Отчет о проведении анализа защищенности ресурса Metasploitable2

Оглавление

1. Введение

Цель данного анализа - симуляция атаки потенциального злоумышленника на ресурс metasplotable2, оценка уровня его защищенности, обнаружение уязвимостей, анализ и разработка рекомендаций по их устранению.

1.2 Объект тестирования

В процесс тестирования не включены активные атаки на отказ в

обслуживании, статический анализ кода, стресс тестирование и социальная инженерия. Оценка серверного программного обеспечения и конфигурации также находится вне данного проекта. Объектом тестирования является сетевой узер metasploitable2, ip-адрес — 192.168.56.12.

1.3 Основная классификация

Каждой уязвимости, обнаруженной в ходе проведения тестирования, присваивается определенная степень риска. Критерии данной классификации указаны ниже.

Высокий
Уязвимости присваивается высокая степень риска, если ее использование может привести к компрометации данных, доступности сервера или сервисов, выполнению произвольного кода, манипуляции с данными. Сюда же входят уязвимости связанные с отказом в обслуживании, слабые или стандартные пароли, отсутствие шифрования, доступ к произвольным файлам или конфиденциальных данных
Средний
Уязвимость средней степени риска не приводит напрямую к компрометации или неавторизованному доступу, но предоставляют возможность или информацию, которая может быть использована потенциальным злоумышленником для дальнейшего использования в совокупности с другими уязвимостями для компрометации ресурса. Например незащищенный доступ к некритичным файлам, листинг некритичных директорий, раскрытие полных путей.
Низкий
Все остальные уязвимости, которые не могут привести к компрометации ресурса, но которые могут быть использованы потенциальным злоумышленником, для сбора информации, формировании векторов атаки и т.д.

2. Обзорный отчет

2.1 Общая оценка уровня защищенности

В результате проведенного тестирования сетевой узел metasploitable2 оценивается как высоко критичное, так как были обнаружены несколько уязвимостей высокой степени риска, позволяющие получить удаленный доступ к серверу и конфиденциальным данным.

2.2 Уязвимости по уровню риска

Степень риска	Количество	Описание
Высокая	1	Данные уязвимости оцениваются как высокие и несут наибольшую угрозу. Их эксплуатация может привести к получению удаленного доступа,

		выполнения произвольного кода злоумышленником, раскрытие конфиденциальной информации.
Средняя	1	Уязвимости имеют ограниченное воздействие, однако могут быть использованы для получения чувствительной информации и в совокупности с другими уязвимостями позволят получить удаленный доступ.
Низкая	1	Не несут реальной угрозы, но могут быть использованы для сбора информации, формировании и развитии векторов атаки.

2.3 Уязвимости по классификации

Для описания степени риска и оценки критичности обнаруженных уязвимостей используются классификации “The Common Vulnerability Scoring System (CVSSv2)”, MITRE (CAPEC) и OWASP.

Тип	Количество	Степень риска
Brute force attacks	1	**Высокая**
General	2	**Средняя, Низкая**

3. Отчет по уязвимостям

3.1 Уязвимости по типу

Имя	**Краткое описание**	**Воздейст-вие (CVSS)**	**Ссылки на классификацию и описание**	**ID уязвимости**
SSH Brute Force Logins With Default Credentials	Для входа в систему по протоколу SSH используется ряд известных учетных данных по умолчанию.	**7.5**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108013	1.3.6.1.4.1.25623.1.0.108013
SSH Weak Encryption Algorithms Supported	Удаленный сервер SSH настроен на использование слабых алгоритмов шифрования.	**4.3**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105611	1.3.6.1.4.1.25623.1.0.105611
SSH Weak	Удаленный SSH-	**2.6**	http://www.securityspac	1.3.6.1.4.1.25623.

MAC Algorithms Supported	сервер настроен на использование слабых алгоритмов MD5 и / или 96-битных MAC.		e.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.105610	1.0.105610

3.2 Подтверждение наличия уязвимостей

Удалось получить удаленный доступ к сервер по протоколу SSH с помощью учетных записей (Логин:Пароль):

- msfadmin:msfadmin
- postgres:postgres
- service:service
- user:user

4. План по устранению

Уязвимость	Риск	Рекомендации
SSH Brute Force Logins With Default Credentials	Получение доступа к серверу дает злоумышленнику возможность выполнения произвольных скриптов. Есть риск повышения привилегий и вызова отказа в обслуживании (например, переполнение диска).	Следует сменить пароли стандартных учетных записей. Если учетной записине требуется удаленный доступ, следует ограничить возможность подключения. Для защиты от перебора паролей рекомендуется установить fail2ban (https://help.ubuntu.ru/wiki/fail2ban)
SSH Weak Encryption Algorithms Supported	может позволить злоумышленнику восстановить открытый текст из блока зашифрованного текста	Рекомендуется отключить нестойкие алгоритмы. Рекомендации по использованию криптоалгоритмов (https://www.ssh.com/ssh/sshd_config/)
SSH Weak MAC Algorithms Supported	Низкая вероятность эксплуатации	

5. Журнал

- Дата тестирования: 25.04.2020
- Объект тестирования: Metasploitable2 (192.168.56.12)

- Метод тестирования: Black box
- Используемое ПО: OpenVAS
- Исполнитель: melnikov

6. Вывод

Данный анализ базируется на технологиях и известных уязвимостях на момент проведения тестирования. Мы советуем следовать рекомендациям указанным в настоящем отчете в порядке и степени критичности уязвимостей.

В заключение хотим добавить, что ресурс metasploitable2 подвержен высокой степени риска, что может привести как финансовым так и репутационным тратам. Мероприятия по устранению не следует откладывать.

Также мы крайне рекомендуем провести повторное тестирование сайта, после проведения указанных выше мероприятий. Тем самым вы сможете убедиться, что ваш ресурс более не подвержен подобным рискам, мероприятия выполнены верно.