CYBER SECURITY

AZURE SKYNET

6/10/2018

SD Sai Vamshi
Cyber security
Azure Skynet

Training By
Manish Bharadwaj

Table of Contents

Malwares

- Viruses
- Worms
- Trojans
- Rootkits
- Adwares
- Spywares

Wi-Fi Hacking

- Bypassing WEP
- Bypassing WPA/WPA2

Website Security

- HTTP vs HTTPS
- Automated SQL Injection

Denial of Service

- DoS vs DDoS
- Countermeasures

Cryptography

- Introduction
- Types of Encryption
- Hashing
- Steganography

Firewall

- IPS
- IDS
- Firewalls

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

❖ INTRODUCTION:

➢ Need of Cyber Security:

- It refers to the security offered through on-line services to protect our online information.
- CYBER is a combining form relating to information technology, the Internet, and virtual reality.
- Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

➢ Basic commands of Kali Linux:

- **Awk**: Find and Replace text, database sort/validate/index.
- **Cat:** Concatenate and print (display)the content of files.
- **Cd:** Change Directory.
- **Clear:** Clear terminal Screen.
- **Cut:** Divide a file into several parts.
- **Dir:** Briefly list directory contents.
- **Echo:** Display message on screen.
- **Exit:** Exit the shell.
- **Grep:** Search file(s) for lines that match a given pattern.
- **Help:** Display help for a built-in command.
- **Ifconfig:** Configure a network interface.
- **Kill:** Stop a process from running.
- **Killall:** Kill processes by name.
- **Ls:** List information about files.
- **Man:** Help manual.
- **Mkdir:** Create new folder(s).
- **Mv:** Move or rename files or directories.
- **Ping:** Used to test the ability of the source computer to reach a specified destination computer.
- **Pwd:** Print working Directory.
- **Set:** Manipulate shell variables and functions.
- **Ssh:** Secure Shell client (remote login program).
- **Touch:** Change file timestamps.

❖ Work Given(AWK,CUT):

- **$** awk '{print}' employee.txt
- **$** ifconfig | grep "broadcast" | awk '{print $2}'
- **$** cut -d ' ' -f2

The above commands are the answers for the given work to find errors. The error is we have to use single quotes instead of double quotes.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- **Networking:**
  - **IPv4 and IPv6:**
    - IP address (like pet name) (exchange of data).
    - 00000000. 00000000. 00000000. 00000000
    - 2^8 = 256 (0-255)
    - Max value IPv4 = 255 (256 128 64 32 16 8 4 2 1).
    - Five classes of IPv4 (Subnet Mask (N=255, H=0))
      - A (0-127) → Personal (N.H.H.H) 2^24 (255.0.0.0)
      - B (128-191) → Personal (N.N.H.H) 2^16 (255.255.0.0)
      - C (192-223) → Personal (N.N.N.H) 2^8 (255.255.255.0)
      - Network bits fixed value
      - Host bits means you can add systems/end devices here.
      - D (224-239) → Multicast / T.V
      - E (240-255) → Research
    - NO 127 as IP.
    - IP on the system is called private IP whereas IP on the Internet is called public IP.
    - Private
      - A 10.0.0.0 – 10.255.255.255
      - B 172.16.0.0 – 172.31.255.255
      - C 192.168.0.0 – 192.168.255.255
    - HUB == DUMB DEVICE
      - HUB sends msg to all.(Running same advertisements on all screens in a bus)
    - Router (Routing Table so sends correctly without broadcasting)
    - SWITCH ==== Increase the systems/Host/hops in a Network
    - ***THERE IS NO PLACE LIKE 127.0.0.1***
  - **OSI Layer:**
    - P – Physical (wires/0, 1)(Transmission and reception of raw bit streams over a physical medium)
    - D – Data-Link (senders.mac + receivers.mac)
    - N – Network (senders.ip + receivers.ip) router l3 devices
    - T – Transport. TCP/UDP (for Texting/ for Video calling)
    - S – Session. Timing (Interhost Communication)(OTP)
    - P – Presentation .pdf, .jpeg, .avi (Data representation and encryption)
    - A – Application gateway real-virtual. Web browser
  - **Networking Devices**
    - **Network Hub:**
      - Network Hub is a networking device which is used to connect multiple network hosts. A network hub is also used to do data transfer. The data is transferred in terms of packets on a computer network. So when a host sends a data packet to a network hub, the hub copies the data packet to all of its ports connected to. Like this, all the ports know about the data and the port for whom the packet is intended, claims the packet.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- **Network Switch:**
  - Like a hub, a switch also works at the layer of LAN (Local Area Network) but you can say that a switch is more intelligent than a hub. While hub just does the work of data forwarding, a switch does 'filter and forwarding' which is a more intelligent way of dealing with the data packets. So, when a packet is received at one of the interfaces of the switch, it filters the packet and sends only to the interface of the intended receiver. For this purpose, a switch also maintains a CAM (Content Addressable Memory) table and has its own system configuration and memory. CAM table is also called as forwarding table or forwarding information base (FIB).
- **Modem:**
  - A Modem is somewhat a more interesting network device in our daily life. So if you have noticed around, you get an internet connection through a wire (there are different types of wires) to your house. This wire is used to carry our internet data outside to the internet world. However, our computer generates binary data or digital data in forms of 1s and 0s and on the other hand, a wire carries an analog signal and that's where a modem comes in. A modem stands for (**Modulator + Demodulator**). That means it modulates and demodulates the signal between the digital data of a computer and the analog signal of a telephone line.
- **Network Router:**
  - A router is a network device which is responsible for routing traffic from one to another network. These two networks could be a private company network to a public network. You can think of a router as a traffic police who directs different network traffic to different directions.
- **Bridge:**
  - If a router connects two different types of networks, then a bridge connects two subnetworks as a part of the same network. You can think of two different labs or two different floors connected by a bridge.
- **Repeater:**
  - A repeater is an electronic device that amplifies the signal it receives. In other terms, you can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances. For example, inside a college campus, the hostels might be far away from the main college where the ISP line comes in. If the college authority wants to pull a wire in between the hostels and main campus, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distances they can carry the data for.

➢ **Network Address Translation:**
- NAT is a method of remapping one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

❖ **Enumeration, Scanning and Information Gathering:**

➢ **Information Gathering:**
- There are seven steps of Information gathering
  - Unearth Initial Information

- Locate the Network Range
- Ascertain Active Machines
- Discover Open Ports/Access Points
- Detect Operating Systems
- Uncover Services on Ports
- Map the Network

- We have used MALTEGO in order to get information of the person by just entering his/her mail.
- DNS enumeration is the process of locating all the DNS severs and their corresponding records for an organization. A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems. NSlookup and Whois can be used to gain information that can then be used to perform DNS enumeration.

➢ **Name Server Lookup and WHOIS:**
- NSlookup queries DNS servers for recoed information. Hacking tools such as Sam Spade also include NSlookup tools.
- Building on the information gathered from Whois, you can use NSlookup to find additional IP addresses for servers and other hosts. Using the authorative name server information from Whois, we can discover the IP address of mail server.
- Nslookup www.hightechdude.ml .
- A simple way to run whois is to connect to a website (for instance, ww.hightechdude.ml) and conduct the whois search.
- A (Address), SOS (Start of Authority), CNAME (Canonical Name), MX (Mail Exchange), SRV (Service), PTR (Pointer), NS (Name Server).

➢ **Traceroute:**
- Traceroute is a packet-tracking tool that is available for most operating systems. It operates by sending an Internet Control Message Protocol (ICMP) echo to echo hop (router or router gateway) along the path, until the destination address is reached. When ICMP messages are sent back from the router, the time to live (TTL) is decremented by one for each router along the path. This allows a hacker to determine how many hops a router is from the sender.
- One problem with using the traceroute tool is that it times out when it encounters a firewall or a packet-filtering router. Although a firewall stops the traceroute tool from discovering internal hosts on the network, it can alert an ethical hacker to the presence of a firewall; then, the techniques for bypassing the firewall can be used.

➢ **PORT Scanning Steps:**
- Determining if the System is alive
  - Network ping sweeps.
- **Port Scanning**
  - Nmap: It's a network mapping tool.
    - -f fragments options
    - -D Launches decoy scans for concealment
    - -I Ident Scan – finds owners of processes
    - -b FTP Bounce

- Port Scan types.
  - TCP Connect Scan
  - TCP Syn Scan
  - TCP Fin Scan
  - TCP Xmas Tree scan (FIN, URG, PUSH)
  - TCP Null Scan
  - TCP Ack Scan
  - UDP scan
- **Banner-Grabbing:**
  - Banner grabbers just collect those banners the easiest way to banner grab. (telnet <ipaddress>80).
- **Operating System Fingerprinting**
  - Active Stack Fingerprinting
    - Nmap
    - Xprobe2
  - **Passive Fingerprinting**
    - Siphon
    - P0f

- **Vulnerability Scanning:**
  - A vulnerability scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, OS, and software applications) they may have originated from a vendor, system administration activities, or general day-to-day activities:
    - Vendor-originated: This includes software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.
    - System administration-originated: this includes incorrect or unauthorized system configuration changes, lack of password protection policies, and so on.
    - User-originated: This includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious activities, such as deliberately introducing system backdoors.
  - **Network-based scanners:**
    - **Port Scanners**
      - Nmap
      - Superscan
    - **Network vulnerability scanners**
      - Nessus
      - GFI LANguard Network Security Scanner (N.S.S) (commercial)
    - **Web Server Scanners**
      - Nikto
      - Wikto
    - **Web application Vulnerability Scanners**
      - Paros
      - Acunetix Web Vulnerability Scanner (commercial)
  - **Host based Scanners**
    - Host vulnerability scanners

- MBSA (Microsoft Baseline Security Analyser)
- Altiris Security Expressions (commercial)

- **Database Scanners**
  - Scuba by Imperva Database Vulnerability Scanner
  - Shadow Database Scanner

➢ **COMMANDS USED:**
- Tracert www.hightechdude.ml (for Windows).
- Whois www.hightechdude.ml
- Ping www.hightechdude.ml
- host hightechdude.ml
- dig hightechdude.ml
- nslookup mighrtchdude.ml
- We can set the type like mx etc.
- Nslookup set type = mx host:www.hightechdude.ml
- Supsescan, id sever are used.
- Netdiscover -r 10.0.2.0/24 (for scanning)
- Nmap 10.0.2.3
- Nmap -o 10.0.2.15 (OS detection)
- Nmap -A 10.0.2.15 (OS and Service detection)
- Nmap -p 80-180 10.0.2.15-120 (ports)
- Nmap -sV 10.0.2.15 (Service Detection)
- We a=can use Zenmap in kali linux like we have to choose target such as 10.0.2.15, profile as Intense scan, Quick Scan, Command nmap -sn 10.0.2.15, -T4 -F 10.0.2.15.
- Nmap -sV testphp.vulnweb.com.
- Nginx 1.41. vulnerability.

❖ **Hping3**

➢ hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features.

➢ While hping was mainly used as a security tool in the past, it can be used in many ways by people that don't care about security to test networks and hosts. A subset of the stuff you can do using hping:
- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Manual path MTU discovery
- Advanced traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- hping can also be useful to students that are learning TCP/IP.

- **Google Hacking Database:**
  - **Advanced Information Gathering:**
    - Interesting Information:
      - Domains and subdomains
      - Ip addresses
      - Applications and technologies
      - Hotspots (known Vulnerabilities)
      - Usernames and passwords
      - Sensitive Information
    - **Passive**
      - As little contact as possible with target
      - No direct scanning, no intrusion
      - No logging and no alarm triggering
  - **Google Dorks/Operators**
    - A Google Dork query, sometimes just referred to as a dork, is a search string that uses advanced search operators to find information that is not readily available on a website.
    - In other words, in other words, we can use Google Dorks to find vulnerabilities, hidden information and access pages on certain websites. Because Google has a searching algorithm and indexes most websites, it can be useful to a hacker to find vulnerabilities on the target.
    - The basic syntax for advanced operators in Google is:
      - Operator_name:Keyword
    - For example, this operator_name:keyword syntax can be typed as 'filetype:xls intext:username' in the standard search box, which results in a list of Excel files which we contain the term 'Username'.
    - **Simple Google Dorks Syntax**
      - ***site*** – will return website on following domain
      - ***allintitle*** and ***intitle*** – contains title specified phrase on the page
      - ***inurl*** – restricts the results contained in the URLS of the specified phrase
      - ***filetype*** – search for specified filetype formats
    - The Data we can find using Google Dorks
      - Admin login pages
      - Username and passwords
      - Vulnerable documents
      - Sensitive Documents
      - Govt/Military Data
      - Email lists
      - Bank account details and lots more
    - Google Dorks can also be used for network mapping; we're able to find the subdomain of the target site using Simple Dorks.
  - **Spider/Crawler:**
    - A web crawler, sometimes called a spider, is an Internet bot that systematically browses the world wide web, typically for the purpose of web indexing(web spidering).

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- Web search engines and some other sites use Web crawling or spidering software to update their web content or indices of others sites' web content. Web crawlers copy pages for processing by a search engine which indexes the downloaded pages so users can search more efficiently.
- Crawlers consume resources on visited systems and often visit sites without approval. Issues of schedule, load, and "politeness" come into play when large collections of pages are accessed. Mechanisms exist for public sites not wishing to be crawled to make this known to the crawling agent. For instance, including a robots.txt file can request bots to index only parts of a website, or nothing at all.
- The number of Internet pages is extremely large; even the largest crawlers fall short of making a complete index. For this reason, search engines struggled to give relevant search results in the early years of the World Wide Web, before 2000. Today relevant results are given almost instantly.
- Crawlers can validate hyperlinks and HTML code. They can also be used for web scraping(see also data-driven programming).

➢ **Windows 10 product key:**
- **Windows 10** Home **-** TX9XD-98N7V-6WMQ6-BX7FG-H8Q99
- **Windows 10** Home Single Language - 7HNRX-D7KGG-3K4RQ-4WPJ4-YTDFH
- **Windows 10** Home Country Specific (CN) - PVMJN-6DFY6-9CCP6-7BKTT-D3WVR

➢ **Windows XP product keys:**
- DELL - KG7G9-67KHV-4FQKV-4DYXK-BHQTJ
- LENOVO – VF4HT-MPWB8-TWV6R-K6QM4-W6JCM
- ACER - KDD3G-HGVGM-M24P4-6BMMY-9XHF8

➢ **Windows 7 product keys:**
- Lenovo – 22TKD-F8XX6-YG69F-9M66D-PMJBM
- Dell – 342DG-6YJR8-X92GV-V7DCV-P4K27
- Acer – FJGCP-4DFJD-GJY49-VJBQ7-HYRR2

➢ **Quick heal product keys:**
- N3WKX-GU1ZL-MC7MJ-65VQD
- L99OV-5DD2Q-JOUH7-8LHVY
- DS89U-4UY6X-Z9MYQ-7XR9F

❖ **System Hacking:**

➢ Password cracking is one of the crucial stages of hacking a system. Password cracking used for legal purposes recovers the forgotten password of a user; if it is used by illegitimate users, it can cause them to gain unauthorized privilege to the network or system. Password attacks are classified based on the attackers actions to crack a password. Usually there are of four types:
- Passive Online Attacks
- Active Online Attacks
- Offline Attacks
- Non-electronic Attacks

➢ **Active Attack: (Direct Contact)**
- An active online attack is the easiest way to gain unauthorized administrator-level access to the system. There are four types of Active Online Attacks. They are:
  - Password guessing

- Trojan/spyware/key logger
- Hash injection
- Phishing

- **Passive Attack: (Indirect Contact)**
  - A passive attack is an attack on a system that does not result in a change to the system in any way. The attack is to purely monitor or record data. A passive attack on a cryptosystem is on in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based upon observed data. There are three types of passive online attacks. They are:
    - Wire sniffing
    - Man-in-the-middle
    - Replay
- **Default Passwords:**
  - A default password is a standard pre-configured password for a device. Such passwords are the default configuration for many devices and, if unchanged, present a serious security risk. Typical examples of default passwords include *admin*, *password* and *guest*. Furthermore, a vendor generally uses a single default password, which can be easily found online through search or on websites that provide compiled lists.
- We can use msfconsole in order to enter others computer like using same IP.(norse attack map, Digital attack map)

❖ **Wireshark:**
- Wireshark is a protocol analyzer that captures and decodes network traffic
- Wireshark is not aware of what process generates traffic.
- As with Process Monitor, the key is using filters to focus on what is relevant.

❖ **Malwares:**
- Any code that performs evil Today is called malware (RAT-remote access tools)
- Executable content with unknown functionality that is resident on a system of investigative interest
  - Viruses (cmd.exe)
  - Worms
  - Intrusion Tools
  - Spyware:
  - Rootkits (Motherboard, RkHunter)
- **Viruses:**
  - A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spread to other computers by attaching themselves to various programs and executing code when a user launches one of those infected programs. Viruses can also spread through script files, documents, and cross-site scripting vulnerabilities in web apps. Viruses can be used to steal information, harm host computers and networks, create botnets, steal money, render advertisements, and more.
- **Worms:**
  - These are among the most common types of malware. They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

networks by consuming bandwidth and overloading web servers. Computer worms can also contain "payloads" that damage host computers. Payloads are pieces of code written to
- perform actions on affected computers beyond simply spreading the worm. Payloads are commonly designed to steal data, delete files, or create botnets. Computer worms can be classified as a type of computer virus, but there are several characteristics that distinguish computer worms from regular viruses. A major difference is that computer worms have the ability to self-replicate and spread independently while viruses rely on human activity to spread (running a program, opening a file, etc). Worms often spread by sending mass emails with infected attachments to users' contacts.

- **Intrusion Tools:**
  - Intrusion detection systems are now essential for any network. Fortunately, **these systems are very easy to use and most of the best IDSs on the market are free to use**. In this review you will read about the ten best intrusion detection systems that you can install now to start protecting your network.
- **Spyware:**
  - Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections. Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans.
- **Rootkits:**
  - It is a type malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is possible for the malicious party behind the rootkit to remotely execute files, access/steal information, modify configurations, alter software, install concealed malware, or control the computer as part of a botnet.
- Dark comet, njrat, Jp virus maker/tera bit virus maker.

❖ **Wi-Fi Hacking: (Wi-Fi – Wireless Fidelity (1994)) (1997 WEP) (IV's = Initialization Vector)**
- Search wifi
- Wifi name
- Click on wifi
- Password required
- Password crosschecked
- Optained IP address

- 2004 WPA2 (WPA – WiFi protected access)
- You can patch the problem of software but you can patch human stupidity.
- **Bypassing WEP:** (Wireless equivalent privacy)
  - It did not include a key management protocol, relying instead on a single shared key among users.
  - The use of WEP was optional, resulting in many installations never even activating it.
- **Bypassing WPA/WPA2:**
  - Connect the external wireless interface into the notebook's USB port.
  - Check if the connected external wireless interface was recognized by operating system: (using iwconfig)

- Create a monitor interface putting the external wireless interface in monitor mode: (airmon-ng start wlan0)(Managed Mode).(Kill 401 447 554 1300).
- (Now monitor mode) Use airodump-ng for searching every near wireless network and choose one of them to try to crack it: (airodump-ng start wlan0).
- Now, notedown the target IP address (airodump-ng wlan0mon)
- Airodump-ng - - bssid 94:65:2D:8D:0A:DC -c 1 -w rogers wlan0mon.
- Locate rockyou.txt
- Aircrack-ng rogers.cap -w /usr/share/wordlists/rockyou.txt
- And the password is found.

❖ **Website Security:**

- Static – don't have database (blog)
- Dynamic – with database (fb,gmail)
- Front end – HTML/CSS
- BACK END - .NET/PHP
- DB – MYSQL
- GET- WWW.WEB.COM/LOGIN.PHP?ID=123
- POST – WWW.WEB.COM/LOGIN.PHP
- <SCRIPT>ALERT(1)</SCRIPT>
- <SCRIPT>ALERT("HACKED")</SCRIPT>
- Visit web browser
  - Type metasploitable2 IP address in url
  - Select DVWA
  - ID – admin, Password = password
  - Select dvwa security and change it to low
  - Click on stored XSS
  - Write name and our script in the comment section
  - Go back for to home page and re click on stored XSS
  - And then we will get a popup

HTTP vs HTTPS:

- **HTTP:**
  - HTTP – Hyper Text Transfer Protocol.
  - One of the application layer protocols that make up the internet.
    - HTTP over TCP/IP
    - Like SMTP, POP, IMAP, NNTP, FTP, etc.
  - The underlying language of the web
  - HTTP sits atop the TCP/IP Protocol Stack
    - Application Layer (HTTP), Transport Layer (TCP), Network Layer (IP), Data Link Layer (Network Interfaces).
  - It requires a TCP connection
  - Request Methods:
    - GET:
      - Retrieves a resource from the server.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- POST:
  - Allows passing of data in entity rather than URL.

- **HTTPS**
  - HTTP + SSL (Secure Socket Layer)
    - Application Layer (HTTP), SSL, Transport Layer (TCP), Network Layer (IP), Data Link Layer (Network Interfaces).
  - The SSL protocol inserts itself between an application like HTTP and the TCP transport layer. TCP sees SSL as just another application, and HTTP communicates with SSL much the same as it does with TCP.

- **Automated SQL Injection:**
  - SQL injection is an attack in which the SQL code is inserted or appended into application user input parameters that are later passed to a back-end SQL server for parsing and execution. Any procedure that constructs SQL statements could potentially be vulnerable, as the diverse nature of SQL and the methods available for constructing it provide a wealth of coding options. The primary form of SQL injection consists of direct insertion of code into parameters that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata. When the stored strings are subsequently concatenated into a dynamic SQL command, the malicious code is executed. When a Web application fails to properly sanitize the parameters which are passed to dynamically created SQL statements (even when using parameterization techniques) it is possible for an attacker to alter the construction of back-end SQL statements. When an attacker is able to modify an SQL statement, the statement will execute with the same rights as the application user; when using the SQL server to execute commands that interact with the operating system, the process will run with the same permissions as the component that executed the command (e.g. database server, application server, or Web server), which is often highly privileged.
- **XSS (Cross Site Scripting):**
  - We can use Burpsuite in Kali Linux for this
  - First go to the browser and select preferences, then advanced → Network → Settings → Select Manual proxy configuration and set port to 8080 and select ok.
  - We are testing testphp.vulnweb.com
  - In proxy, Intercept we can see forward, Drop, Intercept is ON, Action
  - Click on Action and send that to spider, there we can see spider running.
  - Now go to target select testphp.vulnweb.com and select spider the host.
  - On right select a POST method and send that to repeater
  - Change something in raw and select go and click show response in browser and now we can see the message we entered in the popup.
- **SQL Injection**
  - Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart - -tables
  - Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users - - columns
  - Sqlmap -u testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users – C uname,pass - - dump
  - Now we will get the username and password .
- **Top 10 OWASP: (Open Web Application Security Project) (According to 2017)**
  - Injection

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting
- Insecure Deserialization
- Using Components with known Vulnerabilities
- Insufficient Logging & Monitoring

❖ **Denial of Service:**

➢ **DoS vs DDoS**

- **DoS (one attacking machine)**
  - Aim to consume limited servers OS-level resources typically by misusing lower-layer protocols (TCP,IP,…)
  - Buffers holding arriving IP packets.
  - Tables of open TCP connections
  - TCP – SYN Flood
    - ♦ Attacker sends a flood of TCP-SYN requests in possibly spoofed IP packets => 3 – way handshake never completed.
    - ♦ Half-open connections bind server resources – no new connections can be made
  - Involve valid looking application requests that
    - ♦ Consume significant application resources, or
    - ♦ Cause application to crash
  - HTTP attack requesting large PDF files from a server
  - Attack on a web server that makes database queries using computationally – costly requests.

- **DDoS (distributed DoS attack)**
  - Employ numerous attacking machines – so called botnets
    - ♦ Direct DDoS attacks
    - ♦ Reflector DDoS attacks
    - ♦ Amplification DDoS attacks
  - Botnet for DDoS
    - ♦ Botnet – a network of compromised machines (bots, zombies, or agents) controlled by the attacker.
    - ♦ Attacker/master – machine that is physically used by the bot master/herder
      - ➢ Can be anywhere with any type of internet connection
    - ♦ Stepping Stone – Attacker can use 1 or more stepping stones to hide his or her true identity and location
      - ➢ Typically, there is a telnet connection between botnet master and its stepping stones
      - ➢ Due to legal issues and physical location, using stepping stones located in foreign countries make it much more difficult to trace the original attacker.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- **Counter Measures:**
  - The available DoS and DDoS defenses cover various aspects, such as prevention, mitigation strategies and security architectures. During a Dos and DDoS attack, the most important thing is to maintain the availability for the service providers, the end users and the Cloud infrastructure managers.
  - Defending against Dos and DDoS attacks is difficult. A DoS or DDoS could theoretically be stopped by identifying and then blocking the unique source of the attack. Most of the time, the attack leverages a huge amount of bots through a DDoS attack.
  - Prevention - Service Level Agreements (SLA). SLA helps to prevent DoS and DDoS attacks.
  - Attack Mitigation – VMM (Virtual Machine Monitor), IDS, Behavior and Knowledge Analysis etc.

- **Cryptography:**
  - **Introduction:**
    - Cryptography is the art and science of making a cryptosystem that is capable of providing information security.
    - It deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.
    - Changing plain text to cipher is called as encryption.
    - Changing cipher text to plain text is called decryption.
    - The primary objective of using cryptography is to provide the following foure fundamental information security services. Let us now see the possible goals intended to be fulfilled by cryptography.
      - Confidentiality
      - Data Integrity
      - Authentication
      - Non-reputation
  - **Types of Encryption**
    - Fundamentally, there are two types of cryptosystems based on the matter in which encryption-decryption is carried out in the system.
      - Symmetric Key Encryption
      - Asymmetric Key Encryption
    - The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.
    - **Symmetric Key Encryption:**
      - The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.
      - The study of symmetric cryptosystems is referred to as symmetric cryptography.
      - Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.

- A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.
- Challenges of Symmetric key Cryptosystem are key establishment and Trust Issue.

- **Asymmetric Key Encryption:**
  - The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption.
  - Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible.
  - Asymmetric Key Encryption was invented in the 20 Th century to come over the necessity of pre - shared secret key between communicating persons. The salient features of this encryption scheme are as follows:
    - Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other decrypt the ciphertext back to the original plaintext.
    - It requires to put the public key in public repository and the private key as a well -guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.
    - Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
    - When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits.
    - Host2 uses his private key to extract the plain text. Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
    - Processing power of computer system required to run asymmetric algorithm is higher.
  - A – pub/priA
    - ((priA(Vamshi))pubB)
  - B - priB/pubA
  - C – pubA

- **Hashing:**
  - A cryptographic hash function is a special class of hash function that has certain properties which make it suitable for use in cryptography. It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is designed to be a one-way function, that is, a function which is infeasible to invert. The only way to recreate the input data from an ideal cryptographic hash functions output is to see if they produce a match, or use a rainbow table of matched hashes.
  - In theoretical cryptography, the security level of a cryptographic hash function has been defined using the following properties
    - Pre-image resistance
    - Second pre-image resistance
    - Collision resistance
  - Example
    - I AM BEST k = 2
    - K CO DGUV

- **Steganography:**
  - It is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.
  - The word steganography is of Greek origin and means concealed writing from the Greek words Steganos – covered or protected, and graphein meaning writing.
  - Steganography means hiding one piece of data within another.

- ***Since Everyone Can Read, Encoding Text In Neutral Sentences Is Doubtfully Effective.***
  - SECRET INSIDE
  - Unknown message passing
  - Prevents discovery of the very existence of communication
  - Little known technology
  - Once detected message is known

❖ **Firewall:**

➢ It is a piece of software. This software monitors the network traffic. A firewall has a set of rules which are applied to each packet. The rules decide if a packet can pass, or whether it is discarded. Usually a firewall is placed between a network that is trusted, and one that is less trusted. When a large network needs to be protected, the firewall software often runs on a computer that does nothing else. It protects one part of the network against unauthorized access.

➢ **IDS: (Intrusion Detection System)**

- An IDS is designed to analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event. The IDS contains a database of known attack signatures and it compares the inbound traffic against to the database. If an attack is detected then the IDS reports the attack. The main function of an IDS product is to warn you of suspicious activity taking place but not prevent them. The major flaw is that they produce a lot of false positives.

➢ **IPS: (Intrusion Prevention System)**

- The IPS sits between your firewall and the rest of your network. Because, it can stop the suspected traffic from getting to the rest of the network. The IPS monitors the inbound packets and what they are really being used for before deciding to let the packets into the network. An IPS will inspect content of the request and be able to drop, alert, or potentially clean a malicious network request based on that content. The determination of what is malicious is based either on behaviour analysis or through the use of signatures.

➢ **Firewalls:**

- A traditional firewall is the rules-based engine that analyzes packet headeron protocol type, source address, destination address, source port, and/or destination port. If the Packets are not match with firewall rules, packets will be dropped. There is something called a Next

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

Generation Firewall (NGFW). This can make a single device act as both a traditional Firewall and IPS.

- A firewall is a rule based engine, But IDS also use own huge data-base to detect intrusion. An IDS evaluates a suspected intrusion once it has taken place and warns to administrator. An IDS also watches for attacks that originate from within a system. An IDS is not a replacement for a firewall or a good antivirus program. An IDS should be considered a tool to use in conjunction with your standard security products (like anti-virus and a firewall) to increase your system specific or network-wide security. So I hope we can't replace an IDS device by a firewall.
- **Types of Firewall:**
  - **Bastion Host**
    - Krutz and Vines have described a **bastion host** as any computer that is fully exposed to attack by being on the public side of the DMZ, unprotected by a **firewall** or filtering router. **Firewalls** and routers, anything that provides perimeter access control security can be considered **bastion hosts**.
    - It is a special purpose computer on a network specifically designed and configured to withstand attacks.
  - **Screened subnet (triple-homed firewall)**
    - In network security, a **screened subnet firewall** is a variation of the dual-homed gateway and **screened** host **firewall**. It can be used to separate components of the **firewall** onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.
  - **Multi-Homed firewall**
    - Multihomed describes a computer host that has multiple IP addresses to connected networks. A multihomed host is physically connected to multiple data links that can be on the same or different networks. For example, a computer with a Windows NT 4.0 Server and multiple IP addresses can be referred to as "multihomed" and may serve as an IP router.
    - Using the Stream Control Transmission Protocol (SCTP), multihoming allows a single SCTP endpoint to support multiple IP addresses, which means that a session is more likely to survive a network failure. In a single-homed session, a network failure can isolate the end system or make transport temporarily unavailable. Multihoming means that redundant local area networks (LANs) can be used to support local access. Various approaches, such as using addresses with different prefixes to force routing through different carriers, or even using redundant core networks, can be taken to reduce the effects of failures.
  - **Packet filtering**
    - It filters the packets.
    - As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters. An allow or deny decision is made based on the results of the comparison. Each packet is examined individually without regard to other packets that are part of the same connection.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

- You use packet filters to instruct a firewall to drop traffic that meets certain criteria.
- For example, you could create a filter that would drop all ping requests. You can also configure filters with more complex exceptions to a rule.

- **Application gateway/Proxies**
  - The proxy plays middleman in all connection attempts.
  - The application gateway/proxy acts as an intermediary between the two endpoints. This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination. Each endpoint can only communicate with the other by going through the gateway/proxy.
  - This type of firewall operates at the application level of the OSI model. For source and destination endpoints to be able to communicate with each other, a proxy service must be implemented for each application protocol.
  - The gateways/proxies are carefully designed to be reliable and secure because they are the only connection point between the two networks.
- **Stateful Inspection**
  - As packets pass through the firewall, packet header information is examined and fed into a dynamic state table where it is stored. The packets are compared to pre-configured rules or filters and allow or deny decisions are made based on the results of the comparison.
  - The data in the state table is then used to evaluate subsequent packets to verify that they are part of the same connection.

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140

The END

By SD SAI VAMSHI
INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRICITY
CSE

Linkedin account id: https://www.linkedin.com/in/sai-vamshi-6a4955140