Ayuda de Memoria

Dificultad	Sin empezar
Finalizada	☐

IPs

Nombre	IP
HTB VPN	
Target	

Credentials

Username	Hash	Password	Purpose	Additional Notes

Reconnaissance

1. Tenga en cuenta que algunos sitios web sólo son accesibles a través de navegadores antiguos como Internet Explorer.
2. Ten en cuenta que algunos sitios web pueden carecer de la página de índice y no redirigirte en absoluto a la página de inicio. Si ese es el caso, intente adivinar manualmente una ruta completa a la página de inicio, use wayback machine (gau) para encontrar URLs antiguas, o intente directory fuzzing con DirBuster.
3. Busca en Internet rutas y archivos predeterminados para una aplicación web específica. Utilice la información recopilada en combinación con Google Dorks o httpx para encontrar las mismas rutas/archivos en diferentes sitios web. Para aplicaciones web no tan comunes, intente encontrar y navegar por el código fuente en busca de rutas/archivos por defecto.

4. Puedes encontrar el código fuente de la aplicación en GitHub, GitLab, searchcode, etc.
5. Busca en el código fuente de la aplicación claves API, claves SSH, credenciales, tokens, hosts y dominios ocultos, etc. No olvides comprobar los commits antiguos de GitHub en busca de claves de API antiguas pero aún activas, tokens secretos, etc.
6. Inspecciona la consola web en busca de posibles errores. Inspecciona el código fuente de la aplicación en busca de posibles comentarios.
7. No olvides acceder al servidor web a través de una dirección IP porque podrías encontrar la página de bienvenida por defecto del servidor o algún otro contenido.

▼ Scanning/Enumeration

1. Tenga en cuenta que las aplicaciones web pueden alojarse en otros puertos además de 80 (HTTP) y 443 (HTTPS), por ejemplo, pueden alojarse en el puerto 8443 (HTTPS).
2. Ten en cuenta que en los puertos 80 (HTTP) y 443 (HTTPS) un servidor web puede alojar diferentes aplicaciones web o algunos otros servicios por completo. Utilice Ncat o Telnet para la captura de banners.
3. Tenga en cuenta que en diferentes rutas URL un servidor web puede alojar diferentes aplicaciones web o algunos otros servicios por completo, por ejemplo, somesite.com/app_one/ y somesite.com/app_two/.
4. Mientras escanea en busca de vulnerabilidades o ejecuta cualquier otro escaneo intensivo, compruebe periódicamente la aplicación/servicio web en caso de que se bloquee para poder alertar a su cliente lo antes posible. Además, muchas veces puede que el cortafuegos de aplicaciones web (WAF) o algún otro producto de seguridad te bloquee temporalmente y todas tus peticiones posteriores no sean válidas.
5. Si una aplicación web deja de responder de repente, intenta acceder a la aplicación web con tus datos móviles (es decir, utiliza una IP diferente). Es posible que tu IP actual haya sido bloqueada temporalmente.
6. Envíe un mensaje de correo electrónico a una dirección inexistente en el dominio del objetivo, a menudo revelará información útil de la red interna a

través de una notificación de no entrega (NDN).

7. Intente invertir en Nessus Professional y Burp Suite Professional o cualquier otra herramienta permium similar si puede permitírselo.

▼ Exploiting

1. Pruebe siempre el inicio de sesión nulo (es decir, sin contraseña) o busque en Internet las credenciales predeterminadas para una aplicación web específica.
2. Intente manipular cookies o tokens para obtener acceso o elevar privilegios.
3. Intentar cambiar una solicitud HTTP POST en una solicitud HTTP GET (es decir, en una cadena de consulta) y ver si un servidor la acepta.
4. Desactiva JavaScript en tu navegador y comprueba de nuevo el comportamiento de la aplicación web.
5. Comprueba el comportamiento de la aplicación web en dispositivos móviles, por ejemplo, busca vulnerabilidades en m.somesite.com porque algunas funciones podrían funcionar de forma diferente.
6. Si desea automatizar sus pruebas de inyección de código, consulte la subsección Listas de palabras para ver las listas de palabras de inyección de código. La mayoría de las listas de palabras también incluyen inyecciones de código ofuscado.
7. **No olvides eliminar todos los artefactos creados una vez que hayas terminado las pruebas.**

▼ Post Exploiting

1.

▼ Password Cracking

1. Busca un hash en Google antes de intentar descifrarlo porque podrías ahorrarte mucho tiempo y problemas.
2. Utiliza Google Dorks, Chad, o FOCA para encontrar archivos y dentro de los metadatos del archivo los nombres de usuario del dominio para hacer fuerza bruta.
3. Ten en cuenta que podrías bloquear las cuentas de otras personas.

4. Ten en cuenta que algunos formularios web implementan CAPTCHA y/o tokens de envío ocultos que pueden impedirte la fuerza bruta. Intenta enviar solicitudes sin tokens o CAPTCHA.
5. Puedes encontrar un montón de listas de palabras en SecLists.