CSUF SPRING 2021

INTRODUCTION TO COMPUTER SECURITY CPSC 353 SECTION 02

ASSIGNMENT #2

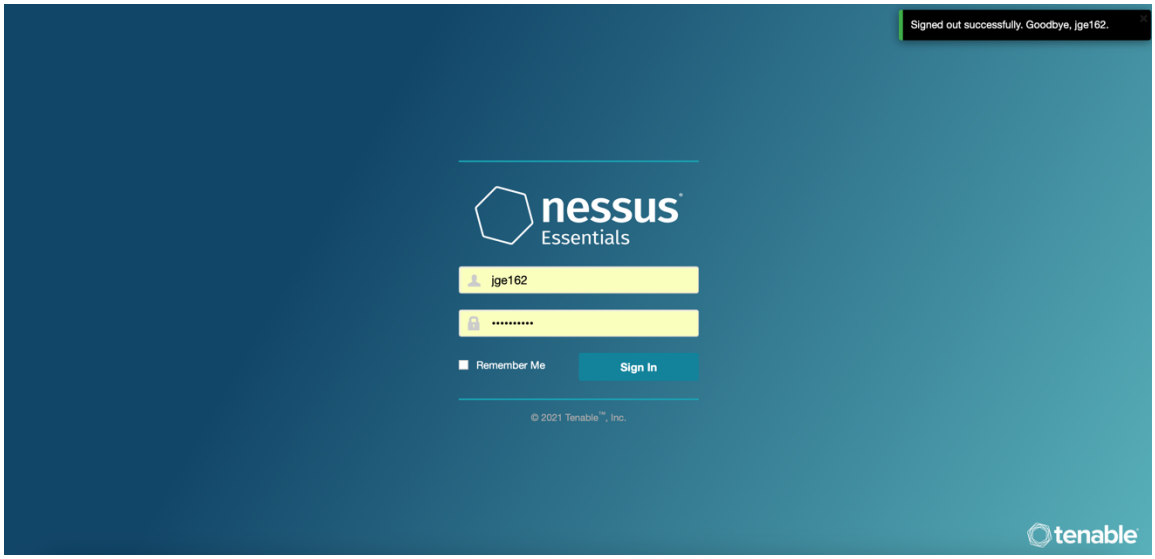
PROFESSOR: LINH TRINH

Jeremy Escobar

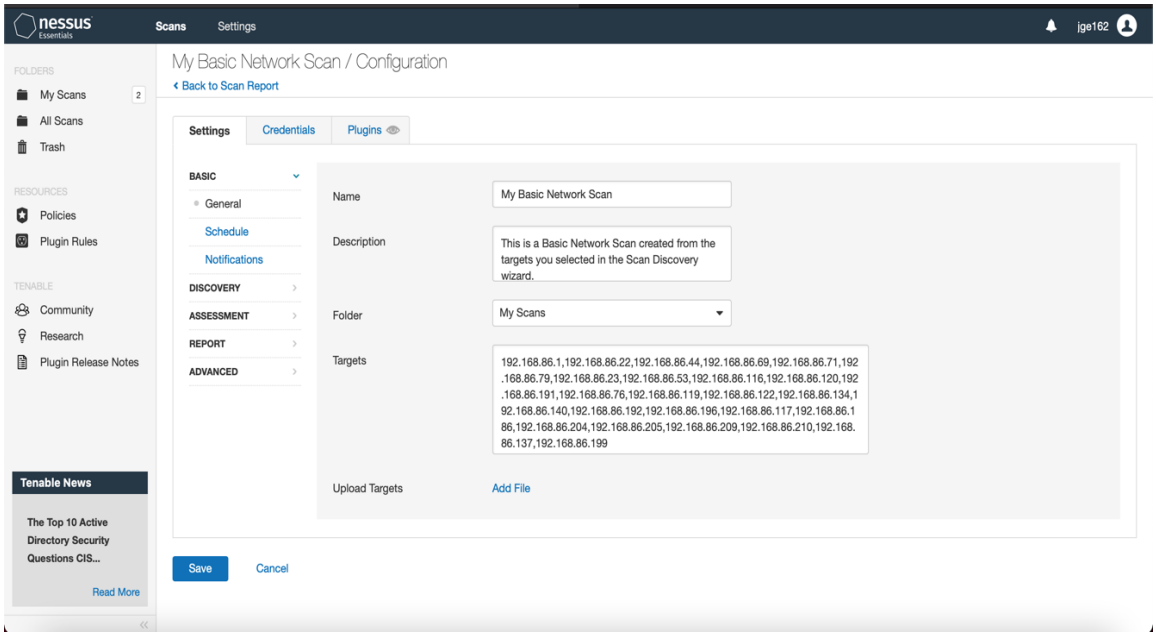
Create a Basic Network Scan to assess the vulnerabilities of the hosts/devices on your home network. You can specify a range of host IP addresses for the scan.

Provide the followings in your report. Refer to the Appendix section for examples of screen captures.

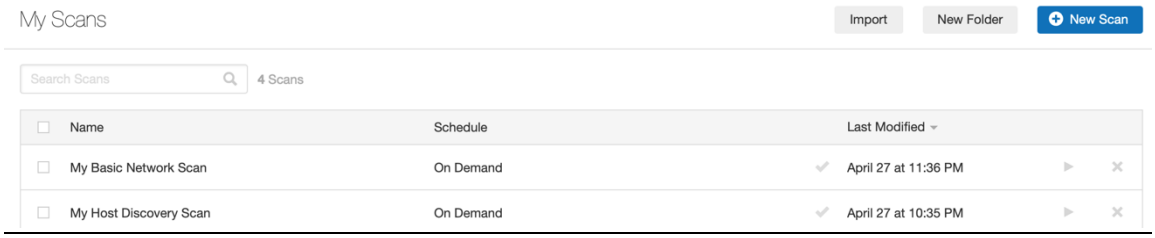
1. **A screen capture showing your Nessus login screen.**

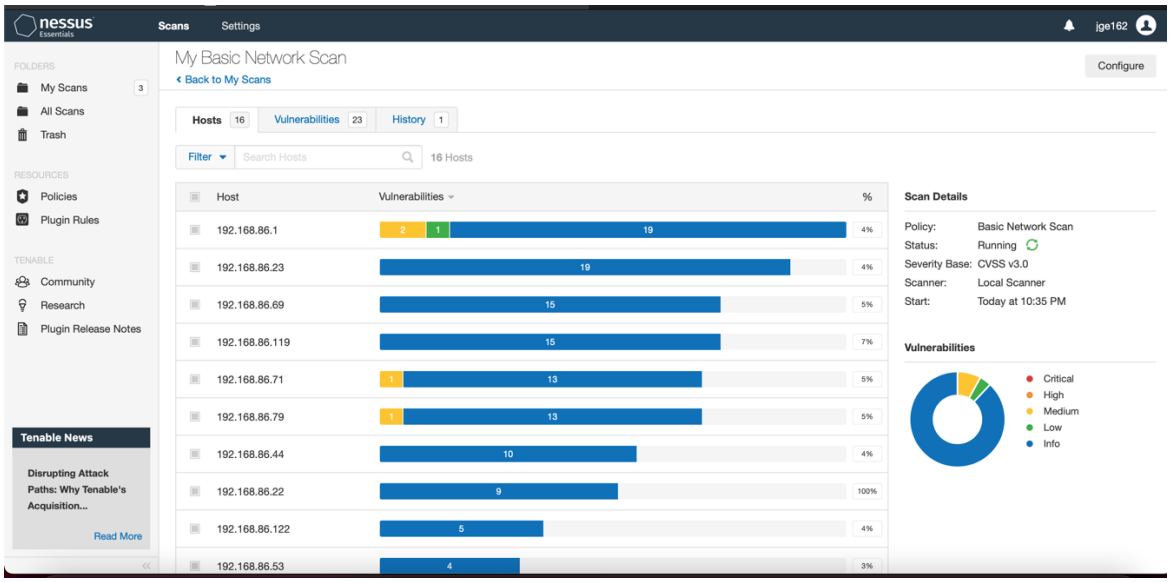


2. **A screen capture showing the creation of a new Basic Network Scan.**

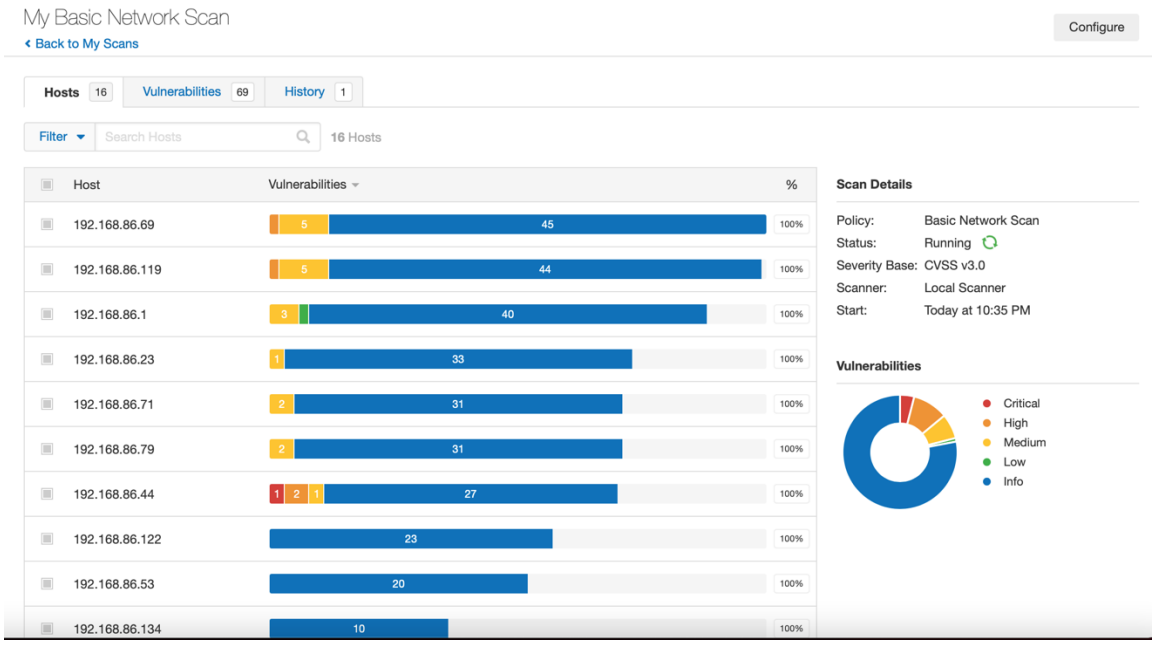


3. A screen capture showing the completion of the scan.





4. **A screen capture showing the result summary of the scan.**



5. **Identify the host/device which has the highest number of vulnerabilities.**

    a. **Briefly describe this host/device**
    What it is (PC, tablet, mobile phone, router, server, etc.…), the operating system type if applicable.

The host device identified with the most and highest vulnerabilities was an Apple Tv designed by apple computer. The device is not a pc but a pc of hardware running Apple TV OS software 7.0.3 version.

    b. **What is the highest level of the vulnerability for this host/device? (critical, high, medium, low, info)? Provide a screen capture to illustrate.**

The Apple Tv had multiple vulnerabilities four in all. Critical, high, high and Medium.

c. **Describe the details of the vulnerability and provide a screen capture to support the provided details.**

Multiple vulnerabilities exist due to software design issues developed by Apple. The most serious is stated to be "the most serious of which can result in arbitrary code execution."

CRITICAL Apple TV < 7.0.3 Multiple Vulnerabilities

Description

According to its banner, the remote Apple TV device is a version prior to 7.0.3. It is, therefore, affected by the following vulnerabilities :

- Multiple memory corruption issues exist, related to the included version of WebKit, that allow application crashes or arbitrary code execution. (CVE-2014-3192, CVE-2014-4459, CVE-2014-4466, CVE-2014-4468, CVE-2014-4469, CVE-2014-4470, CVE-2014-4471, CVE-2014-4472, CVE-2014-4473, CVE-2014-4474, CVE-2014-4475, CVE-2014-4476, CVE-2014-4477, CVE-2014-4479)

- A state management issue exists due to improperly handling overlapping segments in Mach-O executable files. A local user can exploit this issue to execute unsigned code. (CVE-2014-4455)

- A security bypass issue exists due to improper validation of SVG files loaded in an IMG element. An attacker can load a CSS of cross-origin resulting in information disclosure. (CVE-2014-4465)

- An issue exists due to the symbolic linking performed by the 'afc' command which allows an attacker to access arbitrary files on the system. (CVE-2014-4480)

HIGH Apple TV < 7.0.2 Multiple Vulnerabilities

Description

According to its banner, the remote Apple TV device is a version prior to 7.0.2. It is, therefore, affected by the following vulnerabilities :

HIGH Apple TV < 7 Multiple Vulnerabilities

Description

According to its banner, the remote Apple TV device is a version prior to 7. It is, therefore, affected by multiple vulnerabilities, the most serious of which can result in arbitrary code execution.

Solution

Upgrade to Apple TV 7 or later. Note that this update is only available for 3rd generation and later models.

MEDIUM Apple TV < 7.0.1 Multiple Vulnerabilities (POODLE)

Description

According to its banner, the remote Apple TV device is a version prior to 7.0.1. It is, therefore, affected by the following vulnerabilities :

- An error exists related to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. A man-in-the-middle attacker can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. This is also known as the 'POODLE' issue. (CVE-2014-3566)

- A error exists that permits unencrypted connections for Human Interface Device (HID) class Bluetooth Low Energy accessories. This allows a local attacker to spoof another legitimate Bluetooth device to bypass pairing. (CVE-2014-4428)

Solution

Upgrade to Apple TV 7.0.1 or later. Note that this update is only available for 3rd generation and later models.

d. **What is the recommended action? Provide a screen capture to support the answer.**

Every recommended action given is to upgrade Apple TV OS.

Solution

Upgrade to Apple TV 7.0.2 or later. Note that this update is only available for 3rd generation and later models.

Solution

Upgrade to Apple TV 7.0.3 or later. Note that this update is only available for 3rd generation and later models.

Solution

Upgrade to Apple TV 7.0.2 or later. Note that this update is only available for 3rd generation and later models.

Solution

Upgrade to Apple TV 7 or later. Note that this update is only available for 3rd generation and later models.

e. **What are the available solutions? Provide a screen capture to support the answer.**

Available solutions are like what is previously screen shotted for letter d above. Upgrade the TV OS but the only way to do that is to purchase the newer generation of Apple tv device.

f. **Which solution you are going to choose to minimize or eliminate this vulnerability and why?**

I will not be fixing the issue because I do not have the funds needed to purchase a 3rd generation Apple Tv so I can get newer OS. So, the vulnerabilities will remain for the foreseeable future unless apple decides to support their older hardware with newer software.

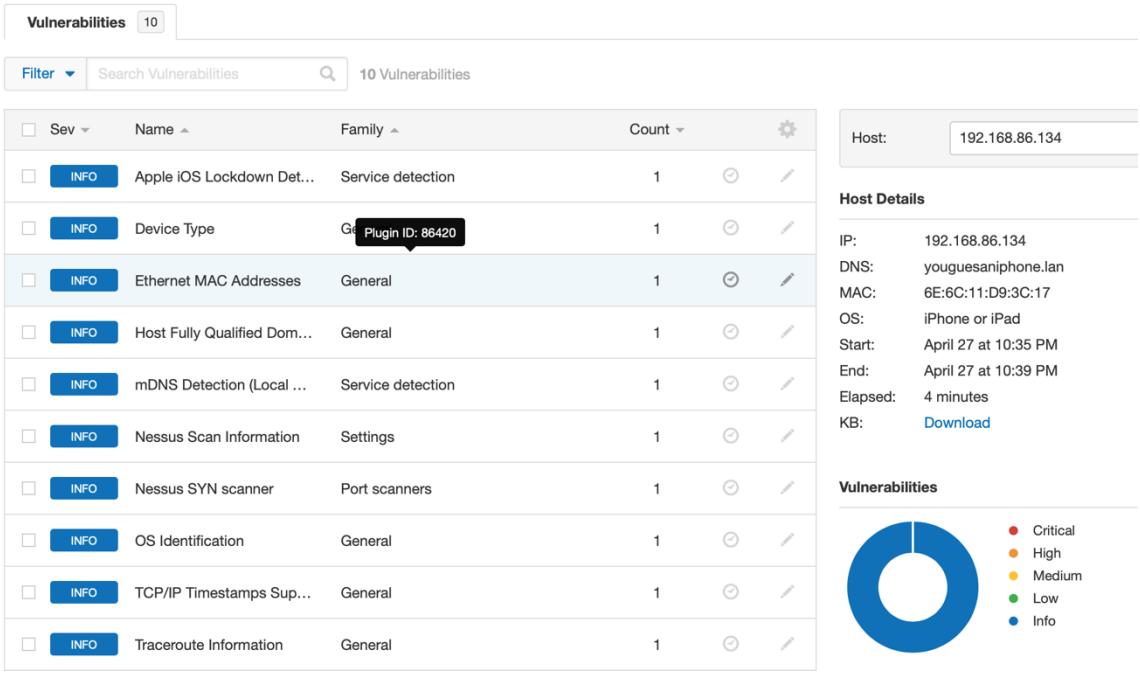
6. **Identify the host/device which has the lowest number of vulnerabilities.**

   a. **Briefly describe this host/device**
   What it is (PC, tablet, mobile phone, router, server, etc.…), the operating system type if applicable.

My iPhone was the device with the lowest number of vulnerabilities. It had 10 total non-critical. My iPhone is running Apple's latest iOS 14.5 public release version.

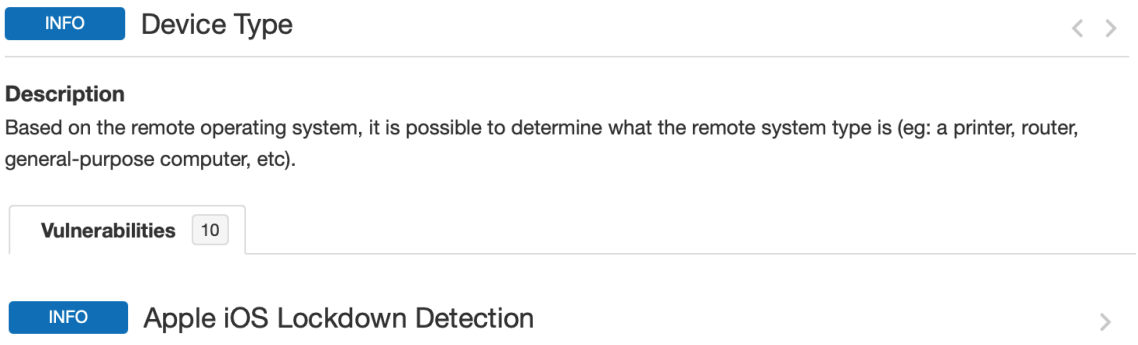
   b. **What is the highest level of the vulnerability for this host/device? (critical, high, medium, low, info)? Provide a screen capture to illustrate.**

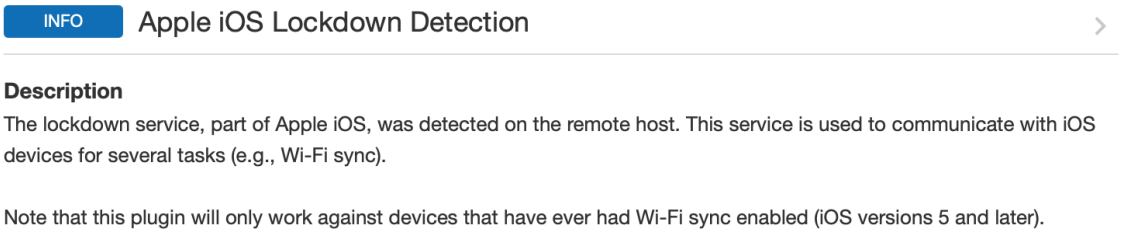
Highest level was info, with 10 total alerts.

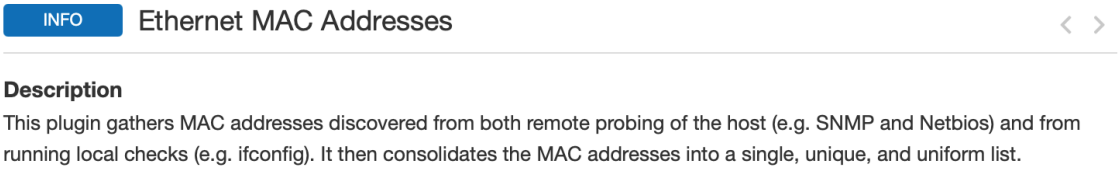


c. **Describe the details of the vulnerability and provide a screen capture to support the provided details.**

It appears none of the “info” vulnerabilities seem to be dangerous but otherwise more of a checklist completed by Nessus. One alert asks to change port used for DNS to 5353.

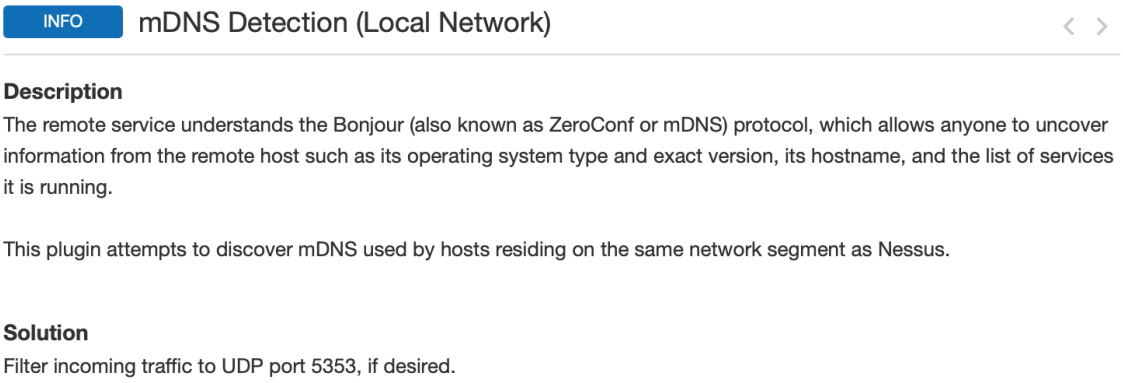






d. **What is the recommended action? Provide a screen capture to support the answer.**

Recommended action is to filter incoming traffic to a different port (DNS). Another mention is to target using a IP filter.



INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

e. **<u>What are the available solutions? Provide a screen capture to support the answer.</u>**

Solutions are to protect target device and filter incoming traffic with an IP filter.

INFO mDNS Detection (Local Network)

Description

The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

This plugin attempts to discover mDNS used by hosts residing on the same network segment as Nessus.

Solution

Filter incoming traffic to UDP port 5353, if desired.

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

f. **Which solution you are going to choose to minimize or eliminate this vulnerability and why?**

I do not have an ability on an iPhone to use an IP filter. Also, for the DNS to change to port 5353 I do not see a way to do that on an iPhone either. So, I cannot fix these issues based on the closed operating system Apple uses on their iPhone iOS operating systems.

7. **Describe several uses of Nessus vulnerability scanner.**

Nessus scanner is very in-depth scan of all your target devices using internet as access points. I look at the devices OS, device type, checks routers and more. While checking these devices it checks for vulnerabilities that are relevant to your security. It gives suggestions on how to fix issues and methods/links to company websites when available.

8. **Which feature of Nessus did you find the most useful and why?**

I like the fact that the scanner gave you suggested action to protect your security. Essentially the full scan feature was my favorite.

9. **Which feature of Nessus did you find the most difficult to use and why?**

For me the installation process and first scan proved difficult. I did not know how to search an IP range and had to figure that out with maybe failing it three times. I eventually had to go on my MacBook and see what the IP address was and then start from 0 and go to 100. e.g. (192.168.86.0 – 192.168.86.100). Then finally once I got the results u was very happy.

Read the National Institute of Standards Technology Standard, “Chapter 20 Assessing and Mitigating the risks to a hypothetical computer system”, An Introduction to Computer Security: The NIST Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Provide answers to the following questions:

1. **What are the different types of payroll fraud threats?**

Submitting fraudulent time sheets for hours or days not worked, or for pay periods following termination or transfer of employment. The former may take the form of overreporting compensatory or overtime hours worked, or underreporting vacation or sick leave taken. Alternatively, attempts have been made to modify time sheet data after being entered and approved for submission to payroll.

Falsifying or modifying dates or data on which one's "years of service" computations are based, thereby becoming eligible for retirement earlier than allowed, or increasing one's pension amount.

Creating employee records and time sheets for fictitious personnel, and attempting to obtain their paychecks, particularly after arranging for direct deposit.

2. **What are the control measures currently in use to protect against payroll fraud?**

Authorized users are assigned a secret log-in ID and password, which they must not share with anyone else. They are expected to comply with all of HGA's password selection and security procedures (e.g., periodically changing passwords). Users who fail to do so are subject to a range of penalties.

Attend a security awareness and training course or complete an interactive computer-aided-instruction training session and sign an acknowledgment form indicating that they understand their security responsibilities.

3. **What are the vulnerabilities related to payroll fraud found by the risk assessment team?**

Falsified Time Sheets, Unauthorized Access, Bogus Time and Attendance Applications, Unauthorized Modification of Time, and Attendance Data

4. **What's the recommendation by the risk assessment team?**

Require stronger I&A for dial-in access or, alternatively, that a restricted version of the mail utility be provided for dial-in, which would prevent a user from including files in outgoing mail messages.

replace its current modem pool with encrypting modems, and provide each dial-in user with such a modem; and

work with the mainframe agency to install a similar encryption capability for server-to-mainframe communications over the WAN.

To remove the vulnerabilities related to payroll fraud, the risk assessment team recommended the use of stronger authentication mechanisms based on smart tokens to generate one-time passwords that cannot be used by an interloper for subsequent sessions. Such mechanisms would make it very difficult for outsiders.

5. **What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.**

After reviewing the risk assessment, HGA's management concluded that the agency's current safeguards against payroll errors and against accidental corruption and loss of time and attendance data were adequate. Thus, the costs and procedural difficulties of implementing such controls would be substantial.

6. **What are the different types of payroll errors?**

Errors in the entry of time and attendance data; failure to enter information describing new employees, terminations, and transfers in a timely manner; accidental corruption or loss of time and attendance data; or errors in interagency coordination and processing of personnel transfers.

7. **What are the control measures currently in use to protect against payroll errors?**

In addition, each department has one or more Time and Attendance Supervisors who are authorized to review these reports for accuracy and to approve them by running another server program that is part of the time and attendance application. The data are then subjected to a collection of "sanity checks" to detect entries whose values are outside expected ranges.

8. **What are the vulnerabilities related to payroll error found by the risk assessment team?**

The greatest source of vulnerabilities, however, is the mainframe.

9. **What's the recommendation by the risk assessment team?**

However, previous audits have shown that the difficulties of system administration may present some opportunities for intruders to defeat access controls.

10. **What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.**

test

11. **What are the different types of interruption of operations?**

HGA's building facilities and physical plant are several decades old and are frequently under repair or renovation. As a result, power, air conditioning, and LAN or WAN connectivity for the server aretypicallyinterruptedseveraltimesayearforperiodsofuptooneworkday. For example, on several occasions, construction workers have inadvertently severed power or network cables. Fires, floods, storms, and other natural disasters can also interrupt computer operations, as can equipment malfunctions.

12. **What are the control measures currently in use to protect against interruption of operations**?

COG is responsible for developing and maintaining a contingency plan that sets forth the procedures and facilities to be used when physical plant failures, natural disasters, or major equipment malfunctions occur sufficient to disrupt the normal use of HGA's PCs, LAN, server, router, printers, and other associated equipment.

The plan prioritizes applications that rely on these resources, indicating those that should be suspended if available automated functions or capacities are temporarily degraded. COG personnel have identified system software and hardware components that are compatible with those used by two near by agencies. HGA has signed an agreement with those agencies, whereby they have committed to reserving spare computational and storage capacities sufficient to support HGA's system-based operations for a few days during an emergency.

No communication devices or network interfaces may be connected to HGA's systems without written approval of the COG Manager. The COG staff is responsible for installing all known security-related software patches in a timely manner and for maintaining spare or redundant PCs, servers, storage devices, and LAN interfaces to ensure that at least 100 people can simultaneously

13. **What are the vulnerabilities related to continuity of operations found by the risk assessment team?**

The risk assessment team found that many of the risks to which HGA is exposed stem from (1) the failure of individuals to comply with established policies and procedures or (2) the use of automated mechanisms whose assurance is questionable because of the ways they have been developed, tested, implemented, used, or maintained. The team also identified specific vulnerabilities in HGA's policies and procedures for protecting against payroll fraud and errors, interruption of operations, disclosure and brokering of confidential information, and unauthorized access to data by outsiders.

14. **What's the recommendation by the risk assessment team?**

The risk assessment team found that many of the risks to which HGA is exposed stem from (1) the failure of individuals to comply with established policies and procedures or (2) the use of automated mechanisms whose assurance is questionable because of the ways they have been developed, tested, implemented, used, or maintained. The team also identified specific vulnerabilities in HGA's policies and procedures for protecting against payroll fraud and errors, interruption of operations, disclosure and brokering of confidential information, and unauthorized access to data by outsiders.

15. **What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.**

If a division relies exclusively on computer resources maintained by COG (e.g., the LAN), it need not duplicate COG's contingency plan, but is responsible for reviewing the adequacy of that plan. If COG's plan does not adequately address the division's needs, the division must communicate its concerns to the COG Director. In either situation, the division must make known the criticality of its applications to the COG. If the division relies on computer resources or services that are not provided by COG, the division is responsible for (1) developing its own contingency plan or (2) ensuring that the contingency plans of other organizations (e.g., the WAN service provider) provide adequate protection against service disruptions.

16. **What are the different types of network threats? Give a scenario where HGA had experienced a network related attack**

the Internet, (2) the Interagency WAN, and (3) the public-switched (telephone) network. Although these networks are a source of security risks, connectivity with them is essential to HGA's mission and to the productivity of its employees; connectivity cannot be terminated simply because of security risks. In one case, an attacker made use of a bug in an e-mail utility and succeeded in. acquiring System a significant breach. HGA found no evidence that the. Attacker attempted to exploit these privileges before being discovered two days later.

17. **What are the control measures currently in use to protect against network threats?**

Attend a security awareness and training course or complete an interactive computer-aided-instruction training session and (2) sign an acknowledgment form indicating that they understand their security responsibilities.

Authorized users are assigned a secret log-in ID and password, which they must not share with anyone else. They are expected to comply with all of HGA's password selection and security procedures (e.g., periodically changing passwords). Users who fail to do so are subject to a range of penalties.

18. **What network-related vulnerabilities found by the risk assessment team?**

The assessment recommended that HGA improve its security awareness training (e.g., via mandatory refresher courses) and that it institutes some form of compliance audits. The training should be sure to stress the penalties for noncompliance. It also suggested installing "screen lock" software on PCs that automatically lock a PC after a specified period of idle time in which no keystrokes have been entered; unlocking the screen requires that the user enter a password or reboot the system.

The assessment recommended that HGA modify its information-handling policies so that employees would be required to store some kinds of disclosure-sensitive information only on PC local hard disks (or floppies), but not on the server. This would eliminate or reduce risks of LAN eavesdropping.

19. **What's the recommendation by the risk assessment team?**

require stronger I&A for dial-in access or, alternatively, that a restricted version of the mail utility be provided for dial-in, which would prevent a user from including files in outgoing mail messages.

Replace its current modem pool with encrypting modems and provide each dial-in user with such a modem.

And work with the mainframe agency to install a similar encryption capability for server-to-mainframe communications over the WAN.

20. **What are the final decisions made by HGA management? Justify their decisions based on cost benefit analysis.**

As with previous risk assessment recommendations, HGA's management tasked COG to analyze the costs, benefits, and impacts of addressing the vulnerabilities identified in the risk assessment. HGA eventually adopted some of the risk assessment's recommendations, while declining others. In addition, HGA decided that its policy on handling time and attendance information needed to be clarified, strengthened, and elaborated, with the belief that implementing such a policy would help reduce risks of Internet and dial- in eavesdropping. Thus, HGA developed and issued a revised policy, stating that users are individually responsible for ensuring that they do not transmit disclosure-sensitive information outside of HGA's facilities via e-mail or other means. It also prohibited them from examining or transmitting e-mail containing such information during dial-in sessions and developed and promulgated penalties for noncompliance.