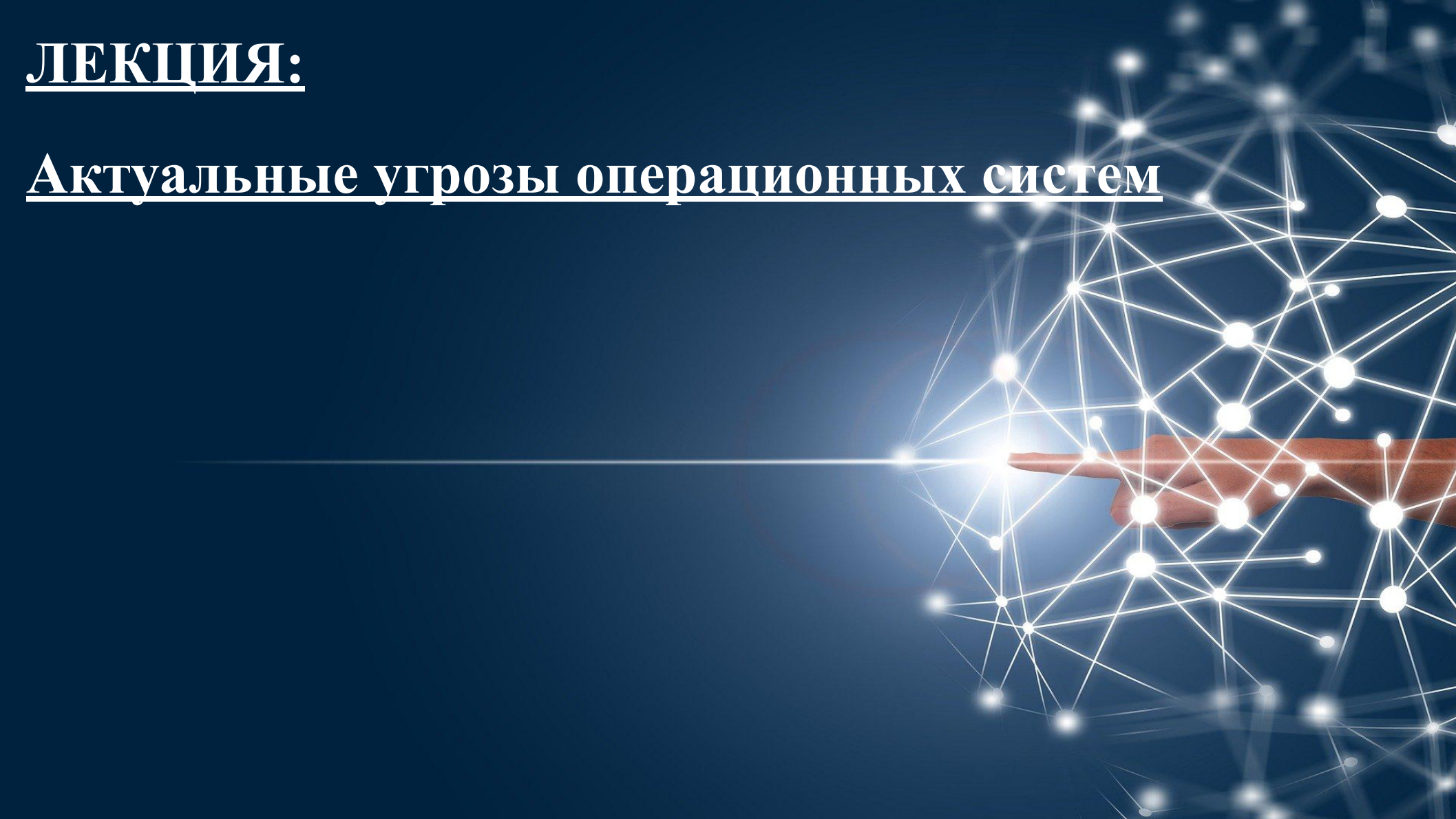
ЛЕКЦИЯ:

Актуальные угрозы операционных систем



ВОПРОСЫ:

1. Классификация угроз операционных систем.

2. Угрозы операционных систем в среде виртуализации.

ВОПРОСЫ:

1. Классификация угроз операционных систем.

Классификация угроз операционных систем.

CASE

Серверные дистрибутивы Linux являются основой большинства дата-центров, а также предприятий различной формы и размера. Кроме этого, на базе этой операционной системы сегодня работает значительная часть сети Интернет, включая серверы таких компаний, как Google, Facebook и Twitter. Поэтому неудивительно, что в течение нескольких предыдущих лет было немало примеров атак, в результате которых понесли убытки пользователи именно этой ОС.

В 2018 году специалисты **ESET** обнаружили **семейство бэкдоров в OpenSSH**, которые злоумышленники использовали для управления от имени администраторов. Исследователи обнаружили 21 семейство вредоносных программ, в том числе десять, которые до этого никогда не были зафиксированы. Это исследование стало результатом трехлетней работы, которая позволила получить большое количество информации об экосистеме вредоносного программного обеспечения для этой операционной системы в целом.

Классификация угроз операционных систем.

В ходе анализа бэкдоров специалисты ESET использовали одно из предыдущих исследований — **операции Windigo**, во время которой было заражено более **25 000 серверов**, большинство из которых работали на базе Linux.

Windigo была раскрыта **ESET совместно с CERT-Bund**, **исследовательским центром SNIC и европейской организацией ядерных исследований (CERN)**.

Эти машины использовались для кражи учетных данных, проведения спам-кампаний, а также для перенаправления веб-трафика на вредоносные веб-страницы. Для получения контроля над зараженными серверами и кражи данных использовался **бэкдор Linux/Ebury**. Стоит отметить, что этот бэкдор до сих пор обновляется и использ[illegible]ется в реальной среде, в частности в 2020 году были выявлены новые образцы.

Классификация угроз операционных систем.

По цели атаки:

- несанкционированное чтение информации;
- несанкционированное изменение информации;
- несанкционированное уничтожение информации;
- полное или частичное уничтожение ОС.

Классификация угроз операционных систем.

По принципу воздействия на операционную систему:

- использование известных (легальных) каналов получения информации;
- Например, угроза несанкционированного чтения файла, где пользовательский доступ определен неправильно, то есть доступ разрешен пользователю, которому согласно политике безопасности должно быть отказано в доступе;
- использование скрытых каналов для получения информации; например, угроза со стороны злоумышленника, использующего недокументированные возможности ОС;
- создание новых каналов получения информации с помощью программных закладок.

Классификация угроз операционных систем.

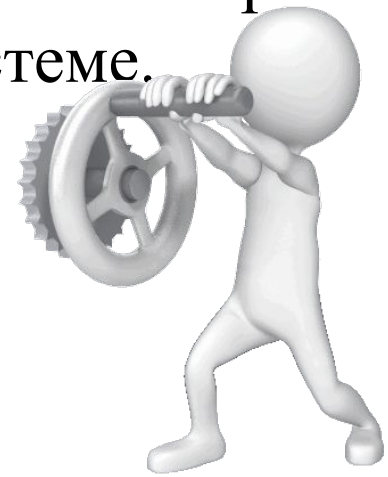
По типу защиты уязвимости, использованной злоумышленником:

- «неадекватная» политика безопасности, в том числе ошибки системного администратора;
- ошибки и недокументированные возможности программного обеспечения ОС, в том числе так называемые люки — случайно или намеренно встроенные в систему «служебные входы», позволяющие обойти систему защиты;
- ранее реализованная программная закладка.

Классификация угроз операционных систем.

По характеру воздействия на операционную систему:

- активное влияние — несанкционированные действия злоумышленника в системе;
- пассивное влияние — несанкционированный мониторинг злоумышленником процессов, происходящих в системе.



Классификация угроз операционных систем.

Классификация типичных атак:

Сканирование файловой системы. Злоумышленник просматривает файловую систему компьютера и пытается прочитать (скопировать) все файлы подряд. Рано или поздно обнаруживается хотя бы одна ошибка администратора. В результате злоумышленник получает доступ к информации, которая должна быть ему запрещена.

Классификация угроз операционных систем.

Классификация типичных атак:

Угадывание пароля. Есть несколько методов подбора паролей пользователей:

- тотальный поиск;
- брутфорс, оптимизированный по статистике появления символов или с помощью словарей;
- подбор пароля с учетом знаний о пользователе (его имя, фамилия, дата рождения, номер телефона и т. д.).

Классификация угроз операционных систем.

```
root@pc:/home/user# hydra
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [
-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap
2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp
s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at https://github.com/vanhauser-thc/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

Классификация угроз операционных систем.

Классификация типичных атак:

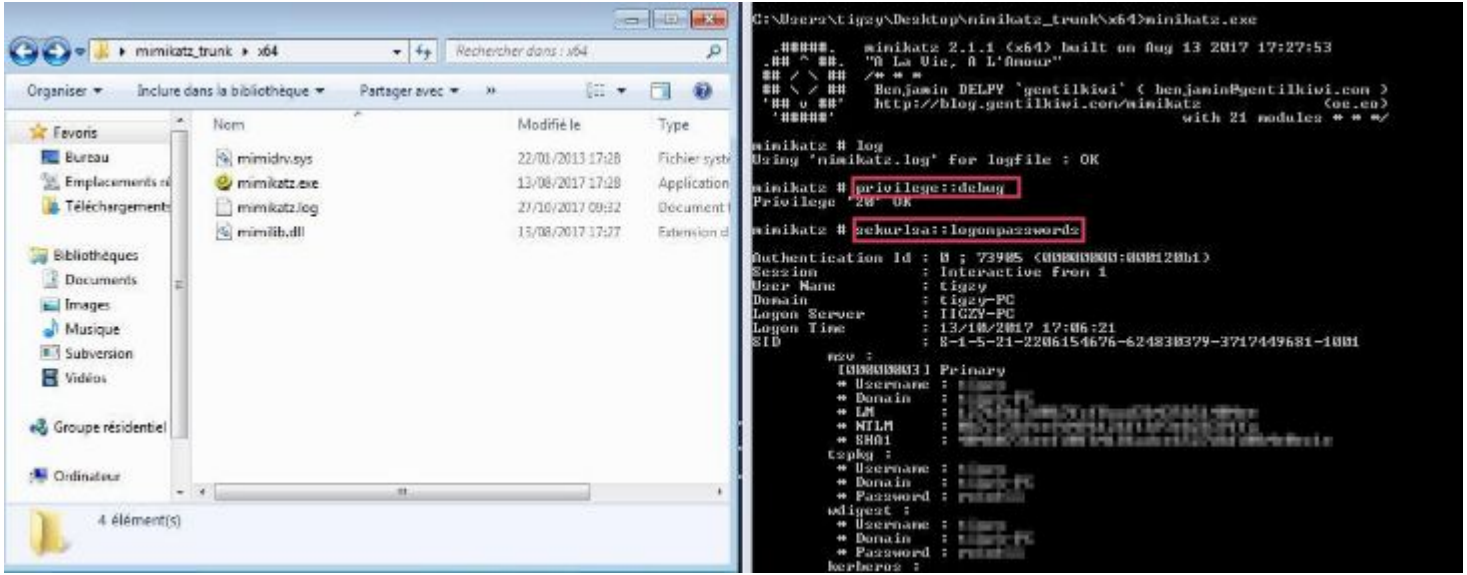
Кража ключевой информации. Злоумышленник может следить за паролем, введенным пользователем, или восстанавливать введенный пароль, перемещая руки по клавиатуре. Можно просто украсть.

Классификация угроз операционных систем.

Mimikatz — это приложение с открытым исходным кодом, которое позволяет пользователям просматривать и сохранять учетные данные аутентификации, такие как тикеты Kerberos. Бенджамин Делпи продолжает руководить разработкой Mimikatz, поэтому набор инструментов работает с текущей версией Windows и включает самые современные виды атак.

Злоумышленники обычно используют Mimikatz для кражи учетных данных и повышения привилегий: в большинстве случаев программное обеспечение для защиты конечных точек и антивирусные системы обнаруживают и удаляют его. И наоборот, специалисты по тестированию на проникновение используют Mimikatz для обнаружения и тестирования уязвимостей в ваших сетях, чтобы вы могли их исправить.

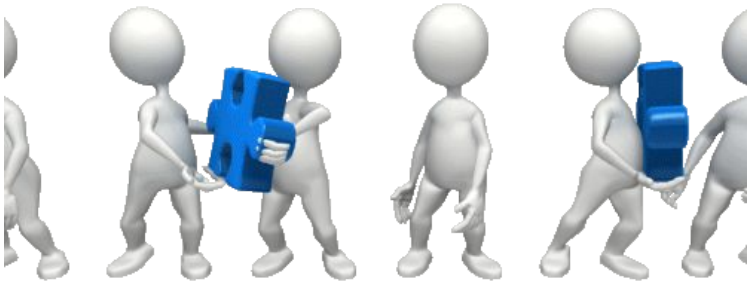
Классификация угроз операционных систем.



Классификация угроз операционных систем.

Классификация типичных атак:

Сборка мусора. Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная (так называемый мусор). Злоумышленник восстанавливает эту информацию, просматривает и копирует интересующие его фрагменты.



Классификация угроз операционных систем.

Утилита dd – мощная программа, включенная по умолчанию во все основные дистрибутивы Linux. С ее помощью мы можем заполнить содержимое диска нулями или случайными данными.

В обоих случаях мы можем использовать данные, сгенерированные специальными файлами: /dev/zero и dev/urandom (или /dev/random) соответственно. Первый возвращает нули каждый раз, когда над ним выполняется операция чтения; второй возвращает случайные байты, используя генератор случайных чисел ядра Linux.

Чтобы заполнить диск нулями, мы можем запустить:

sudo dd if=/dev/zero of=/dev/sdx

Чтобы использовать случайные данные, вместо этого:

sudo dd if=/dev/urandom of=/dev/sdx

Классификация угроз операционных систем.

Классификация типичных атак:

Злоупотребление властью. Злоумышленник, использующий ошибки в рейтинге программного обеспечения ОС или политике безопасности, имеет полномочия, превышающие полномочия, предоставленные ему в соответствии с политикой безопасности. Обычно это достигается запуском программы от имени другого пользователя.

Классификация угроз операционных систем.

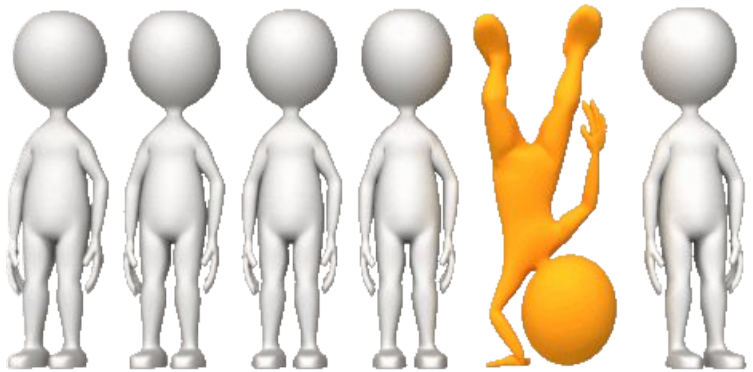
Классификация типичных атак:

Закладки программы. Программные закладки, встроенные в ОС, программно не отличаются от закладок других кл[illegible].

Классификация угроз операционных систем.

Классификация типичных атак:

Жадные программы — это программы, которые намеренно потребляют большие ресурсы компьютера, чтобы создать медленную работу других программ. Запуск жадной программы может привести к сбою ОС.



ВОПРОСЫ:

2. Угрозы операционных систем в среде виртуализации.

Угрозы операционных систем в среде виртуализации.

Kaspersky

Есть распространенное мнение, что виртуализация значительно снижает риски от киберугроз. Действительно, на виртуальной машине, как правило, не хранятся данные. И даже если ее пользователь случайно активирует трояна, то все вредоносные изменения автоматом исчезнут после перезапуска: гипервизор просто поднимет свежую машину из образа. Однако, как показывает практика, шифровальщики могут атаковать и виртуальную инфраструктуру. Конкретный пример — атака через уязвимые версии VMware ESXi, о которой не так давно писали в издании ***ZDNet****.*

Угрозы операционных систем в среде виртуализации.

Kaspersky

Гипервизор VMware ESXi *позволяет множеству виртуальных машин хранить информацию на одном сервере. Осуществляется это через протокол Open SLP (Service Layer Protocol), который, помимо всего прочего, позволяет обнаруживать сетевые устройства без предварительной конфигурации. Речь идет о двух уязвимостях этого протокола —* ***CVE-2019-5544*** *и* ***CVE-2020-3992****, обе известны уже достаточно давно, и обе не в первый раз используются злоумышленниками. Первая позволяет провести атаку переполнения динамической памяти (heap overflow), а вторая относится к типу Use-After-Free, то есть связана с некорректным использованием той же самой динамической памяти в процессе работы.*

Угрозы операционных систем в среде виртуализации.

Области воздействия

- Дисковое пространство
- Оперативная память
- Процессора
- Сеть

Угрозы операционных систем в среде виртуализации.

Источники воздействия

- Виртуальные машины
- Гипервизоры
- Менеджмент машина
- Внешней сетевой периметр

Угрозы операционных систем в среде виртуализации.

Способы внедрения вредоносного ПО

- Из дисков подгружаемых в виртуализацию
- При повседневной работе с VM (установка зависимостей, обновление)
- Из образов для разворота VM

Угрозы операционных систем в среде виртуализации.

Необходимо использовать:

- программные продукты для анализа трафика и предотвращения вторжений, разработанные специально для виртуальной среды;
- ПО для разграничения прав доступа к виртуальной инфраструктуре;
- продукты для проведения аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности;
- продукты обеспечения безопасного, аппаратно контролируемого подключения терминалов тонкого клиента к ВМ, исполняемым на сервере.

СПАСИБО ЗА ВНИМАНИЕ!