

**Домашнее задание № 35-36**

***Pentest***

***metasploit pro/nessus-cybersecurity forum***

1. **Ознакомиться с основными ресурсами Pentest лекции**
2. **Скачать** [**вирутальную машину**](https://www.vulnhub.com/entry/hacklab-vulnix,48/) **и получить флаг vulnix \*root**
3. **Скачать** [**dump сети**](https://disk.yandex.ru/d/44gcTedPdeVCGw) **и найти флаг, прислать скрин флага (пароль: teachmeskills, ищем image)**

*Repeat кто не делал:*

1. **Объединить Kali Linux и Metasploit в одну подсеть**
   1. провести сканирование Metasploit VM с использованием nmap (2 способами, без флагов и с script=vuln)
2. **На Kali сделать брут Metasploit VM с использованием hydra, прислать скрин об успешном бруте.**
3. **Провести повышение привилегий используя найденные уязвимости над Metasploit VM**

Ссылки на дополнительные ресурсы

* [Гайд эксплоита metasploitable 2](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide)
* [Словари, атаки на пароли](https://github.com/danielmiessler/)
* [Hashcat таблица хешей](https://hashcat.net/wiki/doku.php?id=example_hashes)
* [Hashcat примеры](https://hackware.ru/?p=14217)
* [Hydra brute force](https://github.com/vanhauser-thc/thc-hydra)
* [Exploit database](https://www.exploit-db.com)
* [Cobalt Strike](https://www.cobaltstrike.com/)