جامعة الحسين التقنية
Al Hussein Technical University

ASSIGNEMNT BRIEF

HTU Course No: 10203360	HTU Course Name: Penetration Testing
BTEC Unit No: N/A	BTEC UNIT Name: N/A

Version: 3

جامعة الحسين التقنية
Al Hussein Technical University

Assignment Brief

Student Name/ID Number/Section	
HTU Course Number and Title	10203360 Penetration Testing
BTEC Unit Number and Title	
Academic Year	2023-2024 Spring
Assignment Author	Sami AlMashaqbeh
Course Tutor	Sami AlMashaqbeh
Assignment Title	AnimeBlast Attack
Assignment Ref No	1
Issue Date	10/04/2024
Formative Assessment dates	From 25/04/2024 to 30/05/2024
Submission Date	13/06/2024
IV Name & Date	Safaa Hriez 09/04/2024

Submission Format

The submission for this assignment is:

1. An individual written **detailed report** (word format) that provides thorough, evaluated, or critically reviewed technical information on all the points illustrated in the *Assignment Brief and Guidance* section. **All snapshots must be very clear, with a computer timestamp and date. This will serve as evidence of your work. Additionally, you should include a watermark by using any watermarking tool to place your first and last name on the snapshots. *Including signed student assessment submission and declaration form in a separated file.***

2. **An in-class written exam will be held on 18-05-2024.**

3. **An oral discussion about the report, followed by a practical presentation to demonstrate students' skills. If there is a failure in any criteria during the oral discussion or the practical presentation, the criteria will not be considered fulfilled, even if they were done correctly in the submitted report.**

PS: Files should be uploaded separately rather than in a zipped file. (two files)

Report guidelines:

In your report, you should make use of headings, paragraphs, and subsections as appropriate. The expected word limit is about 5000 words (recommended 15-20 pages not including snapshots), although you will not be ***penalised*** for exceeding the total word limit. Do your best to be within the word limit. Your report should be:

1. In a form of a **soft copy** submitted via the URL below.
2. Written in a formal business style using **single spacing and font size 12 Times New Roman (Headings CS)**.
3. Must be supported with research and referenced using the Harvard or APA referencing system.

Note: Soft copies submissions should be done through the university's eLearning system within the deadline specified above from below link: https://elearning.htu.edu.jo/

Unit Learning Outcomes

LO1 Gain foundational skills in penetration testing.

LO2 Gain comprehensive knowledge of CPU instructions, memory addressing mechanisms, and vulnerability exploitation techniques, while mastering Python and Bash scripting for automating tasks and executing complex penetration testing scripts effectively.

LO3 Gain proficiency in advanced exploit development techniques by mastering essential debugging skills, understanding memory corruption vulnerabilities, and exploring strategies for bypassing exploit mitigations.

LO4 Gain proficiency in privilege escalation techniques, pivoting, tunnelling, and port forwarding.

Assignment Brief and Guidance

AnimeBlast Productions is a leading name in the animation industry, dedicated to producing captivating and immersive anime content. Established recently, our company has swiftly emerged as a frontrunner in the world of anime production, captivating audiences worldwide with our diverse range of anime series and films. At AnimeBlast Productions, we prioritize not only the creativity and storytelling of our anime but also the technological advancements and innovation driving our operations. We've harnessed state-of-the-art IT infrastructure to ensure seamless production processes, robust data management, and adherence to industry standards, guaranteeing that every frame of our anime meets the highest quality benchmarks. ***Below is a list of the main IT servers required for AnimeBlast Productions:***

Application Servers: These servers are the backbone of AnimeBlast Productions, hosting a suite of software applications critical to our anime production operations. They manage tasks such as scriptwriting, storyboard creation, animation software, and post-production editing tools. Additionally, they oversee monitoring systems for animation rendering, ensuring efficiency and adherence to quality standards.

Database Servers: Housing a vast repository of anime assets, including character designs, background art, sound effects, and episode scripts, these servers are essential for efficient project management and content organization.

Web Servers: Responsible for hosting AnimeBlast Productions' official website and online platform, these servers provide users with a seamless and responsive experience when browsing our anime catalog, viewing trailers, and accessing exclusive content.

Email Servers: Facilitating internal and external communications within AnimeBlast Productions, email servers ensure secure and efficient correspondence among team members, collaborators, and stakeholders.

File Servers: Enabling seamless collaboration among animators, artists, and production staff, file servers allow for the easy sharing and storage of animation assets, project files, and production resources.

Backup and Recovery Servers: Safeguarding against data loss and system failures, these servers continuously back up critical animation projects and assets, ensuring swift recovery in the event of unforeseen incidents.

Authentication and Authorization Servers: Managing user access to sensitive animation files and production tools, these servers ensure that only authorized personnel can access and modify crucial resources, enhancing security and data integrity.

Domain Controllers: Playing a pivotal role in network security, domain controllers manage user access permissions and enforce security policies across AnimeBlast Productions' IT environment, bolstering overall cybersecurity posture.

Firewalls and Security Servers: Protecting AnimeBlast Productions' network infrastructure from cyber threats and unauthorized access attempts, these servers maintain the confidentiality, integrity, and availability of our animation projects and proprietary information.

Monitoring and Management Servers: Essential for overseeing the health and performance of AnimeBlast Productions' IT infrastructure, monitoring and management servers enable real-time monitoring, proactive issue resolution, and resource optimization.

Compliance and Audit Servers: Ensuring compliance with industry regulations and internal policies, compliance and audit servers store and manage critical logs of IT activities, facilitating both internal audits and regulatory assessments.

AnimeBlast Productions prioritizes customer engagement and accessibility through various channels:

Online Platform (Website): Customers can explore AnimeBlast Productions' anime catalog, watch trailers, and access exclusive content through the user-friendly website. They can also interact with the community, participate in forums, and provide feedback on their favorite anime series.

Mobile Applications: Dedicated mobile apps for Android and iOS devices offer on-the-go access to AnimeBlast Productions' anime library, allowing customers to stream episodes, receive notifications for new releases, and engage with interactive features.

In-Store Kiosks: For customers who prefer a hands-on experience, in-store kiosks provide an intuitive interface for browsing anime titles, making selections, and purchasing merchandise at physical locations or events.

API Integration: Business clients and partners can integrate AnimeBlast Productions' anime streaming services into their own platforms or applications using APIs. This seamless integration facilitates content distribution, licensing agreements, and revenue sharing partnerships.

Payment Options: AnimeBlast Productions offers flexible payment options, including point-of-sale terminals for in-store purchases, online payment gateways for digital transactions, and contactless payment methods for convenience and security.

As an Penetration tester at AnimeBlast Productions, your mission is to conduct thorough security assessments on the company's existing systems, ensuring the protection of valuable intellectual property and sensitive data. Your primary objective is to uncover vulnerabilities and potential threats, providing actionable insights to bolster security measures and enhance overall reliability.

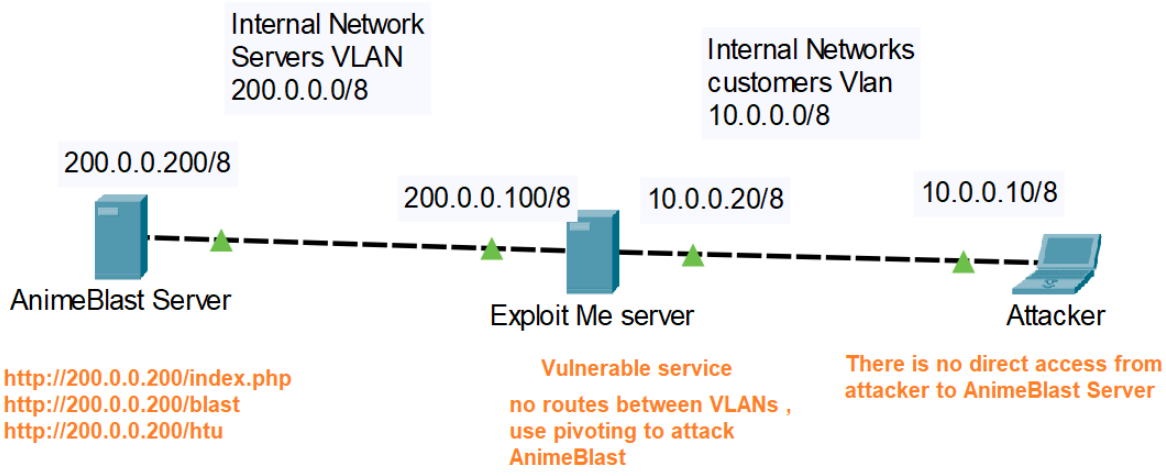
To facilitate your work and maintain the integrity of our infrastructure, you will receive an identical copy of our servers, operating within Oracle VirtualBox. These servers images will be provided in "ova" format, accessible for download from the following link: **"AnimeBlast_2024_pentest.ova". and Exploit ME server.ova** These virtual servers will faithfully replicate our original setup, offering an authentic environment for your assessments. you will need these files also. "Needed files"

Your responsibilities will involve actively simulating cyberattacks on these virtual servers to pinpoint potential weaknesses in our infrastructure. By conducting these simulated attacks, you will assist in evaluating the security posture of our systems, ensuring their resilience against real-world threats. Your insights and recommendations will be instrumental in fortifying our security measures, safeguarding our valuable assets, and preserving our reputation in the industry.

Your dedication to uncovering vulnerabilities and strengthening our security measures will play a crucial role in maintaining the trust of our stakeholders and ensuring the long-term success of AnimeBlast Productions.

جامعة الحسين التقنية
Al Hussein Technical University

Your setup environment must be as below:



Instead of the above topology, you can create another network adapter and connect the two networks using NATed network with two different subnet ranges, and use DHCP to assign IPs.

The tasks that need to be completed are listed below this line. Please carefully review the specified goals for achieving them.

- ***The only way to reach Servers Vlan network from Kali Linux, is through the Exploit Me server.***
- ***Each goal should be met using the designated method, and no alternative methods should be employed. Ensure that the testing requirements for each task serve as the basis for accomplishing each goal.***
- ***You must provide snapshots to support your work documentation for each point. Choose the best two snapshots that conclude your work.***

Part1: ***An in-class written exam will be held on 18-05-2024.***

Assessment criteria and instructions will be determined and explained further later.

Will cover (P1,P2,P3,P4,P5,M1,M2,M4,D1, and D3)

Part2: Penetration Testing foundations:

The CEO of AnimeBlast Productions has requested a detailed explanation of the following points before you commence your role as an ethical hacker. This request is to ensure your ability to perform the task effectively and assess your professionalism for the assignment. Please provide a clear and comprehensive discussion of each point.

A. What are the common jumping strategies necessary for crafting a successful memory exploit? Could you elaborate on the significance of back jumps, forward jumps, long jumps, short jumps, and other types of jumps in this context? Please explain in detail.

B. What are the common memory corruption techniques, and please explain in detail the mitigation strategies such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), the Visual Studio /GS Flag, and Visual Studio Safe SEH? Additionally, kindly discuss bypassing techniques for these protections.

C. During a penetration testing engagement, you encounter a system with restricted user privileges. Explain the concept of privilege escalation in detail and discuss its significance within the context of penetration testing.

Part3: Target #1 Exploit-Me server

A. Create a bash script to automate this task: Print 'Scan started' on the screen, then use nmap to scan Target #1. Save only the open port numbers in a new text file named 'open_ports'. Finally, print 'Scan finished' on the screen.
B. Creating custom network scanning scripts and efficiently executing them to scan the target in order to identify vulnerable services on it using python.
C. Use fuzzers such as Spike Fuzzer or any equivalent tool, along with debuggers like Immunity Debugger, to analyze software running in memory and successfully fuzz it to determine ways to crash the software.
D. Use the NASM tool to create a short jump for 10 bytes and a back long jump for 4000 bytes.
E. Create the full Python script to exploit this service using one of the memory corruption techniques, such as JMP ESP, SEH, or Egg hunt. Explain each step inside the script using comments, detailing why each line of code is included. You can use the provided python template as starting point.
F. Provide proof that your script exploits the target system using a message box for the first exploit, and then using shellcode to create a payload for either a bind shell or a reverse shell for the second exploit. Utilize MSFvenom to generate the necessary payload as Python bytecode.
G. Load the backdoor you created through the msfconsole multi-handler, then exploit the target machine

Part4: Target #2 AnimeBlast server

A. Scan the target #2 to find open ports after creating a route to the target using the session created in the last part as the gateway for this route, which is required for pivoting.

B. Create as many tunnels (pivoting points) as needed to reach and attack the AnimeBlast server. These pivoting points could include FTP, HTTP, etc.

C. Identify the vulnerable services on the server using Metasploit auxiliary modules.

D. Identify a SQL Injection vulnerability, exploit it, and extract the entire database.

E. Show proof of a Cross-Site Scripting (XSS) vulnerability and explain how an attacker (Pentester) could benefit from it, such as gaining the cookies of a user.

F. Find a Remote Code Execution (RCE) vulnerability and utilize it to add a user to the system.

G. Find any network service such as FTP and attempt to discover its user and password through brute force. You can utilize the predefined list of usernames and passwords provided.

H. Find a file upload vulnerability and exploit it to upload a PHP shell. Provide evidence of the actions achievable through the PHP shell (such as meterpreter or a c99 shell). You can utilize the provided file.

I. **CTF (Capture the Flag):** Find the 10 flags inside the server and decode them from Base64 to human-readable format. There is one encrypted flag that needs to be decrypted using the RC4 algorithm with a password. Use https://gchq.github.io/CyberChef/ to decrypt and decode.

Learning Outcomes and Assessment Criteria		
Pass	**Merit**	**Distinction**
LO1 Gain a solid foundation in penetration testing.		
P1 Explain the importance of penetration testing in cybersecurity for assessing organizational security and fortifying defences. **P2** Discuss the types of penetration assessment and penetration testing strategies.	**M1** Discuss common areas of penetration testing and the ethical considerations of a penetration tester. **M2** Explain how to initiate, engage, and proceed with the penetration testing.	**D1** Analyze in detail the risks associated with penetration testing.
LO2 Gain comprehensive knowledge of CPU instructions, memory addressing mechanisms, and vulnerability exploitation techniques, while mastering Python and Bash scripting for automating tasks and executing complex penetration testing scripts effectively.		
P3 Demonstrate understanding of CPU instructions by identifying and explaining the operation of common instruction sets and their impact on system performance. **P4** Discuss the stack buffer overflow and how it can crash or control the running software inside the memory.	**M3** Develop Python and Bash scripts to automate routine tasks, such as data manipulation and system administration, demonstrating proficiency in scripting languages. **M4** Comparing in detail between CPU pointers and their importance in controlling the running program inside the memory.	**D2** Creating custom penetration testing scripts, such as network scanning scripts, vulnerability scanning scripts, and efficiently executing them.
LO3 Gain proficiency in advanced exploit development techniques by mastering essential debugging skills, understanding memory corruption vulnerabilities, and exploring strategies for bypassing exploit mitigations.		
P5 Discuss in detail the differences between static and dynamic code analysis, and their importance in penetration testing. **P6** Ability to use fuzzers and debuggers like Immunity Debugger to analyze software running in memory and successfully fuzz it to determine ways to crash the software.	**M5** Demonstrated skills in creating successful exploits using one of memory corruption techniques such as JMP ESP, SEH, EGG HUNT, ROP, PE, etc. **M6** Compare memory corruption techniques alongside defensive mechanisms such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), the	**D3** Explain in detail the jumping strategies required to create a successful exploit. Why do we need back jumps, forward jumps, long jumps, short jumps, etc.? Additionally, create successful assembly jump instructions for use in Python scripts, such as utilizing the NASM tool.

	Visual Studio /GS Flag, and Visual Studio Safe SEH. Additionally, explore the bypassing techniques for these protections.	
LO4 Gain proficiency in privilege escalation techniques, pivoting, tunnelling, and port forwarding.		
P7 Discuss in detail privilege escalation and its importance in penetration testing. **P8** Using a compromised system as a launching point or pivot to attack other systems within a network, by creating multiple tunnels.	**M7** Identify the ports and vulnerable services associated with the hidden systems by leveraging the created pivots or tunnels. **M8** Exploit common vulnerabilities, such as SQL injection, remote code execution, XSS, and file upload, through pivots or tunnels.	**D4** Locate the concealed flags within the compromised system (CTF).