**Архитектура**

1. В инфраструктуре небольшой организации находятся: 2 домен контроллера, файловый сервер, онлайн-магазин (Web-сервер, SQL сервер). Отдельным сотрудникам требуется удаленный доступ для работы с данными на файловом сервере. Нарисуйте схему сети с указанием серверов, сетевых сегментов и рекомендуемых сетевых правил.

Рекомендация поставить межсетевой экран аппаратный и сервер прокси.



1. В инфраструктуре одной организации ресурсы находятся в 2ух доменах с полным двухсторонним доверием. В домене А – конфиденциальные ресурсы, в домене B- обычные. При этом, пользователям из домена А нужны ресурсы из домена А и домена B, а пользователям из домена B - только ресурсы из домена B.

Опишите возможные риски ИБ и предложите меры по их митигации.

Риски ИБ утечка конфиденциальных данных, действия неблагонадежных сотрудников (человеческий фактор).

Предложения по мере митигации домен А, домен В внести в разные подсети и настроить маршрутизацию к ресурсам домена В, поставить межсетевой экран и прокси сервер, установить антивирусную защиту, secret net.

1. Организация срочно решила полностью перевести своих сотрудников на удаленную работу. Половина из них имеет корпоративные ноутбуки, другая половина – работают с личных домашних компьютеров. При этом часть сотрудников продолжает периодически приезжать в офис. Предложите способы организации безопасного удаленного доступа к конфиденциальной информации, находящейся на внутренних серверах

Организовать прямой доступ пользователей. Пользователь получает IP-адрес из своего VPN-пула и может идти напрямую к необходимым ресурсам (через межсетевой экран например WATCHGUARD). Политики придется создавать непосредственно на VPN-шлюзе либо использовать RADIUS

Другой вариант организации удаленного доступа **Терминальный доступ.** Имеется NGFW с политиками по пользователям и терминальный сервер, то можно сделать так. При реализации терминального доступа (например, с помощью MS RDS) пользователь, получивший удаленный доступ, логинится на терминальный сервер. Установить специальный агент от производителя межсетевых экранов.. Этот агент будет сообщать межсетевому экрану IP-адрес залогинившегося пользователя.

Рабочие места пользователей.  
  
Установить на рабочие станции необходимое ПО безопасности (antivirus, host-based IPS/Sandbox и т.п. Одним из хороших вариантов также будет публикация на VDI конкретного приложения для работы (браузера, почтового клиента). Это позволит разрешить доступ только к конкретным используемым приложениям. Запретить подключение съемных носителей.  
Отключены небезопасные протоколы и службы (NetBios, LLMN, FTP, HTTP, POP3, SMTP, Telne и другие), нелишним будет включить шифрование диска, отобрать права привилегированного доступа, запретить изменения сетевых настроек пользователей, доступ узлов нфраструктуры ко внешним DNS-серверам,

исключить использование утилит для удаленного доступа TeamViewer, Ammyy Admin, RMS.

**Антивирусная защищенность**

1. Какие механизмы защиты от вирусов-шифровальщиков используют современные антивирусы? Сигнатурный анализ, эвристический анализ, HIPS защита, VirusScope, Anti-Ransomware Tool

2. Опишите последовательность действий ИБ-специалиста при обнаружении вируса на компьютере пользователя.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации подразделения (технологического участка) должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

• приостановить работу;

• немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности своего подразделения, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

• совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

• провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов ОА);

• в случае обнаружения нового вируса, не поддающегося лечению ' применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске в ОА для дальнейшей отправки его в организацию, с которой заключен договор на антивирусную поддержку;

• по факту обнаружения зараженных вирусом файлов составить служебную записку в отдел обеспечения безопасности информации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

**SIEM**

1. О чем говорит большое количество событий Event ID 4625? Большое количество говорит, что выполнялся подбор пароля. учетная запись не смогла войти в систему.

Что более опасно в этом случае – LogonType 3 или LogonType 2?

Тип входа 3: Сетевой. Пользователь по сети подключился к этому компьютеру и авторизовался на нем.

1. О чем может говорить нахождение в логах для одной и той же учетки

двух событий подряд: Event ID 4625 и Event ID 4672?

К учетной записи присвоены специальные привилегии

1. Анализом каких событий в логах можно обнаружить атаку Kerberoasting?

Детектирование по журналам **событий**. В журналах **событий** нужно **выявлять** аномалии в запросах TGS-билетов (**событие** 4769 «Запрошен билет службы **Kerberos**»): анализировать все учетные записи и IP-адреса, с которых был выполнен запрос к сервису, и проверять, запрашивает ли обычно учетная запись с этого же IP-адреса TGS-билет к рассматриваемому сервису

**AD**

1. Что такое krbtgt, где и для чего он используется?

Учетная запись **KRBTGT** – это специальная учетная запись в AD, которая подписывает все. Злоумышленники, получившие доступ к контроллеру домена (DC), могут **использовать** эту учетную запись для создания, который даст **им** неограниченный доступ к практически любой системе в корпоративной сети.

1. В каких механизмах защиты участвует группа Protected Users?

В версии Active Directory, представленной в Windows Server 2012, появилась **группа** пользователей нового типа под названием **Группа** Защищенных пользователей (**Protected** **Users**). Она предоставляет дополнительные инструменты **защиты** и предотвращает аутентификацию пользователей с использованием шифрования RC4

1. Какие параметры регулирует опция в AD PasswordComplexityEnabled?

Регулирует параметры, чтобы пользователь использовал сложный пароль

**Пароли**

1. Опишите подробно -что делает указанный ниже скрипт ?

$credentials = Get-Credential contoso\administrator  
$key = @(1..24)  
$credentials.Password | ConvertFrom-SecureString -Key $key | Set-Content pass.txt

Выгружает список учетных записей и паролей преобразовывает пароль в шифрованную строку записывает новое содержимое в текстовый файл

1. Для управления ИТ инфраструктурой организации используется решение Ansible с помощью которого на целевые сервера разливаются обновления и устанавливается различное ПО. Соответственно, в плейбуках хранится множество логинов\паролей и ssh-ключей. Предложите меры по минимизации рисков утечки данных секретов

Шифровать данные с помощью Vault

**Облака**

1. В чем отличие между OAuth и OpenID?

[OpenID](http://openid.net/) -это аутентификация (т. е. доказательство того, кто вы есть), [OAuth](http://oauth.net/) -авторизация (т. е. чтобы предоставить доступ к functionality/data/etc.. без необходимости иметь дело с первоначальной аутентификацией).

OAuth может использоваться на сайтах внешних партнеров для предоставления доступа к защищенным данным без необходимости повторной аутентификации пользователя.

1. Для чего предназначен WS-Security?

WS-Security предлагает защиту конфиденциальности и целостности от создания сообщения до его потребления. Таким образом, вместо того, чтобы гарантировать, что содержимое сообщений может быть прочитано только правильным сервером, оно гарантирует, что оно может быть прочитано только правильным процессом на сервере. Вместо того, чтобы предполагать, что все сообщения в безопасно инициированном сеансе принадлежат аутентифицированному пользователю, каждый из них должен быть подписан.

**Workstation**

1. По какому пути хранятся журналы ОС на машине с Windows 10?

**C**:\ **Windows**\ System32\ winevt\ Logs

1. К чему приведет установка параметра Cached Credentials Count =0?

Если задать **0**, это запретит Windows кэшировать учетные данные пользователей. В этом случае при недоступности домена, при входе пользователя появится ошибка “There are currently no logon servers available to service the logon request”.

1. Для чего обычно используется следующая команда и какое известное ПО использует результаты ее выгрузки: procdump.exe -accepteula -ma lsass.exe lsass.dmp?

Используется ПО Procdump, чтобы сдампить процесс LSASS для выгрузки паролей из памяти в чистом виде можно при помощи утилиты [mimikatz](http://blog.gentilkiwi.com/securite/mimikatz/minidump)

**Web**

1. Какой заголовок используется защиты от XSS-атак, с блокировкой загрузки страницы?

**Заголовок** ответа HTTP X-**XSS**-Protection

1. Чем можно обеспечить защиту от ClickJacking?

Чтобы обеспечить защиту от ClickJacking в http(d)/Apache, нужно добавить заголовок в .htaccess файл.

Header always set X-Frame-Options SAMEORIGIN

Header always set X-Frame-Options DENY

**Vuln**

1. Что общего между атаками Petya и WannaCry?

использует уязвимость EternalBlue, но не ограничивается ею

1. Какие меры защиты можно применить для защиты от уязвимостей
2. CVE-2021-36934

ограничение доступа к проблемной папке и удалению её теневых копий.

вручную ограничить доступ к каталогу Windows\system32\config

b) [CVE-2021-34527](https://www.kaspersky.ru/blog/printnightmare-vulnerability/31025/)

Установка [патча для закрытия уязвимости CVE-2021-34527](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)

[Отключить сервис диспетчера очереди печати](https://docs.microsoft.com/en-us/defender-for-identity/cas-isp-print-spooler) на машинах, которым он наверняка не нужен. В частности, серверам, на которых работают контроллеры доменов.

Отключение входящей удаленной печати с помощью групповой политики.

Снабдить инфраструктуру защитным решением Kaspersky Endpoint Security Cloud

**Скрипты**

1. Напишите короткий скрипт на Powershell который бы выгружал из Active Directory в текстовый файл Display name всех сегодня успешно залогинившихся пользователей, входящих в группы SECURITY, у которых пароль поменялся меньше 3 дней назад.

Get-ADUser -Filter \*).Name | Get-UserLogged

Get-ADGroup -Filter {GroupCategory -eq "Security"} | Get-ADGroupMember | Export-CSV C:\ Display name. txt

**Hardware**

1. Какой бы конфигурации сервер (платформа/вендор/модель, ядра, память, сет.адаптер(ы), диски - кол-во и массив(ы), др. - ключевое на ваш взгляд) вы бы предложили для организации небольшой фермы на базе Hyper-V/VMware ESXi на 4 сервера для фирмы:

* Windows Server для роли Domain Controller (ADDS/DNS/DHCP/др.) на 20 пользователей,
* Linux с прокси для них,
* RDS сервер для них же,
* СУБД на базе MSSQL для баз данных (например, 1С)?

Какие дополнительные меры защиты для этого сервера/сети вы бы предложили? Приведите краткий список технологий/решений.

Windows Server для роли Domain Controller (ADDS/DNS/DHCP/др.) на 20 пользователей сервер Lenovo ThinkSystem ST50 7Y48S04B00 (Tower / Lenovo / ThinkSystem ST50 7Y48S04B00, 4 ядра, 16ГБ память, сет.адаптер с 1 Гбит/c,

4 диска по 500ГБ RAID-10)

Linux с прокси сервер Lenovo ThinkSystem ST50 7Y48S04B00 (Tower / Lenovo / ThinkSystem ST50 7Y48S04B00, 4 ядра, 32ГБ память, сет.адаптер с 1 Гбит/c,

1 диск WD VelociRaptor WD1000DHTZ 1ТБ)

RDS сервер платформа SuperMicro SYS-7049P-TR (Tower / SuperMicro / ThinkSystem SYS-7049P-TR,1 процессор Intel Xeon Gold 6136 12 ядер, 64 ГБ памяти, сет.адаптер с 1 Гбит/c, 2 ssd диска по 250 ГБ RAID-10)

СУБД на базе MSSQL для баз данных (например, 1С) Серверная платформа SuperMicro SYS-7049P-TR (Tower / SuperMicro / ThinkSystem SYS-7049P-TR,1 процессор Intel Xeon Gold 6136 12 ядер, 64 ГБ память, сет.адаптер с 1 Гбит/c, четыре SAS-диска в RAID 10)

Меры защиты поместить сервера в изолированную среду исполнения. Поставить межсетевой экран с поддержкой vpn. Провести Аудит сервисов и реализацию аудита сервисов.

1. Приведите пример скрипта на bash или playbook для ansible для выполнения hardening настроек sshd демона на RHEL8-based машинах (10 машин, IP адреса 10.5.12.14 - 10.5.12.23). Что бы вы изменили из настроек "по умолчанию" в конф.файлах? Будут ли отличия на Ubuntu 20.xx?

hosts.ini

[test]

10.5.12.14

10.5.12.15

10.5.12.16

10.5.12.17

10.5.12.18

10.5.12.19

10.5.12.20

10.5.12.21

10.5.12.22

10.5.12.23

ansible.conf

[test:vars]

ansible\_ssh\_user= root

ansible\_ssh\_pass= /etc/ssh/id\_rsa.pub

---

* name: connect

hosts: test

become: true

tasks:

- name: copy script

copy: src=test.sh dest=/home mode=0777

- name: run script

command: sh /home/test.sh

- name: restart sshd

command: service sshd restart

listing test.sh

sed -i -e "s/Port 22/Port 62325/g;/Port 62325/s/^#//g;s/AddressFamily any/AddressFamily inet/g;/AddressFamily inet/s/^#//g;s/PermitRootLogin yes/PermitRootLogin no/g;/PermitRootLogin no/s/^#//g;s/MaxAuthTries 6/MaxAuthTries 3/g;/MaxAuthTries 3/s/^#//g;s/LoginGraceTime 2m/LoginGraceTime 30/g;/LoginGraceTime 30/s/^#//g;/PermitEmptyPasswords no/s/^#//g;/LogLevel ERROR/s/^#//g;s/ClientAliveInterval 0/ClientAliveInterval 300/g;/ClientAliveInterval 300/s/^#//g;/PrintLastLog yes/s/^#//g;/TCPKeepAlive yes/s/^#//g;/ShowPatchLevel no/s/^#//g;s/MaxStartups 10:30:100/MaxStartups 10:50:20/g;MaxStartups 10:50:20/s/^#//g" /home/test

systemctl restart sshd

sed "20a\Protocol 2" /home/test

systemctl restart sshd

systemctl daemon-reload

Настройки sshd.config в RHEL8-based и Ubuntu 20.xx одинаковые

В sshd.config изменил бы строки:

'/Port 62325/s/^#//g' /home/test

"s/AddressFamily any/AddressFamily inet/g" /home/test

'/AddressFamily inet/s/^#//g' /home/test

"s/PermitRootLogin yes/PermitRootLogin no/g" /home/test

'/PermitRootLogin no/s/^#//g' /home/test

"20a\Protocol 2" /home/test

"s/MaxAuthTries 6/MaxAuthTries 3/g" /home/test

'/MaxAuthTries 3/s/^#//g' /home/test

"s/LoginGraceTime 2m/LoginGraceTime 30/g" /home/test

'/LoginGraceTime 30/s/^#//g' /home/test

'/PermitEmptyPasswords no/s/^#//g' /home/test

'/LogLevel ERROR/s/^#//g' /home/test

"s/ClientAliveInterval 0/ClientAliveInterval 300/g" /home/test

'/ClientAliveInterval 300/s/^#//g' /home/test

'/PrintLastLog yes/s/^#//g' /home/test

"/UseDNS yes/s/^#//g" /home/test

"/TCPKeepAlive yes/s/^#//g" /home/test

"/ShowPatchLevel no/s/^#//g" /home/test

"s/MaxStartups 10:30:100/MaxStartups 10:50:20/g" /home/test

"/MaxStartups 10:50:20/s/^#//g" /home/test

1. Как вы администрируете удалённые сервера? Протоколы, ПО, автоматизация – ваш опыт кратко

Администрирую сервера терминально по протоколу ssh и графикой по vnc, автоматизация бэкап/рестор бд firebird