!! 4B TUT

Saturday, 3 August 2024 10:19 pm

Q1) Explain the difference Ingress Filtering & Egress filtering firewalls

- **Ingress Filtering**
  - **Examines packets coming into the organisation**
- **Egress filtering**
  - **Examines packets going out of the organisation**

Q2) Firewalls can be deployed to create three security zones to provide layers of defence

A) State & explain the three security zones

- **Untrusted zone**
  - **The outermost zone which is the internet**
- **Trusted zone**
  - **Internal network, i.e. inner secured corporate network**
- **Semi-trusted zone**
  - **Demilitarized zone (DMZ), also known as perimeter network**
  - **Lies btw the internal network (trusted zone) and the Internet (untrusted zone)**

B) Using a diagram, explain how you would deploy 2 firewalls to create the above security zones

Q3) Explain the purpose of the Demilitarized zone (DMZ)

- **The purpose of a DMZ is to add an additional layer of security to an organization's local area network**
- **Outside users can access the DMZ but cannot access the secure internal network**
- **Any services that are being provided to Internet users are placed in the DMZ**

Q4) Explain what is an Intrusion Detection System (IDS)?

- **An intrusion detection system (IDS) is a device/software application that monitors network and/or system activities for possible incidents**
- **Incident can be malicious activities/policy violations**

Q5) List some of the activities which Host-Based IDS (HIDS) & Network-Based IDS (NIDS) can monitor?

- HIDS
  - Login at odd hours
  - Login authentication failures
  - Add new user accounts (especially w/ admin rights)
  - Modification/access to critical system files (such as registry)
  - Start/stop processes (such as anti-virus)
  - Privilege escalation
- NIDS
  - Denial-of-Service attacks
  - Port scans or sweeps
  - Malicious content in data payload of packets
  - Vulnerability scanning

Q6) What are some advantages and disadvantages of Host IDS (HIDS) and Network IDS (NDIS)?

- HIDS
  - Advantages
    - Can analyse activities at a high level of details
    - Can examine data aft decryption
    - Can reduce false positive rates
  - Disadvantages
    - Consume local resources (e.g. processing time, storage & memory)
    - High cost of ownership in terms of deployment and maintenance
    - Has a focused view and cannot relate to activity arnd it

- NIDS
  - Advantages
    - Lower cost of ownership, deployment & maintenance
    - NIDSs are mostly passive devices, hence minimum overheads on network
    - Has visibility into all network traffic and can correlate attacks among multiple systems.
  - Disadvantages
    - Ineffective when traffic is encrypted
    - Must be able to handle high volumes of traffic

Q7) In IDS, explain the difference btw false positives and false negatives. Explain why they are bad
- False positives
  - IDS matches a pattern and generates an alarm for non-hostile traffic
  - Too many false positives will cause security administrators to lose confidence in the IDS
- False negatives
  - Hostile activity that does not match an IDS signature and goes undetected
  - IDS fails to identify a real incident (e.g. an attack). Hence, allowing the incident to cause damage to systems/networks

Q8) What is the difference btw an IDS and a firewall?
- Firewall is a device (or software) that sits btw a local network and the Internet.
  - Main function is to block unauthorized access while permitting authorized communications.
- An IDS is a device (or software) installed on the network (NIDS) or host (HIDS).
  - Main function is to detect and report intrusion attempts inside the host/network
- Firewall is like a security guard at the gate while an IDS is a security camera inside the compound

!! 5A TUT

Friday, 2 August 2024 10:36 pm

Q1) Which statement best describes a computer server?
- A computer designed to process requests and deliver data to another computer

Q2) Which of the fllwing is a major part of the "Server hardening"?
- To apply Operating System updates

Q3) Which of the fllwing is NOT a step to configure security settings?
- Block all attempts to access Internet

Q4) List any 4 types of servers commonly used today
- Web Server
- Domain Name System (DNS) Server
- Email Server
- Database Server
- Application Server
- File Server

Q5) List some of the functions of an operating system
- Managing resources
  - Manage resources of a computer such as printer, mouse, keyboard, memory, disk drives and monitor
- Providing User Interface
  - Graphical user interface (GUI) makes it very easy to use
- Running Applications
- Ability to multitask by running many applications at once
- Support for built-in Utility Programs
- Uses the utility program to identify problems, repair damaged files, locate lost files and back up data

Q6) Describe the FIVE step processes for protecting operating system
1. Develop the security policy
2. Perform host software baselining
3. Configure operating system security and settings
4. Deploy the settings
5. Implement patch management

Q7) Name any 3 security policies that a modern organization shld establish
- Acceptable terms of use of systems
- Basic Anti-virus requirements
- User password management
- Wireless communication restrictions
- Disposal and destruction of resources

!! 5B TUT

Saturday, 3 August 2024 8:35 am

Q1) Which statement best describes server hardening?
- **Process of securing the server and its operating system**

Q2) Picking the first letter of each word in a sentence to create a password is _____
- **Passphrase**

Q4) How are passwords stored in database?
- **They are hashed**

Q5) What are some security measures to consider in order to harden a server
- **Securing Hardware**
- **Securing Operating System**
- **Securing Applications (such as Databases, Web Server, Email Servers, etc)**
- **Implement Access Control Policies**

Q6) Jane set her password for her login credential to "pA5$W0rd".
A. List some advantages and disadvantages of this password.
B. Can you suggest a better password?

a) **Advantages**
- **At least 8 characters**
- **Strong password w/ good complexity - special char, upper and lower case characters and numbers**

Disadvantages
- **Difficult to remember**
- **Commonly used by like-minded people**

b) **A better password is to use passphrase. Extracting the first letter of each word to form a password**
e.g. I love my fish tank of 3 guppies! -
iLmfto3g!

Q7) List some guidelines when implementing a password policy for an organisation
- **Min password length**
- **Password complexity**
- **Password history**
- **Min and max password age**

Q8) What are some common methods of cracking passwords?
- **Brute force Attack**
- **Dictionary Attack**
- **Rainbow Tables**
- **Social Engineering**

!! 6A TUT

Saturday, 3 August 2024 12:45 pm

Q1) HTTP is said to be stateless.

A) What does that mean?

- **It means that a HTTP server (i.e. web server) is not required to maintain any state info abt the HTTP requests that it receives from the web browser.**
  example of state info - who is logged in, what's in the shopping cart, etc.

B) What are the implications of web application on the web server?

- **W/o state, the web application (which resides on the web server) is not able to keep track and differentiate each user. Hence, not able to provide each user w/ personalised and customised content**
  e.g.
  - **Facebook will not be able to show personalised feeds**
  - **Online banks will not be able to show user acc balance etc.**
  - **Online shops will not be able to maintain user shopping cart**

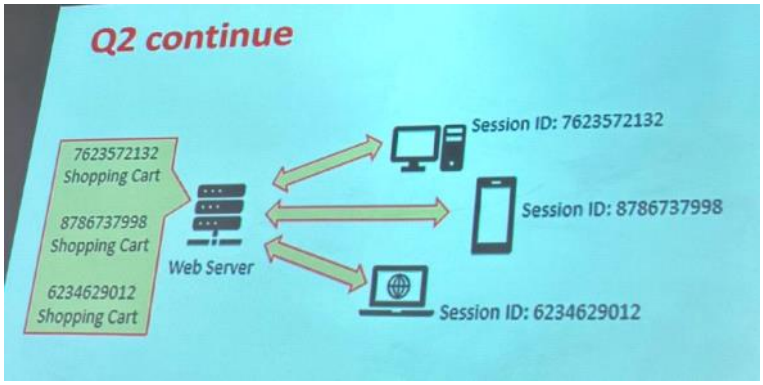
Q2) Sessions

A) What is a session ID?

- **A session ID is a unique number that a Web site's server assigns to a specific web client for the duration of that session.**
- **It is essentially used to identify a session**

B) How do web applications use session ID to maintain state?

- **When the web client makes the first HTTP request, the web application at the server will create a new session ID and send it back to the web client with the HTTP response**
- **Through the session ID, the web server can maintain the states of indv web clients**
  Hence, the web application will be able to identify the user to provide a personalised & customised response



C) What are the ways where session IDs are sent btw web server and client?

- **Session ID can be transmitted via:**
  - **Embedded in the URL (HTTP Request- GET method)**
  - **Stored within the fields of a form, typically hidden and submitted w/ the HTTP Request - POST method**
  - **In a Cookie**

Q3) Web cookies

A) What is a web cookie?

- **A small piece of data sent from a website and stores on the user's computer by the web browser by the web browser while the user is browsing.**

B) What is the purpose of web cookies?

- **They are used by websites to rmb stateful info of the users**
- **Examples of info stores in a cookie:**
  - **Travel websites may store user's travel itinerary**
  - **Personal info provided when visiting a site**
  - **Items in shopping cart**

Q4) Describe the various types of web cookies

- **First-party cookie**
  - **Created by the website that the user is currently visiting**
- **Third-party cookie**
  - **Created by a website the user is NOT currently visiting**
  - **Created by script from other websites embedded in the page by the owner of the current website. E.g. Facebook plugins, Advertisers, etc.**
  - **Used to track user preferences, Social Media "likes", etc.**

- Session cookie
  - Used by websites to identify unique visitors and logged-in users
  - Stored in RAM and deleted when browser is closed
- Persistent cookie
  - Recorded on computer's hard drive
  - Not deleted when browser closes
  - May have expiry date
- Secure cookie
  - Encrypted; used only when browser visits server over secure connection

Q5) List 2 security risks of using web cookies
- May be stolen and used to impersonate user
- Used to tailor advertising (privacy risk)
- Can be exploited by attackers

Q6) Recommend some measures to ensure secure Session Management
- Length of Session Validity
  - Client cancellation, session time-out and server-side revocation
- Session verification
  - Ensure correct session ID length, no unexpected information
- Re-authenticate all significant system actions and re-issue new tokens

!! 6B TUT

Saturday, 3 August 2024 9:47 pm

Q1) Uniform Resource Locator (URL)

A) Explain what is a URL

- It is a unique identifier used to locate a resource on the internet.
- Referred to as a web address

B) What are the major components of a URL?

- A scheme
  - It identifies the protocol, i.e. HTTP / HTTPS
- A host name
  - It identifies the host.
  - e.g. www.example.com
- A path
  - It identifies the specific resource in the host that the web client wants to access.
  - e.g. software/index.html
- A query string
  - It provides a string of info that the resource can use for some purpose.
  - e.g. as parameters for a search/as data to be processed.
- Scheme://host:port/path?query

Q2) Explain what is directory traversal attack. Give an example how the attack works.

- Directory traversal attack enables a malicious user to guess the location of restricted files and views/executes them
- e.g. The correct url: http://www.test.com/getReport.aspx?id=Jan2009.htm
- The attack url: http://www.test.com/getReport.aspx?id=Mar2009.htm
- Hence, the attacker can predict the name of the report and obtain the info early, before the link is published

Q3) Suggest some measures to protect against directory traversal attack

- Effectively filter any user input
- Always compare against a white list (i.e. permitted values / parameters)
- Restrict the web application to serve pages only from a Web root directory and it subdirectories, and not any directories

Q4) Explain why a company's firewall cannot block port 80 or 443

- Firewalls must be configured to open port 80 and allow HTTP traffic so that the public users using web browsers can communicate w/ its web server
- Similarly, firewall must open port 443 for HTTPS traffic

Q6) Failure to properly validate inputs from the client is one of the major causes of web application attacks. Recommend some measures to enforce input validation.

- Validation Strategy
  - Accept only known valid data
  - Reject Known bad data
  - Sanitize bad data
- Check for correct data type, length, format, range
- Never rely on client side data validation, implement validation on server side components as far as possible

Q7) What is Open Web Application Security Project (OWASP) Foundation?

- OWASP is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web

!! 7A TUT

Saturday, 3 August 2024 11:24 pm

Q1) What is NOT an example of digital forensic evd collection?
- Adding outbound firewall rules to prevent internet access

Q2) What is the correct digital forensics process sequence?
- Collection > Examination > Analysis > Reporting

Q3) What correctly defines the process of acquiring evd?
- Dump the memory, power down the system, create an image of the system, and analyze the image

Q4) What are the information that are classified as volatile?
- Network information
- Active Processes
- Logged-on Users
- Open Files

Q5) What correctly defines free space?
- The remaining sectors of a previously allocated file that are available for the operating system to use

Q6) Explain why you should always search the free space and slack space if you suspect a person has deliberately deleted files or information on a workstation that you are analysing.
- When a user deleted a file, the file is not actlly deleted. Only the pointer in the file allocation table is deleted
- The act of "deleting" the file merely removes the pointer and marks the sector(s) holding the file as available for the operating system to use
- The actual data originally stored on remains on the disk in either the slack space/the free space which could still contain some of the deleted info.

Q7) What are the differences btw Steganography VS Watermarking?

- Steganography
  - The art of storing info in such a way that the existence of the info is hidden

    To human eyes, data usually contains known forms, like images, e-mail, sounds, and text. Most Internet data naturally includes gratuitous headers, too. These are media exploited using new controversial logical encodings: steganography and marking.

  - The duck flies at midnight. Tame uncle Sam

- Watermarking
  - Hiding data within data
    - Info can be hidden in almost any file format
    - File formats w/ more room for compression are best
      - Image files (JPEG, GIF)
      - Sound files (MP3, WAV)
      - Video files (MPG, AVI)
    - The hidden info may be encrypted, but not necessarily
    - Numerous software applications will do this for you: Many are freely available online

Q8) Name and describe the 4 phrases of the digital forensic process
- Collect phase aims to identify, label, record and acquire data from possible sources
- Examine phase aims to search and process the collected data to assess and extract data of interest
- Analyse phase aims to analyse results of examination to derive useful info of interest
- Reporting phase aims to report results of analysis incl. tools and procedures use and recommend how to secure identified vulnerabilities

Q9) Name 2 key challenges faced by the forensic team during the collection phase of the digital forensic process and recommend suitable actions.
- Volatile info
  - For collection of volatile info such as network info, active processes, it is impt to capture these from the system core dump before the system is disconnected and powered off
- Anti-forensic software
  - To ensure that the functioning of anti-forensic software are detected and stopped such that target data will not be corrupted/distorted

Q10) Name and describe 5 steps the forensic team can take when handling the data sources during the analysis phase.

- **Check the Recycle Bin for deleted files**
- **Check the Web browser history files and address bar histories**
- **Check the Web browser cookie files**
- **Check the Temporary Internet Files folder**
- **Search files for suspect character strings**
- **Search the slack and free space for suspect character strings as described previously**

!! 7B TUT

Saturday, 3 August 2024 11:24 pm

Q1) What describes an Incident Response?
- Involves a detailed, formal response plan
- Incident response is the response to a negative situation, usually a security breach/attack in the area of network security w/ a formal response plan

Q2) Incident Response plans should be developed …
- As a formal, detailed step-by-step response plan including procedures and tools

Q3) What is the first phase in incident response?
- Preparation
  - Preparing for an incident is the first phase. This phase involves providing the technology and processes so that the other phases will be successful. Without preparation, the other phases will be conducted in an ad-hoc manner and will not be as effective

Q4) What common utility/infrastructure is impt to consider when developing your recovery plans?
- Communications (whether telephone/wireless) is critical for organizations tdy.

Q5) You are a member of your company's computer incident response team and have been called in after office hours to investigate an attack in progress. The network engineers have identified the attack as coming from a workstation in an office area of your company. The attack is still in progress and needs to be terminated. You are in the office where the workstation is located, and the computer is on with the hard disk light flashing occasionally. What steps would you take to handle the attack and secure the computer for later forensic analysis?

- Since the attack is still in progress and you know the source of the attack is one of your own corporate computers, getting a memory image would be invaluable during your investigation.
- If you pulled the plug on this workstation, you would lose the info stores in memory
- You should dump the memory before unplugging this workstation. You would then be able to determine what processes were running, their configurations, and so on. This type of info would be invaluable for your investigation

Q6) Detection is an important aspect in an incident response plan. Why is this so? Based on what you have studied so far in this course and materials on the Internet, give 3 systems/sources of information that provides for detection of malware incidents.

- Detection is the main control which decides if an incident has taken place and activate the plan, if required.
- Without an effective detection system, the incident response plan would not be activated in a timely manner, if at all.
- Systems/sources of info include:
  - Intrusion detection systems
  - Logs from firewalls, network routers and other network devices
  - Logs form application servers (workstation logs are useful but they are usually too massive to be monitored effectively)
  - Reports from national certs or the US CERT
  - Unusual activities such as sudden surge in network traffic / use of disk space

Q7) Consider a malware incident. What are the typical tools that you would prepare for such a situation? List them down and briefly indicate why.
- Typical tools incl.
  - Laptops put on standby for malware incidents. They shld not be in use by someone during normal times. In cases of incidents, they can be deployed immediately.
  - WORM (write once, read many) media such as CD-ROMS or DVD-ROMS, containing all necessary software, incl. OS, application software, anti-virus, etc.
  - Communication equipment, such as walkie-talkies to facilitate communication in case the regular telecommunication systems break down

Q8) State and describe 3 main objectives of having an incident response team.
- To minimise overall impact upon incident
  - Impt to contain the dmg from the incident and control the situation in a very short time
- To recover services quickly
  - Impt to notify all affected stakeholders and record all details for forensic investigation
- To secure the affected systems
  - Impt to lock down all known avenues of attack, assess unseen vulnerabilities and implement effective security measures
- To meet requirements of laws or regulations
  - Impt to ensure all actions dictated by rules and regulations are fulfilled