Отчет о проведении анализа защищенности веб ресурса Metasploitable2

Оглавление

1. Введение

Цель данного анализа - симуляция атаки потенциального злоумышленника на веб 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 веб ресурс metasploitable2 http://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
Remote file access	1	**Высокая**
Web application abuses	11	**Высокая** **Средняя**
Web Servers	1	**Средняя**

3. Отчет по уязвимостям

3.1 Уязвимости по типу

Имя	Краткое описание	Воздейст-вие (CVSS)	Ссылки на классификацию и описание	ID уязвимости
Test HTTP dangerous methods	Неправильная настройка веб-сервера позволяет удаленным клиентам выполнять опасные HTTP-запросы, такие как PUT и DELETE.	**7.5**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10498	1.3.6.1.4.1.25623.1.0.10498
TWiki XSS and Command Execution Vulnerabilities	Хост работает под управлением TWiki и подвержен к межсайтовому скриптингу (XSS) и уязвимости выполнения произвольных команд.	**10.0**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.800320	1.3.6.1.4.1.25623.1.0.800320
PHP-CGI-based setups vulnerability when parsing query string parameters from php files	Мод CGI подвержен уязвимости раскрытия информации. Может быть использован для получения исходного кода и выполнения произвольного кода	**7.5**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.103482	1.3.6.1.4.1.25623.1.0.103482
phpinfo() output Detection	Обнаружена отладочная утилита phpinfo()	**7.5**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108474	1.3.6.1.4.1.25623.1.0.108474

The /doc directory is browsable	Дает доступ к /usr/doc/, позволяется просмотреть установленные пакеты и их версии.	**5.0**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.10056	1.3.6.1.4.1.25623.1.0.10056
Cleartext Transmission of Sensitive Information via HTTP	Сайт передает конфиденциальную информацию (имя пользователя, пароли) в открытом виде.	**4.8**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108440	1.3.6.1.4.1.25623.1.0.108440
TWiki < 6.1.0 XSS Vulnerability	Версия Twiki позволяет осуществить XSS.	**4.3**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.141830	1.3.6.1.4.1.25623.1.0.141830
TWiki Cross-Site Request Forgery Vulnerability	Хост работает под управлением TWiki и подвержен XSS	**6.0**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.800400	1.3.6.1.4.1.25623.1.0.800400
TWiki Cross-Site Request Forgery Vulnerability - Sep10		**6.8**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.801281	1.3.6.1.4.1.25623.1.0.801281
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	Версия Apache позволяет злоумышленнику получить доступ к Cookie	**4.3**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.902830	1.3.6.1.4.1.25623.1.0.902830
HTTP Debugging Methods (TRACE/TRACK) Enabled	На сервере включены функции отладки	**5.8**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.11213	1.3.6.1.4.1.25623.1.0.11213
phpMyAdmin 'error.php' Cross Site Scripting	На сервере работает версия phpMyAdmin подверженная	**4.3**	http://www.securityspace.com/smysecure/catid.html?	1.3.6.1.4.1.25623.1.0.801660

Vulnerability	XSS		id=1.3.6.1.4.1.25623.1.0.801660	
awiki Multiple Local File Include Vulnerabilities	Уязвимость реализуется через форму загрузки файлов на сайт	**5.0**	http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.103210	1.3.6.1.4.1.25623.1.0.103210

4. Журнал

- Дата тестирования: 17.04.2020
- Объект тестирования: веб-сайт (http://192.168.56.12/)
- Метод тестирования: Black box
- Используемое ПО: OpenVAS
- Исполнитель: feshchenkod

5. 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 веб-ресурс 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.