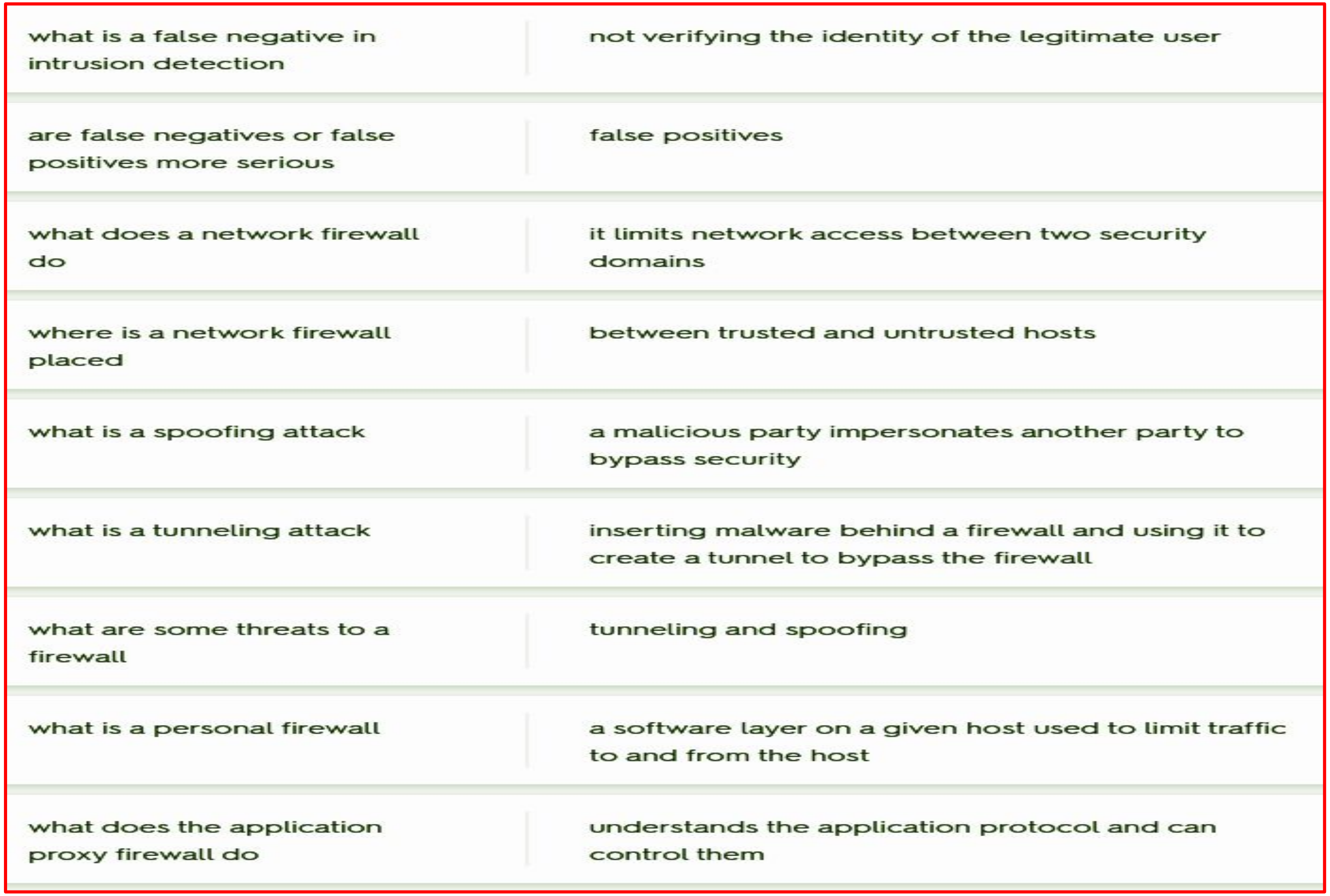
what Is dumpster diving	an attacker combs through garbage to find personal information
User identification depends one one of three things:	having something knowing something or being something
user identification is usually established through:	passwords
passwords must be kept:	secret
what are some ways that passwords can be compromised	guessing, observation, keystroke logging, etc
what is a salt value	a random number added onto a password to make it almost impossible to guess
What is two-factor authentication	adding a second authentication method
what is biometric authentication	authentication based on physical characteristics of the legitimate user
what are two examples of biometric authentication	finger scan and retina scan

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



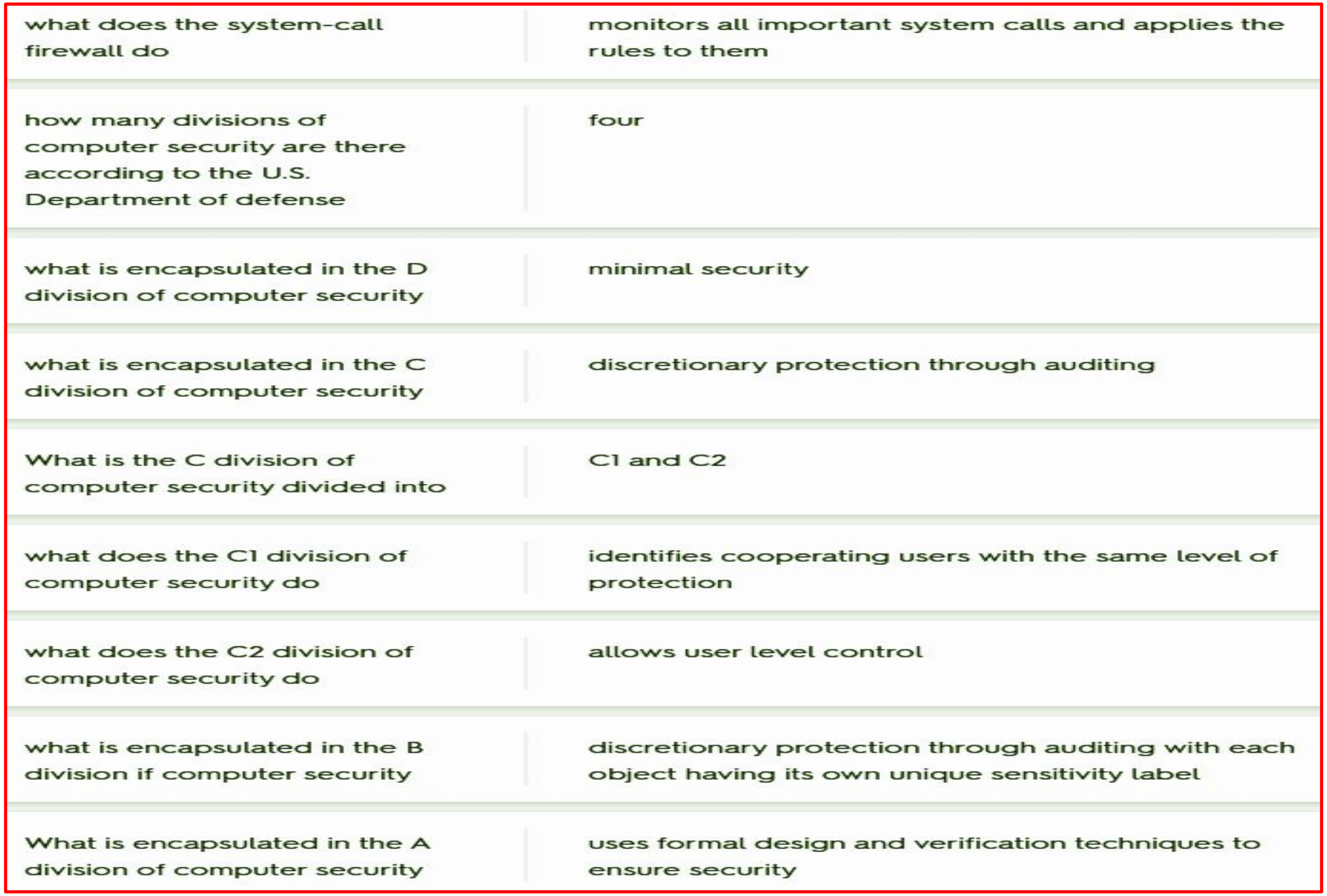
what is the most common security theory	defense in depth
what is defense in depth	implement multiple layers of security
what is the security policy	it describes what is being secured
what does the vulnerability assessment do	it compares the real state of a system or network with the security policy
what are usually the most serious types of vulnerabilities	network vumnerabilities
what is intrusion detection	trying to detect attempted or successful intrustions
what does signature-based detection do	spots known bad patterns
what does anomaly detection do	spots differences from normal behavior
what kind of attacks can anomaly detection detect	zero day attacks
what is a false negative in intrusion detection	verifying the identity of a user who should not have been allowed access

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



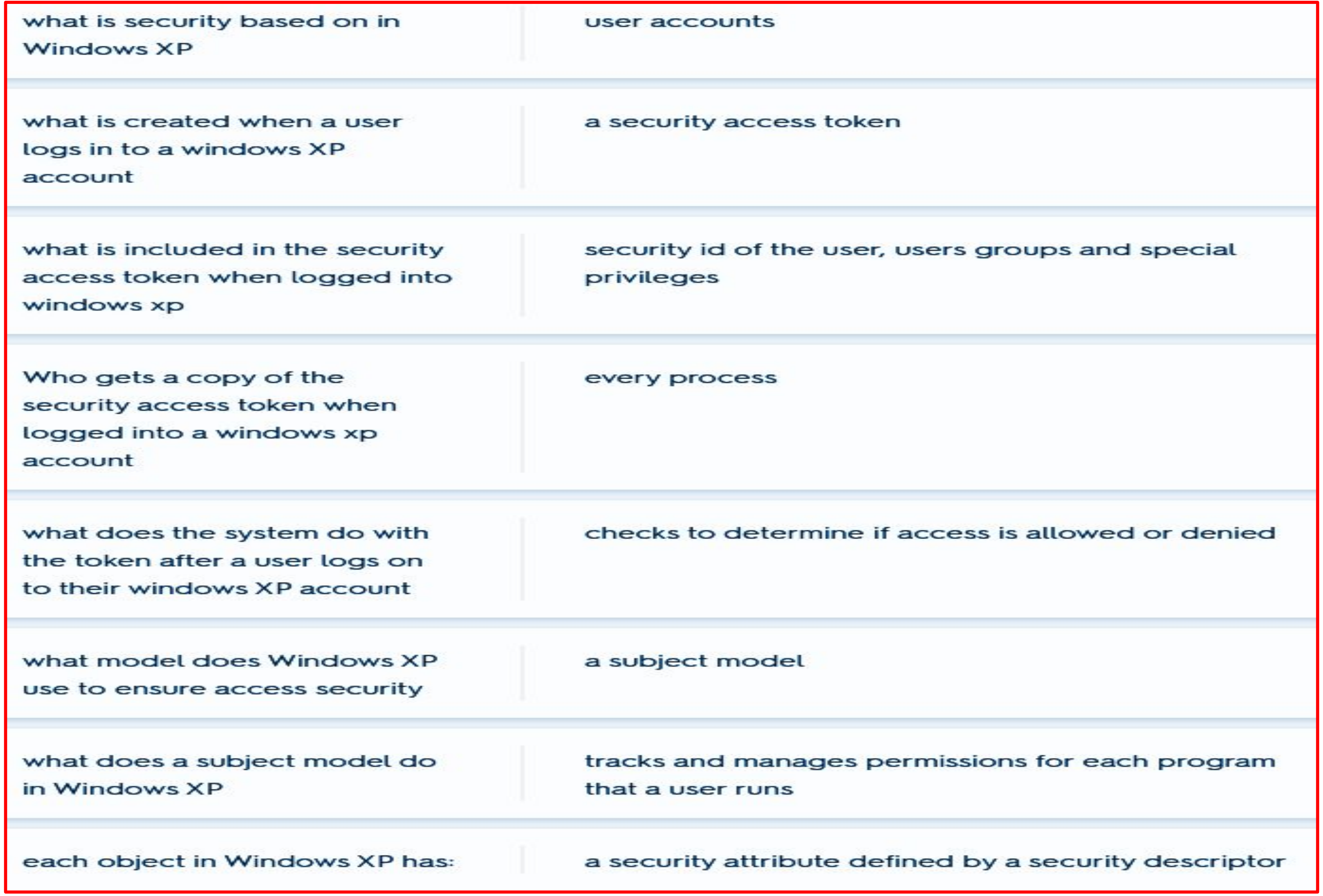
what is a false negative in intrusion detection	not verifying the identity of the legitimate user
are false negatives or false positives more serious	false positives
what does a network firewall do	it limits network access between two security domains
where is a network firewall placed	between trusted and untrusted hosts
what is a spoofing attack	a malicious party impersonates another party to bypass security
what is a tunneling attack	inserting malware behind a firewall and using it to create a tunnel to bypass the firewall
what are some threats to a firewall	tunneling and spoofing
what is a personal firewall	a software layer on a given host used to limit traffic to and from the host
what does the application proxy firewall do	understands the application protocol and can control them

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



what does the system-call firewall do	monitors all important system calls and applies the rules to them
how many divisions of computer security are there according to the U.S. Department of defense	four
what is encapsulated in the D division of computer security	minimal security
what is encapsulated in the C division of computer security	discretionary protection through auditing
What is the C division of computer security divided into	C1 and C2
what does the C1 division of computer security do	identifies cooperating users with the same level of protection
what does the C2 division of computer security do	allows user level control
what is encapsulated in the B division if computer security	discretionary protection through auditing with each object having its own unique sensitivity label
What is encapsulated in the A division of computer security	uses formal design and verification techniques to ensure security

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?



what is security based on in Windows XP	user accounts
what is created when a user logs in to a windows XP account	a security access token
what is included in the security access token when logged into windows xp	security id of the user, users groups and special privileges
Who gets a copy of the security access token when logged into a windows xp account	every process
what does the system do with the token after a user logs on to their windows XP account	checks to determine if access is allowed or denied
what model does Windows XP use to ensure access security	a subject model
what does a subject model do in Windows XP	tracks and manages permissions for each program that a user runs
each object in Windows XP has:	a security attribute defined by a security descriptor

UE18CS302_Unit 5_Revision_Class_Do_You_Know_That ?

For all the other relevant Unit 5 concepts refer to the lecture supplements and relevant videos on PESU Academy

THANK YOU

Nitin V Pujari
Faculty, Computer Science
Dean - IQAC, PES University

nitin.pujari@pes.edu

For Course Deliverables by the Anchor Faculty click on www.pesuacademy.com