

PENETRATION TESTING

BLUEPRINT: СОЗДАВАЯ ЛУЧШИЙ ПЕРО ТЕСТЕР

Ценное тестирование на проникновение включает в себя моделирование методов, используемых настоящими компьютерными злоумышленниками, для поиска уязвимостей и, при контролируемых обстоятельствах, для профессионального и безопасного использования этих уязвимостей в соответствии с тщательно разработанным объемом и правилами взаимодействия. Этот процесс помогает определить бизнес-риски и потенциальные последствия атак, и все это помогает организации повысить уровень безопасности.

Ниже приведены советы для каждого этапа тестирования на проникновение, которые помогут вам повысить бизнес-ценность вашей работы.

PRE-ВЗАИМОДЕЙСТВИЕ

Обсудить **черный ящик** против **кристалл / белый ящик** тестирование при создании вашего **Правил участия**, отмечая, что Тестирование Crystal Box часто дает более подробные результаты, является более безопасным и повышает эффективность бизнеса.

Обсудите с целевыми сотрудниками системы особую важную информацию, которую они имеют в своей среде (такие как PII) и как вы можете измерить доступ к нему, фактически не загружая его. Подумайте о том, чтобы выбрать типовые записи для демонстрации вашего доступа вместо реальных конфиденциальных данных.

Держите свои навыки свежими, выделяя час или два в неделю для участия в **Захват флага соревнования**, в том числе **бесплатно** SANS Holiday Hack Challenge в www.holidayhackchallenge.com или многочисленные бесплатные CTF в <http://www.amanhardikar.com/mindmaps/Practice.html>

РАЗВЕДКА

Внимательно **учитывать все взаимодействия со сторонними серверами и поиски** чтобы вы не разглашали конфиденциальную информацию о цели и не нарушали соглашение о неразглашении, используя их. Вы можете захотеть **рассмотреть возможность использования сети TOR** скрыть ваши отношения с целевой организацией.

Ищите общие служебные документы, размещенные на цели веб-сайты с помощью поиска Google для:
site: <TargetDomain> ext: doc | ext: docx | ext: xls | ext: xlsx | внутр: pdf

Использовать **Директива поисковой системы Shodan «net:»** искать необычные или интересные устройства в целевых диапазонах сетевых адресов. Также используйте **уникальная информация нижнего колонтитула** (например, общее уведомление об авторских правах на целевых веб-страницах) для поиска дополнительных страниц с помощью Shodan с помощью директивы html :

Запомни **проверить сайты социальных сетей** (особенно LinkedIn, Facebook и Twitter), чтобы узнать о целевом персонале и технологии, которые они используют.

СОСТАВЛЕНИЕ ОТЧЕТОВ

Не ждите окончания теста на проникновение, чтобы написать отчет.

Вместо этого пишите отчет во время тестирования, выделяя время каждый день для написания от одной до трех страниц. Вы не только получите лучший отчет, но и сам тест по перу будет лучше.

Включить скриншоты в свой отчет чтобы проиллюстрировать результаты ясно. **Аннотировать скриншоты** со стрелками и кругами, указывающими на важные аспекты иллюстрации.

Чтобы повысить ценность ваших рекомендаций, **подумайте о том, чтобы включить шаги, которые может предпринять специалист по операциям**, чтобы убедиться, что **рекомендуемый файл установлен**, например, команда для проверки наличие патча. В некоторых случаях это может быть трудно сделать, поэтому в этих случаях рекомендуется вопрос подлежит повторной проверке.

Напишите для правильной аудитории в каждом разделе:

- Резюме должно быть для лиц, принимающих решения, которые выделяют ресурсы. Результаты должны быть написаны с технической точки зрения, с учетом бизнес-вопросов. Рекомендации должны учитывать оперативную группу и ее процессы.

Используйте шаблон, чтобы вести голосовой разговор к **определить область а также Правила участия**.

Ежедневно звоните с сотрудниками целевой системы обмениваться идеями и извлеченными уроками. Если ежедневно слишком часто, рассмотрите два звонка или три раза в неделю.

Определить цели по **IP-адресу** (IPv4 и IPv6, если у вас есть), доменное имя и (если вы есть) MAC-адрес (особенно для скомпрометированных клиентских машин, использующих DHCP).

VULNERABILITY АНАЛИЗ

Целевой организации.
проверить, что адреса имеют смысл и действительно принадлежат B LinkedIn, **искать долгосрочные ИТ и организационные изменения**, **использование кто поиски транскрипции** IP-адреса, включенные в область, принадлежит целевой в том числе брандмауэры, разработка среды и многое другое. Дважды проверьте, что вы

Запустите сниффер, такой как Wireshark, пока вы сканируете цель, чтобы вы могли **постоянно проверять** который

Ваш сканер все еще работает надлежащим образом.

Пока открытые порты такие как **TCP 445** часто указывают на машину Windows, это не всегда так. Цель может быть **Самба Демон** или **другая цель** для малого и среднего бизнеса.

Проверить найденные уязвимости по исследовать, как **проверить проблему вручную** или через сценарий bash, PowerShell, Nmap Scripting Engine (NSE) или другой сценарий.

Поместите уязвимости, которые вы **определили в контексте** насколько важен актив, так как это помогает вам определить приоритет и оценить риск.

Если вы используете **виртуальная машина** для ваших атак, **настроить его для мостового соединения** чтобы избежать заполнения таблиц NAT и гарантировать, что обратные соединения оболочки могут вернуться к вам.

ПОСТ-ЭКСПЛУАТАЦИЯ

Когда вы получаете доступ к целевому компьютеру, не используйте его для сканирования других целей, так как это может привести к **преждевременному обнаружению**. Вместо этого грабьте его для получения информации о других потенциальных целях, основанных на сетевой активности:

DNS-кеш (Windows): **c: \> ipconfig / displaydns**
ARP-кеш: **arp -a**
Установленные TCP-соединения: **netstat -na**
Таблица маршрутизации: **netstat -nr**

Когда вы получаете доступ к цели, если на машине установлен **сниффер**

(например, tcpdump или инструмент Wireshark's tshark), **запустите его, чтобы найти сетевой трафик** идентифицировать другие возможные целевые машины, а также протоколы открытого текста, содержащие конфиденциальные или

Полезная информация.

Даже без привилегий root, system или admin на целевом компьютере вы все равно можете

выполнять очень полезные деятельность после эксплуатации, включая получение списка пользователей, определение установленного (и, возможно, уязвимого) программного обеспечения и поворот через систему.

Когда вы получаете Windows box, ищите **УСТАНОВЛЕННЫЕ TCP-соединения** с портами 445 (SMB) и 3389 (RDP), так как эти другие системы могут быть отличными системами для разворота, если они находятся в области действия:

c: \> netstat -na | найти «EST» | найти «: 445» c: \> netstat -na | найти «EST» | найти «: 3389»

Хотя они могут быть очень полезны для демонстрации управления, **будьте осторожны при включении видеокамер и захвата звука с скомпрометированных целевых машин**. Проводить этот уровень инвазивного доступа только с письменного разрешения и иметь его

проверено вашей юридической командой, чтобы обеспечить соблюдение местных законов.

EXP LOITATION

При создании полезных нагрузок, которые уклоняются от инструментов защиты от вредоносных программ, **НЕ отправляйте свой образец на онлайн-сканирование сайтов** например, virustotal.com для проверки на уклонение, поскольку это может привести к потере полезной нагрузки при распространении новых обновлений подписки.

Настроить команду или скрипт который **проверяет доступность целевой службы** каждые несколько секунд, пока вы атакуете его. Таким образом, если вы его сломаете, вы заметите это быстро и сможете работать с целевой системой. персонал, чтобы перезапустить его.

Для ваших полезных нагрузок, **использовать протокол, который, вероятно, разрешен исходящим из целевой среды**, такие как HTTPS (с полезной нагрузкой с поддержкой прокси доступны в PowerShell Empire, Metasploit и Veil Framework) или DNS (например, инструмент DNScat).

Создайте свою полезную нагрузку так, чтобы **они делают обратное соединение с вами**, увеличивая вероятность того, что вы получите через брандмауэр, который разрешает исходящие соединения.

Чтобы снизить вероятность сбоя целевых систем и служб Windows, как только вы получите учетные данные уровня администратора и SMB-доступ к ним, **использовать rsexec или аналогичные функции Windows (WMIC, sc и т. д.)**, чтобы заставить их выполнять код.

вместо переполнения буфера или связанного с ним exploits.

Если ваш exploit не удался, **внимательно прочитайте вывод вашего инструмента exploits**, чтобы увидеть, где он выдает ошибку. Кроме того, запустите сниффер, такой как tcpdump, чтобы посмотреть, как далеко он продвигается в создании соединения, отправке exploits и загрузке сценического устройства и сцены. Если ваш Stager работал, но ваша сцена не может быть загружена, ваша тактика антивирусного уклонения может быть неудачной.

ПАРОЛЬ АТАКИ

Создать список слов, настроенный на целевую организацию основанный на слова с его сайта.

Создать список слов **точно настроен для пользователей на основе** на их профилях социальных сетей.

Когда вы успешно взламываете пароль, используя правила перебора слов, **добавьте этот пароль в свой словарь для дальнейших атак паролем в этом тесте на проникновение**. Таким образом, если вы встретите один и тот же пароль в другом формате хеширования, вам не нужно будет ждать, пока поиск по словам повторно обнаружит этот пароль.

Для подбора пароля всегда **рассмотреть политику блокировки учетной записи** и попытаться избежать этого с помощью **методы распыления паролей** (большое количество учетных записей и целей с небольшим количеством паролей).

Помните, что пароли могут быть получены с использованием различных методов, в том числе автоматическое угадывание, взлом, **сниффинг**, а также регистрация нажатия клавиши.

Иногда вы **не нужен пароль для аутентификации**, потому что простое использование хеша может сделать работу, как с **хакерские атаки против целей Windows и SMB**, и с **хеши паролей хранятся в куки** для некоторых сайтов.


Если у вас есть совместимый графический процессор в вашей системе, **рассмотреть возможность использования взлома паролей на основе графического процессора** инструмент, такой как Hashcat, так как вы получите от 20 до 100 раз больше производительности.

БЛУЭПР И НТ: БУ Я ЛД И НГ ЛУЧШИЙ ПЕРО ТЕСТЕР

ПЕНТ-PSTR-SANS18-BP-V1

SANS PEN TEST CURRICULUM

Категория	Идентификатор	Название	URL	Статус
	SEC460	Оценка угроз и уязвимостей предприятия	www.sans.org/SEC460	
GDIN	SEC504	Хакерские инструменты, методы, эксплойты и обработка инцидентов	www.sans.org/SEC504	
GWAPT	SEC542	Тестирование проникновения веб-приложений и этический взлом	www.sans.org/SEC542	по требованию
	SEC550	Активная защита, наступательные контрмеры и кибер-обман	www.sans.org/SEC550	
OPEN	SEC560	Тестирование проникновения в сеть и этический взлом	www.sans.org/SEC560	по требованию
	SEC561	Захватывающие практические методы взлома	www.sans.org/SEC561	
	SEC562	CyberCity Практическое упражнение по кинетическому диапазону	www.sans.org/SEC562	
	SEC564	Операции Red Team и эмуляция угроз	www.sans.org/SEC564	
	SEC567	Социальная инженерия для тестеров на проникновение	www.sans.org/SEC567	
GRYC	SEC573	Автоматизация информационной безопасности с Python	www.sans.org/SEC573	по требованию
GMOB	SEC575	Безопасность мобильных устройств и этический взлом	www.sans.org/SEC575	по требованию
	SEC580	Metasploit Kung Fu для тестирования пера предприятия	www.sans.org/SEC580	
GAWN	SEC617	Тестирование беспроводного проникновения и этический взлом	www.sans.org/SEC617	
	SEC642	Усовершенствованное тестирование на проникновение веб-приложений, методы этического взлома и эксплуатации	www.sans.org/SEC642	по требованию
GHPN	SEC660	Расширенное тестирование на проникновение, написание эксплойтов и этический взлом	www.sans.org/SEC660	по требованию
	SEC760	Усовершенствованная разработка эксплойтов для тестеров на проникновение	www.sans.org/SEC760	по требованию



GDIN Сертифицированное веб-приложение

GWAPT инцидентов Тестирование Penetration Tester

GPEN Кодер Python

GPYC

GMOB Mobi le Device Security Analyst Оценка и прослушивание

GAWN беспроводных сетей Exploit Research & Adv. Penetration Tester

GXPN тестер

Узнайте больше о курсах SANS PENETRATION и ETHICAL HACKING на www.sans.org/roadmap

PEN TEST BLOGS, ЛОЖКИ, СКАЧАТЬ, РЕСУРСЫ:
<https://pen-testing.sans.org>

POWERSHELL

<h3>Синтаксис</h3> <p>Командлеты - это небольшие скрипты, которые следуют соглашению между глаголом и существительным, например, "Get-Process".</p> <p>ПОХОЖИЕ ГЛАГОЛЫ С РАЗНЫМИ ДЕЙСТВИЯМИ:</p> <ul style="list-style-type: none"> New- Создает новый ресурс Набор- Модифицирует существующий ресурс Получить- Получает существующий ресурс Читать- Получает информацию из источника, такого как файл Найти- Используется для поиска объекта Поиск- Используется для создания ссылки на ресурс Начать- (асинхронный) начать операцию, такую как запуск процесса Вызывать- (синхронно) выполнить такую операцию, как выполнение команды <p>ПАРАМЕТРЫ:</p> <p>Каждый глагол с именем cmdlet может иметь много параметров для управления функциональностью командлета.</p> <p>ОБЪЕКТЫ:</p> <p>Выход большинства командлетов - это объекты, которые могут быть переданы другим командлетам и затем обработаны. Это становится важным в конвейере командлетов.</p>	<h3>5 Основы PowerShell</h3> <table border="1"> <thead> <tr> <th>КОМАНДЛЕТ</th><th>ЧТО ЭТО ДЕЛАЕТ?</th><th>HANDY ALIAS</th></tr> </thead> <tbody> <tr> <td>PS C:\> Get-Help [cmdlet]</td><td>Показывает помощь и примеры</td><td>PS C:\> Помощь [командлет] - Примеры</td></tr> <tr> <td>- примеры PS C:\> Get-Command PS C:\> ForEach-Object { \$ }</td><td>Показывает список команд. Показывает свойства и методы. Принимает каждый элемент в конвейере и обрабатывает его как \$</td><td>Get-Command PS C:\> [командлет] gm</td></tr> <tr> <td>PS C:\> Select-String</td><td>Ищет строки в файлах или выходных данных, например, gtr.</td><td>PS C:\> sls -path [файл] -pattern [строка]</td></tr> </tbody> </table>	КОМАНДЛЕТ	ЧТО ЭТО ДЕЛАЕТ?	HANDY ALIAS	PS C:\> Get-Help [cmdlet]	Показывает помощь и примеры	PS C:\> Помощь [командлет] - Примеры	- примеры PS C:\> Get-Command PS C:\> ForEach-Object { \$ }	Показывает список команд. Показывает свойства и методы. Принимает каждый элемент в конвейере и обрабатывает его как \$	Get-Command PS C:\> [командлет] gm	PS C:\> Select-String	Ищет строки в файлах или выходных данных, например, gtr.	PS C:\> sls -path [файл] -pattern [строка]	<h3>Конвейерная обработка, циклы и переменные</h3> <p>Псевдокод вывода командлета в другой командлет:</p> <pre>PS C:\> Get-Process Format-List -Имя свойства</pre> <p>ForEach-Object в конвейере (псевдонимы!):</p> <pre>PS C:\> ls -l ForEach-Object {cat \$ }</pre> <p>Условие где-объекта (псевдоним где или?):</p> <pre>PS C:\> Get-Process Where-Object { \$ _Name -eq "notepad" }</pre> <p>Генерация диапазонов чисел и циклов:</p> <pre>PS C:\> 1..10 PS C:\> 1..10 % {echo "Привет!"}</pre> <p>Создание и переименование переменных:</p> <pre>\$? = \$total = 42 \$? = переменная !:</pre> <p>Примеры передачи вывода командлета по конвейеру:</p> <pre>PS C:\> ps rex расширение группы Сортировать</pre> <pre>PS C:\> Get-Service dhcp Стом-Сервис -PassThru Set-Service -StartupType отключен</pre>
КОМАНДЛЕТ	ЧТО ЭТО ДЕЛАЕТ?	HANDY ALIAS												
PS C:\> Get-Help [cmdlet]	Показывает помощь и примеры	PS C:\> Помощь [командлет] - Примеры												
- примеры PS C:\> Get-Command PS C:\> ForEach-Object { \$ }	Показывает список команд. Показывает свойства и методы. Принимает каждый элемент в конвейере и обрабатывает его как \$	Get-Command PS C:\> [командлет] gm												
PS C:\> Select-String	Ищет строки в файлах или выходных данных, например, gtr.	PS C:\> sls -path [файл] -pattern [строка]												
<h3>Эффективная PowerShell</h3> <p>ЗАВЕРШЕНИЕ ТАБ:</p> <pre>PS C:\> получить-ребенок <TAB> PS C:\> Get-ChildItem</pre> <p>Сокращение параметра:</p> <pre>PS C:\> ls -Is recursive эквивалентно: PS C:\> ls -Is -r</pre>	<h3>В поисках командлетов</h3> <p>Чтобы получить список всех доступных командлетов:</p> <pre>PS C:\> Get-Command</pre> <p>Get-Command поддерживает фильтрацию. Чтобы отфильтровать команды из набора глаголов:</p> <pre>PS C:\> Get-Command \$verb или PS C:\> Get-Command -Verb Set</pre> <p>Или на существительный "Процесс":</p> <pre>PS C:\> Get-Command "Процесс" или PS C:\> Get-Command -существительный процесс</pre>	<h3>Получать помощь</h3> <p>Чтобы получить помощь с помощью:</p> <pre>PS C:\> Получить помощь</pre> <p>Чтобы просмотреть документацию по командлетам:</p> <pre>PS C:\> Get-Help <cmdlet></pre> <p>Подробная помощь:</p> <pre>PS C:\> Get-Help <cmdlet> -detailed</pre> <p>Примеры использования:</p> <pre>PS C:\> Get-Help <cmdlet> -examples</pre> <p>Полная (все) помощь:</p> <pre>PS C:\> Get-Help <cmdlet> -full</pre> <p>Онлайн-помощь (если есть):</p> <pre>PS C:\> Get-Help <cmdlet> -online</pre>												

METASPLOIT

<h3>Опубликовать модули от Meterpreter</h3> <p>При наличии доступного сванса Meterpreter почтовые модули можно загрузить на целевом компьютере.</p> <p>RUN POST МОДУЛИ ИЗ МЕТЕРПРЕТЕРА</p> <p>измерьте: загрузить, сообщение / модули / собрать / env</p> <p>RUN POST МОДУЛИ НА ФОНОВОЙ СЕССИИ</p> <p>MSF> использовать post / windows / collect / hashdump</p> <p>MSF> показать параметры</p> <p>MSF> установить сессию 1</p> <p>MSF> запустить</p>	<h3>Управление сессиями</h3> <p>МНОГОКРАТНАЯ ЭКСПЛУАТАЦИЯ:</p> <p>Запустите эксплойт, ожидая одну сессию, которая сразу же станет фоновой:</p> <p>MSF> эксплуатировать -x</p> <p>Запустите эксплойт в фоновом режиме, чтобы metasploit можно было использовать во время работы эксплойта:</p> <p>MSF> эксплуатировать -j</p> <p>Перечислите все текущие вакансии (обычно используют слушателей):</p> <p>MSF> работа -i</p> <p>Убить работу:</p> <p>MSF> jobs -k [jobID]</p>	<h3>Metasploit Meterpreter</h3> <p>ОСНОВНЫЕ КОМАНДЫ:</p> <p>/ Помогите: Показать сводку команд</p> <p>выход / выход: Выход из сванса Meterpreter</p> <p>SysInfo: Показать имя системы и тип ОС</p> <p>выполнение / перезагрузка: Self-повторитель</p> <p>КОМАНДЫ ФАЙЛОВОЙ СИСТЕМЫ:</p> <p>команды диск: Изменить каталог</p> <p>ЖК-дисплей: Изменить каталог на локальной (атакующей) машине</p> <p>pwd / getwd: Показать текущий рабочий каталог ls: показать содержимое каталога</p> <p>кошка: Вывести содержимое файла на экран</p> <p>скачать загрузить: Переместить файл в / из целевой машины</p> <p>mkdir / rmdir: Создать / удалить каталог</p> <p>редактировать: Открыть файл в редакторе по умолчанию (обычно vi)</p>
<h3>Полезные вспомогательные модули</h3> <p>СКАНЕР TCP-ПОРТА:</p> <p>MSF> использовать вспомогательный / сканер / portscan / tcp</p> <p>MSF> установить RHOSTS 10.10.10.0/24</p> <p>MSF> запустить</p> <p>DNS ENUMERATION</p> <p>MSF> использовать вспомогательный / собираются / dns_enum</p> <p>MSF> установить DOMAIN target.tgt</p> <p>MSF> запустить</p> <p>FTP СЕРВЕР</p> <p>MSF> использовать вспомогательный / сервер / FTP</p> <p>MSF> установить FTPROOT / tmp / ftproot</p> <p>MSF> запустить</p> <p>ПРОКСИ СЕРВЕР</p> <p>Создайте прокси socks4a на локальном компьютере, который позволяет внешним инструментам использовать маршрутизацию Metasploit.</p> <p>MSF> использовать вспомогательные / сервер / socks4a</p> <p>MSF> запустить</p>	<h3>Основы Metasploit Console (msfconsole)</h3> <p>ПОИСК МОДУЛЯ:</p> <p>MSF> критерий поиска]</p> <p>УКАЗАТЬ ЭКСПЛУАТАЦИЮ ДЛЯ ИСПОЛЬЗОВАНИЯ:</p> <p>MSF> использовать эксплойт / [ExploitPath]</p> <p>УКАЗАТЬ ОПЛАТУ:</p> <p>MSF> установить PAYLOAD [PayloadPath]</p> <p>ПОКАЗАТЬ ВАРИАНТЫ ДЛЯ СОВРЕМЕННЫХ МОДУЛЕЙ:</p> <p>MSF> показать параметры</p> <p>УСТАНОВИТЬ ВАРИАНТЫ:</p> <p>MSF> установить [Option] [Value]</p> <p>НАЧАЛО ЭКСПЛУАТАЦИИ:</p> <p>MSF> эксплуатировать</p>	<p>КОМАНДЫ ПРОЦЕССА:</p> <p>GETPID: Показать идентификатор процесса, внутри которого работает Meterpreter</p> <p>getuid: Показать идентификатор пользователя, с которым работает Meterpreter</p> <p>ps: Показать список процессов</p> <p>убийство: Завершить процесс, учитывая его идентификатор процесса</p> <p>выполнить: Запустить данную программу с привилегиями процесса, в который загрузили Meterpreter</p> <p>мигрировать: Перейти к указанному идентификатору процесса назначения</p> <ul style="list-style-type: none"> - Целевой процесс должен иметь такие же или меньшие привилегии - Целевой процесс должен быть более стабильным - Находиться внутри процесса, можно получить доступ к любым файлам, на который процесс загрузили

RULES OF ENGAGEMENT & SCOPING

Правила участия

- ☐ Контактная информация группы тестирования на проникновение
- ☐ Контактная информация целевой организации Периодичность
- ☐ ежедневного дебринга Время / место ежедневного дебринга
- ☐ Дата начала теста на проникновение Дата окончания теста на проникновение Время, когда проводится тестирование

- ☐ Будет ли объявлен тест для целевого персонала? Будет ли целевая организация изобгать IP-адресов систем атак? Имеет ли сеть целевой организации автоматические возможности сокращения, которые могут нарушить доступ непредвиденными способами (например, создать условие отказа в обслуживании), и если да, какие шаги будут предприняты для снижения риска? Завершит ли тестирование системы атак атаку, и если нет, какие шаги будут предприняты для продолжения, если системы будут изобганы, и какое одобрение (если таковое имеется) потребуется? Каковы IP-адреса систем атак группы тестирования на проникновение? Это тест "черного ящика"? Какова политика в отношении просмотра данных (включая потенциально конфиденциальные / конфиденциальные данные) на скомпрометированных хостах? Будет ли целевой персонал наблюдать за командой тестирования?

Обзорный

☐ Каковы основные проблемы безопасности целевой организации?
(Примеры включают в себя раскрытие конфиденциальной информации, прерывание обработки продукции, смещение из-за порчи сайта и т. Д.)

☐ Какие конкретные хосты, диапазоны сетевых адресов или приложения должны были протестированы? Какие конкретные хосты, диапазоны сетевых адресов или приложения вы НЕ должны тестировать?
 Укажите любые третьи стороны, которым принадлежит системы или сети, входящие в сферу применения, а также системы, которыми они владеют
☐ (письменное разрешение должно быть заранее получено целевой организацией). Будет ли проводиться тестирование в рабочей среде или в тестовой среде?
☐

☐ Какой из следующих методов тестирования будет включать тест на проникновение:

☐ Пинг-размеры сетевых диапазонов?
 ☐ Сканирование портов целевых хостов?
 ☐ Сканирование уязвимостей целев? Проникновение
 ☐ в машины? Манипулирование на уровне
 ☐ приложений? Обратный инжиниринг на стороне
 ☐ клиента? Попытки физического проникновения?
 ☐ Социальная инженерия людей? Другой?
 ☐
☐

☐ Будет ли тест на проникновение включать тестирование внутренней сети?
 ☐ Если да, то как будет получен доступ?

☐ Системы клиента / конечного пользователя включены в область?
 ☐ Если так, сколько клиентских систем будет предназначено?

☐ Разрешена ли социальная инженерия?
 ☐ Если так, как это может использоваться?

☐ Допускаются ли атака типа «колл в обслуживании»?
 ☐ Разрешены ли опасные проверки / эксплуатация?

NMAP

<h3>Базовый синтаксис</h3> <p># nmap [ScanType] [Опции] [Цели]</p> <h3>Целевая спецификация</h3> <p>IPv4-адрес: 192.168.1.1</p> <p>IPv6-адрес: AABB:CCDD::FF%eth0</p> <p>Для хоста: www.target.it</p> <p>Диапазон IP-адресов: 192.168.0.255-0.255</p> <p>Блок CIDR: 192.168.0.0/16</p> <p>Используйте файл со списками целей: -iL «имя файла»</p>	<h3>Типы сканирования</h3> <ul style="list-style-type: none"> - o Только зондирование (обнаружение хоста, а не сканирование портов) - ss SYN Scan - CT TCP Connect Scan - CU UDP Scan - sa Сканирование версий - O Обнаружение ОС - s «ссылка» Установить пользовательский список TCP использовать УРГАКПШЦРЦЮНЧФНЧН в таком порядке 	<h3>Совокупные временные параметры</h3> <ul style="list-style-type: none"> - T8 Паросок: очень медленно, используется для зондирования от IDS - T1 Полно: довольно медленный, используется для уточнения от IDS - T2 Быстрый: замедляет потребление, уменьшает пропускную способность, работает в 10 раз медленнее, чем по умолчанию - T3 Normal: по умолчанию, динамическая модель синхронизации на целевую отзывчивость - T4 Агрессивный: предполагает быстрый и надежный ответ и может сократить цели - T5 Безуныный: очень агрессивный; скорее всего сократит цели или пропустит открытые порты
<h3>Целевые порты</h3> <p>Не указав диапазон портов, который сканирует 1000 самых популярных портов</p> <ul style="list-style-type: none"> - F Сканирование 100 самых популярных портов - p «порт1» - «порт2» Диапазон портов - «порт1», «порт2», ... Список портов - pu: 53, U: 110, T20-445 Смешивая TCP и UDP - p Сканирование линейно (не рандомизировать порты) - -top-ports «n» Сканирование самых популярных портов - p-65535 Если оставить исходный порт, сканирование Nmap начнется с порта 1 - pf Выход из оконечного порта делает сканирование Nmap до порта 65535 - pf Отключение начального и конечного портов делает порты сканирования Nmap 16553-5 	<h3>Мелкозернистые варианты синхронизации</h3> <ul style="list-style-type: none"> - min-hostgroup / max-hostgroup «размер» <p>Размеры группы сканирования параллельного хоста</p> <ul style="list-style-type: none"> - min-parallelism / макс-parallelism «numprobos» <p>Распараллеливание зонда</p> <ul style="list-style-type: none"> - min-rtt-timeout / max-rtt-timeout / i initial-rtt-timeout «время» <p>Определяет время прохождения зонда.</p> <ul style="list-style-type: none"> - max-retries «попытки» <p>Ограничивает количество повторных передач зонда сканирования порта.</p> <ul style="list-style-type: none"> - время ожидания хоста «время» <p>Откажитесь от цели после этого долгого</p> <ul style="list-style-type: none"> - «ограничь сканирование / -максимальная задержка сканирования <p>Формулирует задержку между датчиками</p> <ul style="list-style-type: none"> - минимальная ставка «число» <p>Отправка пакета не медленнее, чем «число» в секунду</p> <ul style="list-style-type: none"> - максимальная скорость «число» <p>Отправлять пакеты не быстрее, чем «число» в секунду</p>	<h3>Скриптовые движок</h3> <ul style="list-style-type: none"> - «ScriptName» «ScriptCategory» - «ScriptName» <p>Запустить скрипты по умолчанию</p> <p>Запустить отдельные или группы скриптов</p> <ul style="list-style-type: none"> - script-args = <Name1 = Value1, ...> <p>Использовать список аргументов скрипта</p> <ul style="list-style-type: none"> - script-updatedb <p>Обновить базу данных скриптов</p>
<h3>Опции зондирования</h3> <ul style="list-style-type: none"> - pi Не проверять (предполагая, что все хосты работают) - PB Зонд по умолчанию (TCP 80, 445 и ICMP) - PS «portlist» <p>Проберит, работает ли цели, проверяя порты TCP</p> <ul style="list-style-type: none"> - CP Использовать ICMP Echo Request - PI Использовать запрос временной метки ICMP - WEIPA Использовать запрос массы метки ICMP 		<h3>Выходные форматы</h3> <ul style="list-style-type: none"> - ON Стандартный вывод Nmap - OG Greppable формат - ox Формат XML - oA «базовое имя» <p>Генерация выходных файлов</p> <p>Норм, Greppable и XML, с использованием базового имени для файлов</p> <h3>Разные варианты</h3> <ul style="list-style-type: none"> - и Отключить обратный поиск IP-адреса - WИспользуйте только - A Используйте несколько функций, включая обнаружение ОС, обнаружение версий, сканирование скриптов (по умолчанию) и трассировку - «причина» Причина отклонения Nmap считает порт открытым, закрытым или тайм-аутным

SCAPY

<h3>Основа Scapy</h3> <p>Для просмотра списка поддерживаемых протоколов:</p> <pre>>>> ls ()</pre> <p>Некоторые ключевые слова:</p> <pre>arg, ip, ipv6, tcp, udp, icmp</pre> <p>Для просмотра полезной связи используйте ls (layer):</p> <pre>>>> ls (IPv6) >>> ls (TCP)</pre> <p>Для просмотра списка доступных команд:</p> <pre>>>> lsc ()</pre> <p>Некоторые ключевые команды для взаимодействия с пакетами:</p> <pre>rdpcap, отправить, sr, sniff, wrpcap</pre> <p>Чтобы получить справку по командам, используйте help (смажьте):</p> <pre>>>> помощь (rdpcap)</pre>	<h3>Базовая обработка пакетов / просмотры</h3> <p>Scapy работает со словами. Слово - это отдельные функции, связанные вместе с символом ":" для создания пакетов. Это создает базовый пакет TCP / IP с "стандартными" в качестве полезной нагрузки:</p> <pre>>>> пакет = IP (dst = "1.2.3.4") / TCP (dport = 22) данные</pre> <p>Примечание: Scapy позволяет пользователю полностью перейти на уровень ether () (Data Link), но будет использовать значения по умолчанию для уровня link data, если он не используется при использовании функций send () или sr (). Чтобы правильно передать трафик, слои должны быть упорядочены по убыванию слева направо (например, ether -> IP -> TCP). Чтобы получить версию пакета:</p> <pre>>>> packet.summary ()</pre> <p>Чтобы получить больше деталей пакета:</p> <pre>>>> packet.show ()</pre>	<h3>Получение и анализ пакетов</h3> <p>Полученные пакеты могут быть сохранены в переменную при использовании функции отправки / получения, такой как sr (), sr3 (), sr1 () и sr1p ().</p> <pre>>>> пакет = IP (dst = "10.10.10.20") / TCP (dport = 0, 1024)</pre> <pre>>>> unans, ans = sr (накет)</pre> <p>Получено 1086 пакетов, получено 1024 ответа, остальные 0 пакетов «ans» будут хранить ответные пакеты:</p> <pre>>>> ans <Результаты: TCP: 1024 UDP: 0 ICMP: 0 Другое: 0></pre> <p>Чтобы увидеть резюме ответов:</p> <pre>>>> ans.summary () IP / TCP [0.1.1.15:ftp, data] 10.10.10.20.netbios_ssn S => IP / TCP 10.10.10.20.netbios_ssn> 10.1.1.15.ftp_data SA / Padding</pre> <p>Примечание: это выход из порта 139 (netbios_ssn). Обратите внимание, как этот порт был открыт и ответил SYN-ACK. Чтобы просмотреть конкретную пару отправленных / ответных пакетов:</p> <pre>>>> ans [15]</pre> <p>Чтобы просмотреть первый пакет в потоке:</p> <pre>>>> ans [15] [0] (это будет пакет, отправленный Scapy)</pre> <pre><IP frag = 0 proto = tcp dst = 10.10.10.20 <TCP dport = netstat flags = S IP frag =</pre>
<h3>Нюхает и pcap</h3> <p>Чтобы прослушать, используйте Berkeley Packet Filter:</p> <pre>>>> пакеты = sniff (фильтр = "хост 1.1.1.1")</pre> <p>Синнифф по счетам:</p> <pre>>>> пакеты = sniff (количество = 100)</pre> <p>Чтение пакетов из pcap:</p> <pre>>>> packages = rdpcap ("filename.pcap")</pre> <p>Записи пакетов в pcap:</p> <pre>>>> wrpcap ("filename.pcap", пакеты)</pre>	<h3>Отправка пакетов</h3> <h4>СОЗДАНИЕ И ОТПРАВКА ПАКЕТА</h4> <pre>>>> пакет = IP (dst = "4.5.6.7") / TCP (dport = 80, флаги = "S")</pre> <p>Отправить пакет или список пакетов без пользовательского уровня эфира:</p> <pre>>>> отправить (пакет)</pre> <h4>ОТПРАВИТЬ ФУНКЦИОНАЛЬНЫЕ ВАРИАНТЫ</h4> <p>«Berkley Packet Filter» rpsrv = количество повторных попыток для неуставных пакетов» timeout = «количество секунд ожидания до отказа» iface = «интерфейс для отправки и получения»</p> <pre>>>> rpacket = sr (packet, retry = 5, timeout = 1.5, iface = "eth0", filter = "хост")</pre> <p>1.2.3.4 и порт 80 ")</p>	<p>Чтобы просмотреть первый пакет в потоке:</p> <pre>>>> ans [15] [0] (это будет пакет, отправленный Scapy)</pre> <pre><IP frag = 0 proto = tcp dst = 10.10.10.20 <TCP dport = netstat flags = S IP frag =</pre> <p>Чтобы просмотреть ответ от дальнего хоста:</p> <pre>>>> ans [15] [1] <Версия IP = 4L ihl = 5L tos = 0x0 len = 40 id = 16355 flags = DF frag = 0L ihl = 128 proto = tcp checksum = 0x368c src = 10.10.10.20 dst = 10.1.1.15 options = [] <TCP sport = netstat dport = ftp data seq = 0 ack = 1 dataofs = 5L зарезервировано = 0L флаги = RA window = 0 checksum = 0x2b4c urgptr = 0 <Загрузка заполнения = "\ x00 \ x00 \ x00 \ x00 \ x00" > >>></pre> <p>Чтобы просмотреть флаги TCP в ответном пакете:</p> <pre>>>> ans [15] [1].sprint ("% TCP.flags %") 'RA'</pre>

SLINGSHOT LINUX DISTRIBUTION

Дистрибуция Slingshot Linux используется для различных курсов SANS Penetration Testing.

Инструментальный арсенал Slingshot был тщательно протестирован, чтобы обеспечить отличные результаты в курсовых лабораториях и в проектах тестирования на проникновение.

Slingshot включает в себя следующие инструменты:

• METASPLOIT FRAMEWORK GUI	• LAIR FRAMEWORK ИНСТРУМЕНТ ДЛЯ СОТРУДНИЧЕСТВА PEN TEST ОБЩАЯ ЦЕЛЬ	• СОЦИАЛЬНЫЙ ИНЖИНИРИНГ ИНСТРУМЕНТ
• ETTERCAP MAN В СРЕДНЕМ ИНСТРУМЕНТЕ EXIFTOOL ДЛЯ АНАЛИЗА METADATA HYDRA PASSWORD ИНСТРУМЕНТ ДЛЯ УДАЛЕНИЯ ПАРОЛЯ ДЖОНА RIPPER	• ИНСТРУМЕНТ TCP / UDP NESSUS СКАНЕР УНИВЕРСАЛЬНОСТИ НИКТО WEB-СКАНЕР NMAP PORT СКАНЕР И ОБЩЕГО НАЗНАЧЕНИЯ ПАКЕТ ИНСТРУМЕНТ RECON-NG	• TCPDUMP СНИФЕР СНИФЕР СНИФЕР
• PASSWORD	• RECONNAISSANCE ПАКЕТ ПАКЕТА	• VILIX-EVASION АНТИВИРУС ЭВАЗИОННЫЙ ИНСТРУМЕНТ POWERSHELL EMPIRE
•	•	• POST-EXPLOITATION TOOLKIT ZED ATTACK PROXY (ZAP) WEB-ПРИЛОЖЕНИЕ АТТАК
		• ИНСТРУМЕНТ