LEVIATHAN WARGAME

Level 0:

Objective: The goal is to gather basic system information and look for potential vulnerabilities or misconfigurations.

Tools Used: SSH , whoami, ls, cat, netstat

Steps:

1. Log in to the server.
2. Navigate to the /home/leviathan0 directory.
3. List files to see what's available.
4. Read the README file to understand the challenge.
5. Explore the directory and identify potential clues or tasks.

Level 0 - 1:

Objective: This level focuses on file and service misconfigurations that may allow unauthorized access, with an emphasis on privilege escalation.

Tools Used: SSH, ls, cat, netstat

Steps:

1. Log in to the server as leviathan1.
2. Navigate to the /home/leviathan1 directory.
3. List the files in the directory.
4. Read the README file for clues and instructions.
5. Look for hidden files or any unusual files that might give hints.
6. Examine files carefully to find clues that will help you progress.

Level 1 - 2:

Objective: Leviathan Level 2 focuses on exploiting vulnerabilities in system configurations or files to capture the flag.

Tools Used: SSH, ls, cat, netstat, find

Steps:

1. Log in to the server as leviathan2.
2. Navigate to the /home/leviathan2 directory.
3. List the files to see what's available.
4. Read the README file for any instructions or hints on solving the level.
5. Search for hidden files or directories that could contain useful information.
6. Explore and identify any challenges or puzzles to solve in order to move to the next level.

Level 2 - 3:

Objective: Level 3 challenges you to explore file permissions and service misconfigurations, requiring a deeper understanding of privilege escalation.

Tools Used: SSH, ls, cat, netstat, find

Steps:

1. Log in to the server as leviathan3.
2. Navigate to the /home/leviathan3 directory.
3. List the files to see what's available in the directory.
4. Read the README file for any instructions or hints.
5. Examine the files carefully to look for hidden files or content.
6. Look for any potential flags or puzzles in the files that will help you advance to the next level.
7. Use commands like cat, ls -la, and others to explore the directory and files more thoroughly if needed.

Level 3 - 4:

Objective: Level 4 requires you to explore system configurations and discover vulnerabilities that lead to privilege escalation or unauthorized access.

Tools Used: SSH, ls, cat, netstat, find

Steps:

1. Log in to the server as leviathan4.
2. Navigate to the /home/leviathan4 directory.
3. List the files in the directory to see what’s there.
4. Read the README file for instructions or hints related to the level.
5. Look for hidden files or directories that might contain important information.
6. Examine the file permissions using ls -la to check for any hidden or inaccessible files.
7. Search for any clues in the files or output that could help you unlock the next step or flag.
8. Use appropriate tools (e.g., cat, grep, strings, or others) to analyze and extract information from files.

Level 4 - 5:

Objective: In this level, you need to exploit configuration issues and mispermissions to gain unauthorized access and find the flag.

Tools Used: SSH, ls, cat, netstat, find

Steps:

1. Log in to the server as leviathan5.
2. Navigate to the /home/leviathan5 directory.
3. List the files to see what’s available in the directory.
4. Read the README file for hints or instructions.
5. Check file permissions using ls -la to see if any files are hidden or restricted.
6. Look for hidden files or directories that might contain useful information.

7. Examine the files carefully for clues, such as encoded data, binary files, or hidden messages.

8. Use various tools like cat, grep, strings, or others to analyze and extract hidden information from the files.

9. Look for clues related to decryption or encoding, which may help you solve the level's puzzle.

Level 5 - 6:

Objective: This level requires exploiting permission misconfigurations, especially SUID/SGID binaries, to escalate privileges and access restricted files.

Tools Used: SSH, ls, cat, netstat, find, grep, strings

Steps:

1. Log in to the server as leviathan6.
2. Navigate to the /home/leviathan6 directory.
3. List the files to see what is available in the directory.
4. Read the README file for instructions or hints for the level.
5. Check the file permissions using ls -la to identify hidden files or unusual access settings.
6. Look for hidden files or directories that may contain useful information.
7. Examine the contents of the files carefully, especially looking for encoded or encrypted data.
8. Use tools like cat, grep, strings, or others to search through the files for any clues or information.
9. Look for clues related to cracking or decrypting data, as this may be part of the challenge.

Level 6 - 7:

Objective: Leviathan Level 7 involves exploring file and user permissions, identifying vulnerable services, and escalating privileges.

Tools Used: SSH, ls, cat, netstat, find, grep, strings

Steps:

1. Log in to the server as leviathan7.
2. Navigate to the /home/leviathan7 directory.
3. List the files in the directory to see what's available.
4. Read the README file for instructions or hints on how to proceed with the level.
5. Check file permissions using ls -la to identify any hidden or restricted files.
6. Look for hidden files or directories that may contain useful clues.
7. Examine the contents of the files, especially searching for encoded, encrypted, or hidden messages.
8. Use tools like cat, grep, strings, or others to analyze files and extract important information.

9. Look for clues related to cracking or decrypting information that will help you move to the next level.

CONCLUSION:

The Leviathan levels help you learn how to explore a system, find weaknesses, and gain higher access. By using tools like SSH, ls, find, ps, and cat, you practice discovering problems, fixing them, and finding the flag, which teaches important cybersecurity skills.