ICSI MODULE 10:

Risk Assessment

10.1 Risk Assessment

Evaluating the security of a network always starts with a risk assessment. This involves considering the assets you are trying to protect, the threats against those assets, vulnerabilities in your systems, and what measures you can take to protect them. There are formulas for calculating risk.

The most basic calculation is for a single loss expectancy (SLE), or what impact a single loss will cause. This is calculated by multiplying the asset value (AV) by the exposure factor (EF). The exposure factor is a percentage value, representing how much of the asset's value you will lose in a given incident. For example, a laptop that has depreciated by 20 percent is now only worth 80 percent of its original value, should it be lost or stolen. This formula is

SLE = AV × EF

Therefore, if a laptop is purchased for $800, and depreciates by 10 percent a year, thus yielding an exposure factor of .9 (90 percent), then the SLE for a stolen or lost laptop is

SLE = 800 (AV) × .9 (EF)

SLE = $720

The next formula is the annualized loss expectancy (ALE). This represents how much loss you can expect from a particular issue in a year. The formula is SLE multiplied by annual rate of occurrence (ARO):

ALE = SLE × ARO

So, in the previous laptop example, if you think you will lose six laptops per year, the calculation is

ALE = 720 (SLE) × 6 (ARO)

ALE = $4320

As you can see, the math is actually quite simple. Another concept to understand is residual risk. Basically, this is how much risk is left over after you have taken all the steps you can to deal with the risk. In addition, that topic brings us to the issue of how you deal with a risk you have identified. There are really only four categories of responses:

- **Mitigation:** This means you take steps to lessen the risk. No matter what you do, there is likely to be some risk left. For example, if you are concerned about malware, then running antivirus is risk mitigation. This is the most common solution.
- **Avoidance:** This is difficult to do. It means you have zero risk. For example, if you are concerned about users downloading a virus from a website, the only way to completely avoid that is to not give them access to the web. This is not usually a viable solution.
- **Transference:** This is transferring the risk to someone else. The clearest example is cyber breach insurance. If you have such insurance, then the cost of a risk that is realized will be passed on to the insurance company.
- **Acceptance:** If the probability of the risk is very remote, or the cost of mitigation is higher than the cost of the risk being realized, you may choose to do nothing, and simply accept the risk.

10.2 Conducting an Initial Assessment

Disaster recovery, access rights, and appropriate policies are topics that are often overlooked by those new to security. To keep it simple and easy to remember, the stages of assessing a system's security can be separated into the "Six Ps":

- Patch
- Ports
- Protect
- Policies
- Probe
- Physical

You should note that these Six Ps are not yet standards in the security industry. They are provided here as a framework for approaching system security.

10.2.1 Patches

Patching a system is perhaps the most fundamental part of security. Therefore, when assessing any system's security, you should check to see whether a procedure is in place to govern the routine updating of all patches. And you should also, of course, check to see that the machines actually have current patches and updates. A written policy is essential, but when performing a security audit, you need to ensure that those policies are actually being followed.

As you are aware, operating system and application vendors occasionally discover security flaws in their products and release patches to correct these flaws. Unfortunately, it is not uncommon to find organisations in which patches have not been applied as late as 30 days or more after their release.

10.2.2 Ports

All communication takes place via some port (TCP/UDP). This is also true for many virus attacks. Frequently virus attacks will utilize some uncommon port to gain access to your system. Recall that ports 1 through 1024 are assigned and used for well-known protocols.

We have examined viruses, Trojan horses, and other dangers that operate on specific port numbers. If those ports are closed, then your vulnerability to these specific attacks is significantly reduced.

Unfortunately, some system administrators do not make a policy of closing unused ports. This is probably due to the fact that many administrators think that if the firewall is blocking certain traffic, then there is no need to block that port on individual machines. However, this approach provides you with only perimeter security, not layered security. By closing ports on individual machines, you provide a backup in case the firewall is breached.

As a rule, any port you do not explicitly need for operations should be closed, and communication should be disallowed on this port. A port is usually associated with a service. For example, an FTP service is often associated with ports 21 and 20. In order to close a port on an individual machine, you would need to shut down the service that uses that port. This means those unused services on servers and individual workstations should be shut down.

Both Windows and Linux have built-in firewall capability that will block certain ports. This means in addition to shutting down the particular unneeded services on all client machines, you should also shut down the ports.

You should also shut down any unused router ports in your network. If your network is part of a larger wide-area network (WAN), then it is likely you have a router connecting you to that WAN. Every open port is a possible avenue of entry for a virus or intruder. Therefore, every port you can close is one less opportunity for such attacks to affect your system.

The specifics of how to close a port on a router are particular to the individual router. The documentation that came with your router or your vendor should be able to provide you with specific instructions for how to accomplish this. If you have a vendor servicing your router, then you should make a list of all required ports and request that the vendor close all other ports on the router.

10.2.3 Protect

The next phase is to ensure that all reasonable protective software and devices are employed. This means at a minimum having a firewall between your network and the outside world. Clearly, more advanced firewalls such as stateful packet inspection firewalls are preferred. When auditing a system, you must note not only whether the system has a firewall, but also what type of firewall it has. You should also consider using an intrusion detection system (IDS) on that firewall and any web servers.

However, IDSs are the only way to know of imminent attacks, and there are free, open source IDSs available. For that reason, most experts highly recommend them. The firewall and IDS will provide basic security to your network’s perimeter, but you also need virus scanning. Each and every machine, including servers, must have a virus scanner that is updated regularly. The point has already been made that a virus infection is the greatest threat to most networks. As also previously discussed, it is probably prudent to consider anti-spyware software on all of your systems. This will prevent users of your network from inadvertently running spyware on the network.

Finally, a proxy server is a very good idea. It not only masks your internal IP addresses, but most proxy servers allow you to discover what websites users visit and put on filters for certain sites. Many security experts consider a proxy server to be as essential as a firewall.

In addition to protecting your network, you must also protect data that is transmitted, particularly outside your network. All external connections should be made via a VPN. Having data encrypted prevents hackers from intercepting the data via a packet sniffer. For more secure locations, you might even look for all internal transmissions to be encrypted as well.

In short, when assessing the protection of the network, check to see whether the following items are present, properly configured, and functioning:

- Firewall
- Antivirus protection
- Anti-spyware protection
- IDS
- Proxy server or NAT
- Data transmissions encryption

Be aware that the first two items are met in most networks. Any network that does not have a firewall or antivirus software is so substandard that the audit should probably stop at that point. In fact, it is unlikely that such an organisation would even bother to have a security audit. The IDS and data encryption options are probably less common; however, they should be considered for all systems.

10.2.4 Physical

In addition to securing your network from unwanted digital access, you must also ensure that it has adequate physical security. The most robustly secure computer that is left sitting unattended in an unlocked room is not at all secure. You must have some policy or procedure governing the locking of rooms with computers as well as the handling of laptops, tablets, and other mobile computer devices. Servers must be in a locked and secure room with as few people as is reasonably possible having access to them. Backup tapes should be stored in a fireproof safe. Documents and old backup tapes should be destroyed before disposal (e.g., by melting tapes, de-magnetizing hard disks, breaking CDs).

Physical access to routers and switches should also be tightly controlled. Having the most high-tech, professional information security on the planet but leaving your server in an unlocked room to which everyone has access is a recipe for disaster. One of the most common mistakes in the arena of physical security is co-locating a router or switch in a janitorial closet. This means that, in addition to your own security personnel and network administrators, the entire cleaning staff has access to your router or switch, and any one of them could leave the door unlocked for an extended period of time.

There are some basic rules you should follow regarding physical security:

- **Server rooms:** The room where servers are kept should be the most fire-resistant room in your building. It should have a strong door with a strong lock, such as a deadbolt. Only those personnel who actually have a need to go in the room should have a key. You might also consider a server room log wherein each person logs in when they enter or exit the room. There are actually electronic locks that record who enters a room, when they enter, and when they leave. Consult local security vendors in your area for more details on price and availability.
- **Workstations:** All workstations should have an engraved identifying mark. You should also routinely inventory them. It is usually physically impossible to secure them as well as you secure servers, but you can take a few steps to improve their security.

- **Miscellaneous equipment:** Projectors, CD burners, laptops, and so forth should be kept under lock and key. Any employee that wishes to use one should be required to sign it out, and it should be checked to see that it is in proper working condition and that all parts are present when it is returned.

These measures should be considered by all organisations. Some organisations go much further in ensuring physical security, and we will list some of the more extreme measures here. Most are probably more extreme than businesses require. However, if you deal with highly sensitive or classified data, then you might want to consider some or all of these measures.

- Biometric locks to all server rooms, or equipment storage rooms. Such locks are triggered by a fingerprint scan, and the identity of the person as well as the time they entered the room are recorded.
- All visitors to the building are logged in (both their entry and exit time) and are escorted by an employee at all times.
- All bags are inspected when personnel leave, or at least some bags are inspected at random.
- No portable devices that might record data are allowed on the premises. This includes USB drives, camera phones, or any device that might copy data or record screen images.
- All printing is logged. Who printed, the time the printing occurred, the document name, and the document size.
- All copying is logged, similarly to printing.

If you are in a situation that demands a greater than normal security level, these measures may be considered.

Probing the Network

10.3 Probing the Network

Perhaps the most critical step in assessing any network is to probe the network for vulnerabilities. This means using various utilities to scan your network for vulnerabilities. Some network administrators skip this step. They audit policies, check the firewall logs, check patches, and so on. However, the probing tools discussed in this section are the same ones that most hackers use.

If you want to know how vulnerable your network is, it is sensible to try the same tools that an intruder would use. In this section, we review the common scanning/probing tools. There are essentially three types of probes that are usually done. These are the same types of probes that skilled hackers use to evaluate your network:

- **Port scanning:** This is a process of scanning the well-known ports (there are 1024) or even all the ports (there are 65,535) and seeing which ports are open. Knowing what ports are open tells a lot about a system. If you see that 160 and 161 are open that tells you that the system is using SNMP. From the perspective of a network administrator, there should be no ports open that are not necessary.
- **Enumeration:** This is a process whereby the attacker tries to find out what is on the target network. Items such as user accounts, shared folders, printers, and so on are sought after. Any of these might provide a point of attack.
- **Vulnerability assessment:** This is the use of some tool to seek out known vulnerabilities, or the attacker might try to manually assess vulnerabilities. Some outstanding tools are available for vulnerability assessment.

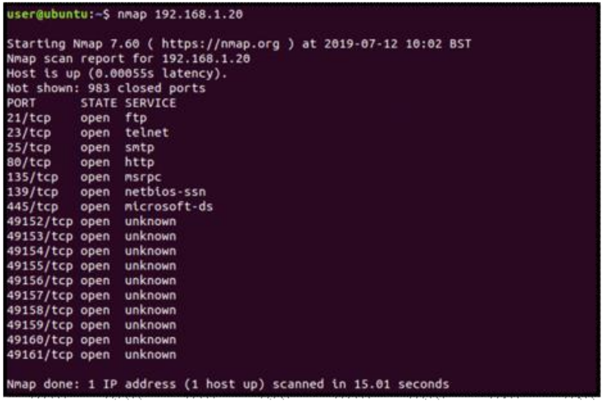
A number of tools are freely available on the Internet for active scanning. They range from the simple to complex. Anyone involved in preventing or investigating computer crimes should be familiar with a few of these. The most famous vulnerability scanners are Nessus, Qualys, Openvas, Netsparker, Acunetix, Nexpose Community, Retina and Core Impact.

Guided Exercise: Probing the Network

10.4 Guided Exercise: Probing the Network

Resources	
Files	None
Machines	Ubuntu Server, Windows Server, Windows 10

In this exercise you will use a tool called Nmap to scan and identify open ports on the Windows Server and Windows 10.
Login to Ubuntu Server. Once logged in run the command nmap 192.168.1.20 to find which ports are open on Windows Server.

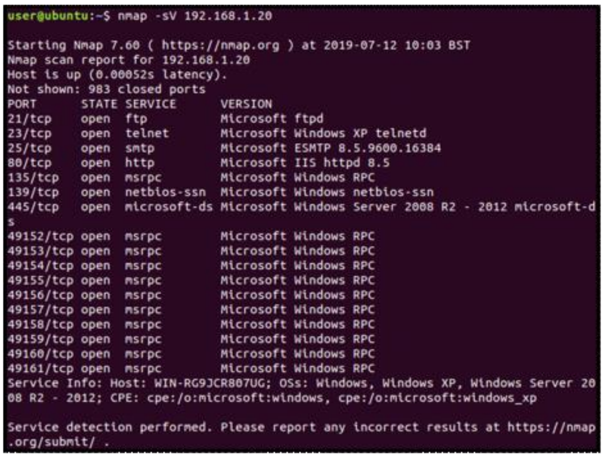


```
user@ubuntu:~$ nmap 192.168.1.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:02 BST
Nmap scan report for 192.168.1.20
Host is up (0.00055s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
49161/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

Determine the actual service running on each port by running the command “nmap –sV 192.168.1.20”

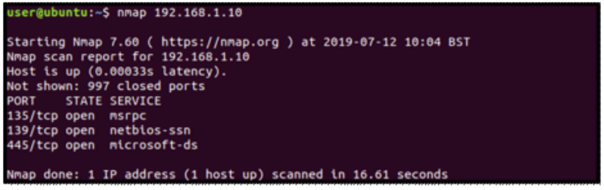


```
user@ubuntu:~$ nmap -sV 192.168.1.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:03 BST
Nmap scan report for 192.168.1.20
Host is up (0.00052s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
23/tcp    open  telnet       Microsoft Windows XP telnetd
25/tcp    open  smtp         Microsoft ESMTP 8.5.9600.16384
80/tcp    open  http         Microsoft IIS httpd 8.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-d
s
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-RG9JCR807UG; OSs: Windows, Windows XP, Windows Server 20
08 R2 - 2012; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
```

Run the command nmap 192.168.1.10 to identify the open ports on the Windows 10 machine.

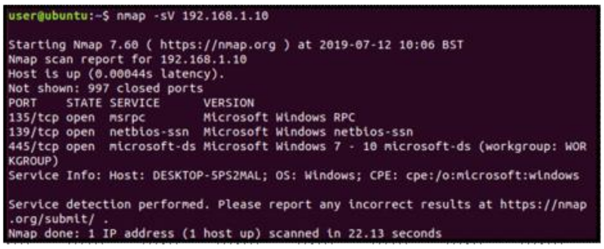


```
user@ubuntu:~$ nmap 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:04 BST
Nmap scan report for 192.168.1.10
Host is up (0.00033s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 16.61 seconds
```

Run the command nmap –sV 192.168.1.10 to identify theactual service running on the open ports.



```
user@ubuntu:~$ nmap -sV 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 10:06 BST
Nmap scan report for 192.168.1.10
Host is up (0.00044s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WOR
KGROUP)
Service Info: Host: DESKTOP-5PS2MAL; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.13 seconds
```

Vulnerabilities

10.5 Vulnerabilities

It is important to understand precisely what a vulnerability is. A vulnerability is some flaw in a system that an attacker could exploit to attack the system.

10.5.1 CVE

The most common list of vulnerabilities is the CVE list. Common Vulnerabilities and Exposures (CVE) is a list maintained by the Mitre Corporation at https://cve.mitre.org/. It is not only the most common, but also the most comprehensive vulnerability list. The CVE list was designed to provide a common name and description for a vulnerability. This allows security professionals to communicate effectively about vulnerabilities. In the past, CVEs had been designated by a CVE ID in the format of CVE-YYYY-NNNN. This format only allows 9,999 unique identifiers per year. The new format is CVE prefix + Year + Arbitrary Digits and allows for any number of digits.

10.5.2 NIST

The U.S. National Institute of Standards and Technology maintains a database of vulnerabilities that you can access at https://nvd.nist.gov/. NIST also uses the CVE format. For example, CVE-2017-12371 is described as "A 'Cisco WebEx Network Recording Player Remote Code Execution Vulnerability' exists in Cisco WebEx Network Recording Player for Advanced Recording Format (ARF) and WebEx Recording Format (WRF) files. A remote attacker could exploit this by providing a user with a malicious ARF or WRF file via email or URL and convincing the user to launch the file. Exploitation of this could cause an affected player to crash and, in some cases, could allow arbitrary code execution on the system of a targeted user."

10.5.3 OWASP

The Open Web Application Security Project is the standard for web application security. They publish a number of important documents. For our current purposes, the most important is their top 10 list, located at https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. Every few years they publish a top 10 web application vulnerabilities list. This list contains the actual vulnerabilities most frequently found in web applications.

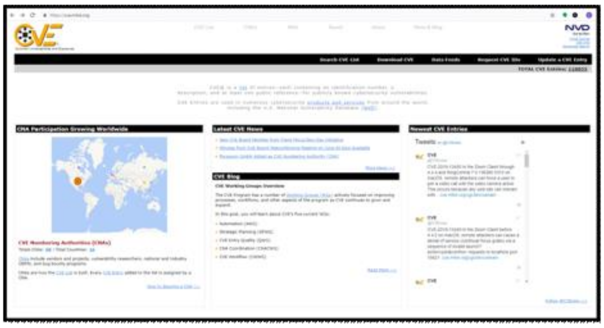
Guided Exercise: Learning about Vulnerabilities

10.6 Guided Exercise: Learning about Vulnerabilities

Resources	
Files	None
Machines	None

In this exercise you will identify details regarding a specific vulnerability. You will need to use a web browser for this exercise not in the lab environment.

Open a web browser and type the following link https://cve.mitre.org.



Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

TOTAL CVE Entries: 118855

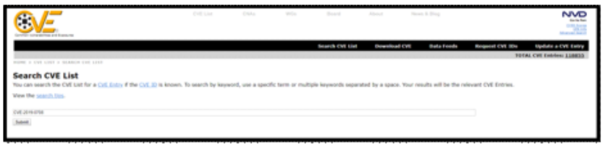
CNA Participation Growing Worldwide

Latest CVE News

CVE Blog

Newest CVE Entries

From the menu click on Search CVE List. In the search box enter CVE-2019-0708 and click on Submit.



Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

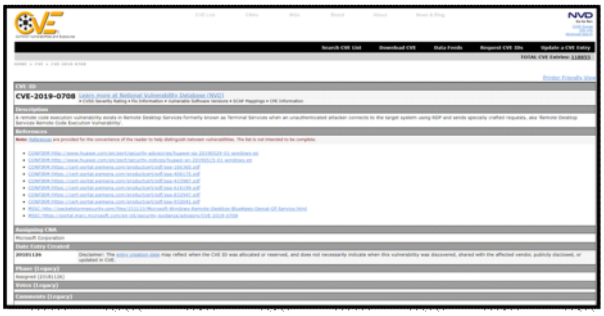
TOTAL CVE Entries: 118855

Search CVE List

CVE-2019-0708

Submit

One entrie will be returned and click on it to learn more about that specific vulnerabilitiry.



Search CVE List Download CVE Data Feeds Request CVE IDs Update a CVE Entry

TOTAL CVE Entries: 118855

CVE-ID

CVE-2019-0708 Learn more at National Vulnerability Database (NVD)

Description

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

References

Assigning CNA

Microsoft Corporation

Date Entry Created

Read the description carefully and you will note that the vulnerability affects the Remote Desktop Services on Windows machines.

Documenting Security

10.7 Documenting Security

By this point, you are undoubtedly aware that you need to document your security. However, you may not be clear as to exactly what documents you should have. Unfortunately, this is an area of network security for which there are not industry standards. There is no manual on documentation.

10.7.1 Physical Security Documentation

You should have a document that lists physical security that is in place. Where are the machines located? This means documenting the location of every single server, workstation, router, hub, or other device. The documentation should contain serial numbers as well as what personnel have access to them. If a device is in a locked room, then the documentation should also have a list of who has keys to that room.

If you log entry to secured rooms, then copies of those logs should be filed with your other physical documentation. In even a medium-sized network, this would quickly become a rather hefty file rather than a single document. You may consider implementing some method whereby after a certain period of time (1 year, for example) the access logs are archived, then after a longer period of time (such as 3 years) they are destroyed.

10.7.2 Policy and Personnel Documentation

All policies must be on file. Any revisions should be filed along with the originals. Assuming you have employees sign an agreement stating they are aware of the policies (and you absolutely should), then copies of that should also be on file.

Along with policy documentation, you should keep a list of personnel along with what items they have access to. This includes physical access as well as any machines (servers, workstations, or routers) that they have login rights. You should also note what level of access they have (standard user, power user, administrator, and so on).

10.7.3 Probe Documents

Any time you conduct any security audit, a report of that audit should be filed. Even audits done by outside consultants should be kept on file. The audit report should include any flaws found, and have a follow-up report of what steps were taken to correct them.

Should you have a security incident (such as a virus infection or intruder), there should be at least a brief memo summarizing what occurred. That document should state what the security incident was, when it occurred, what machines were affected, and how it was corrected.

10.7.4 Network Protections Documents

The most obvious item to document is exactly what network protections you have in place. This documentation should detail the following:

- What firewall are you using and how is configured.
- What IDS are you using and how is configured.
- What antivirus and/or anti-spyware you are using.
- Have you configured any honeypots?
- What individual machine security measures (such as workstation firewalls) have you taken?

One note of caution: These documents should be kept under lock and key, with only limited access. If an intruder were to get access to these documents, they would have a detailed analysis of your network’s weaknesses.

QUIZ:

- 1.What is NOT a primary reason for documenting your security activity and audits?
- 2.You should have a document that lists physical security is in place
- 3.Which of the following is the most fundamental aspect of security?
- 4.All employees within a company must have access to the server room.
- 5.Which of the following is the least necessary security device/software
- 6.Virus attacks utilize uncommon ports to gain access to a system.
- 7.Ports 1 through 1024 are NOT assigned and used for well-known protocols
- 8.Open Web Application Security Project is the standard for risk assessment.
- 9.All visitors to the building must be logged in and escorted by an employee at all times.
- 10.which of the following best describes risk assessment.