Assignment2

Sky Zhou yz5946

Short Answers

1. **1) Description:** A detailed description of the detected vulnerability should be included in the report. **2) Assessment**: A professional assessment of severity level of the vulnerability should be included in the report. **3) Mitigation Suggestion:** The team should provide recommendations to mitigate the vulnerability. **4) Cost:** An approximate cost of mitigation and the cost of assets that may be affected should be included to quantify the dangerousness of the vulnerability. **5) Exploit Details:** Technical details of how the vulnerability could be exploited should be included.
2. First, a human driven penetration test can effectively identify false positives according to the empirical experience of the testing team. An automated test may not detect false positives effectively in the absence of human operators. Second, penetration tests can be customized according to the actual configuration of tested enterprises, while automated tests may not. Third, penetration tests are not limited to technical security analysis. Business logic errors can also be found out. These differences are caused by the ability of adaption and flexibility of human enforcement. Experienced penetration testers can scrutinize aspects that are overlooked in automated tests.
3. In **executive summary**, high level recommendations for remediation for the system are usually included since the **executive summary** serves as a preface of the report, and it should give the reader an overall generalization of the contents. Detailed recommendations for each vulnerability detected should be included in **the Findings** section. This section enumerates all vulnerabilities detected within the system. It would be best to append fixes and recommendations after the detected vulnerabilities. Lastly, recommendations can also be included in appendices. The penetration testing team can included technical details of remediation in appendices to provide technical instructions.
4. Masscan is faster than nmap in large network range scanning due to a simpler feature sets compared to nmap. And masscan identifies open ports with high efficiency. Also, masscan can be configured to control its rate of packet transmission, making it adaptable to different bandwidth capacities and avoiding network congestion. With its high efficiency and speed, masscan is more suitable for scanning a large set of networks or range. However, for more detailed reconnaissance where information beyond just open ports is required, Nmap's comprehensive feature set and accuracy make it the better choice.
5. When Nmap is unable to ascertain whether a port is open or closed because the responses from the network do not provide enough information, it will mark the port as “unfiltered”. This status often indicates that the packets sent by Nmap to the target port are not being blocked by a firewall or filtered along the way—there's no conclusive evidence that they reached a service listening on that port. The absence

of clear, definitive responses from the target network causes Nmap to categorize the port as unfiltered. This information is valuable for understanding the network's security configuration, particularly in identifying how its firewalls or intrusion detection systems are configured. Knowing that a port is unfiltered allows security professionals to perform more targeted testing against those ports. Since these ports are neither definitively open nor closed, they may warrant a closer inspection using different scanning techniques or tools to determine their actual status.

6. The first thing is to filter and validate the list since automated tests may contain false positive results. We can use tools like massdns to resolve each subdomain to confirm if it points to an active IP address. With a refined list of active subdomains, the next step is categorizing them based on their content, functionality, and potential sensitivity. We can write scripts to categorize the subdomains. Then, for categories we can perform vulnerability scanning with tools like Nessus to finish our penetration test.
7. **1) Use Encrypted Storage and Transmissions:** Ensure that all data collected, including real-time test results, are stored on encrypted devices. If test results need to be transmitted during the test, use encrypted communication channels such as VPNs or SSH tunnels. Store the final report and any raw test data on encrypted drives or secure, encrypted cloud storage solutions. **2) Implement Access Control:** Limit access to the test data to only those individuals directly involved in the penetration testing process. **3) Regular Backups and Secure Deletion:** Regularly back up test data to prevent loss due to hardware failure, software issues, or other unforeseen circumstances. Ensure that backups are also encrypted and stored securely. Use tools designed for secure deletion that overwrite data multiple times, ensuring it cannot be recovered.
8. **ARP Request**: When scanning hosts on a local subnet, Nmap sends an ARP request to determine if a host is alive. I**CMP Echo Request:** Nmap sends an ICMP Echo Request (Ping) to the target IP addresses. If an ICMP Echo Reply is received, the host is considered up. **TCP SYN Packet to Port 443:** Nmap sends a TCP SYN packet to port 443 of the target. Port 443 (HTTPS) is chosen because it is commonly open for secure web traffic. If a SYN-ACK response is received, the host is considered up. **TCP ACK Packet to Port 80:** Nmap sends a TCP ACK packet to port 80 (HTTP) of the target. This is not meant to establish a connection but can trigger a response from alive hosts. **ICMP Timestamp Request:** Nmap may also send an ICMP Timestamp Request as part of its host discovery process. If a Timestamp Reply is received, the host is considered up.
9. **A)** No, this open redirect is not in scope. It is clearly mentioned that any subdomain of Dell Premier is out of scope. **Out of scope Dell Premier:** **www.dell.com/premier/***

   B) I found 204 subdomains for indeed.com using **Sublist3r**. I downloaded the driver Sublist3r.py and then run it on indeed.com. Please see the attached file subdomains.txt for the full list of 204 subdomains.

   C) To filter out unique IP addresses, I first use dig to find out the corresponding IP addresses given subdomains. The command is ***while read subdomain; do dig***

+short "$subdomain" | grep '^[.0-9]*$' >> ips.txt; done < subdomains.txt
Then, I used ***sort*** function in bash to filter out unique IP addresses. The command is ***sort -u ips.txt > unique_ips.txt***
Then, I write a shell script (see ***check.txt***) to ping all IP addresses in ***unique_ips.txt*** to check whether they are online or not. After running the script, I got 122 online IP addresses. Please see the attached file ***online_ips.txt.***
D) I use EyeWitness to capture the screenshots of the listed subdomain and found several subdomains saying that **Authorization Header Missing.** The address is **https://cortex-gateway-europe.indeed.com/** and the IP address is **172.64.145.11.** This might be a web page that requires token to login. Also, it is interesting that I found some subdomain with "admin" keyword in it. http://admin.chatbot.indeed.com This might be the admin website to manage chatbot of indeed.com. However this page cannot be accessed. It may be because the website blocks visits from outside IP addresses that are not part of indeed.com. However, an attacker can spoof an internal IP address and may have access to the admin site. Both subdomains may be useful for further research and might contains vulnerabilities.