АНАЛИЗ ЗАЩИЩЕННОСТИ СЕГМЕНТА СЕТИ НА ОСНОВЕ СКАНЕРОВ ЗАЩИЩЕННОСТИ

Р. И. Поляков

Белорусский государственный университет, г. Минск;
raman.paliakou@gmail.com
науч. рук. – Г. К. Резников, канд. техн. наук, доцент

На текущий момент мировая статистика свидетельствует о значительном ежегодном росте количества сетевых атак, в связи с чем актуальным является исследование сети сканерами защищенности с целью выявления уязвимостей и предотвращения их эксплуатации, а также определения функциональности сетевого сканера как инструмента адаптивной безопасности сети. Достаточное количество свободно распространяемых сетевых сканеров также указывает на возможность их использования при атаке на целевую сеть, в связи с чем сравнительный анализ такого программного обеспечения также является актуальным. В работе исследовано 8 сетевых сканеров последних версий – «LanSpy 2.0», «Xscan v3.3», «Superscan 4.1», «Network Scanner», «NMap», «LanState Pro», «10-Страйк Сканирование Сети», «Nessus», проведен анализ быстродействия, информативности, функциональности и оптимизированности отчетной информации к дальнейшему использованию, пригодности сканера к построению карты исследуемой сети. Сканеры тестировались на операционных системах семейств Windows, Linux, Linux Server, а также на работающем сетевом окружении с количеством компьютеров более 100. Приведены и классифицированы по степени важности обнаруженные уязвимости, предложены действующие способы их закрытия, также приведены наиболее уязвимые к сетевым атакам порты TCP и UDP, для каждого сканера определен наиболее подходящий сценарий использования, а также оптимальные параметры.

Ключевые слова: сетевой сканер; адаптивная безопасность сети; сетевой порт; уязвимость; сетевая атака; способы закрытия уязвимостей.

МЕХАНИЗМЫ РАБОТЫ СЕТЕВОГО СКАНЕРА

Известные на данный момент сетевые сканеры работают на 3 (сетевом) и 4 (транспортном) уровне сети, согласно модели OSI/ISO. Сканирование осуществляется с использованием протоколов TCP, UDP, ICMP, ARP, SNMP. Цель любой подобной проверки – выявить открытые TCP/UDP порты, обнаружить сервисы, ответственные за открытое состояние порта, и собрать всю доступную информацию о хосте. Обычно в нее входит: пинг, доменное имя, netbios -имена, mac -адрес, информация о сервере, информация о домене и рабочей группе, контроллеры домена, подключённые пользователи, глобальные группы, локальные группы, настройки безопасности, разделяемые ресурсы, сессии, сервисы, процессы, данные о реестре, журнал событий, сетевая статистика и др.

Существует множество типов выполняемых сканерами проверок. Самые основные -TCP connect scan, TCP SYN scan, TCP FIN scan, TCP Xmas Tree scan, TCP Null scan, UDP scan, ACK scanning, ICMP scan, Idle scan, Proxy scan, ARP (mac for IP) scan. Простейшая из них – TCP connect scan – выполняется как стандартное трехэтапное рукопожатие через обмен пакетами с битами SYN, SYN+ACK, ACK и последующим разрывом соединения во избежание атаки типа DDOS. Данный тип проверок имеет низкую скорость, и является легко обнаружимым, поэтому хоть он и является поддерживаемым современными сканерами, большинство из них в качестве стандарта используют более быстрое сканирование TCP SYN Scan, при котором сетевой сканер непосредственно генерирует пакеты SYN+Port и делает вывод об открытом порте на основании ответа SYN/ACK. В тех же случаях, когда подобный тип сканирования невозможен ввиду блокировок, используется ACK Scanning и TCP FIN Scan, а также другие типы проверок.

АНАЛИЗ ИССЛЕДУЕМЫХ ПРОГРАММ

В исследовании требовалось определить характеристики исследуемых сканеров, для чего было создано виртуальное локальное окружение на операционных системах семейств Windows, Linux (Ubuntu, Debian), Linux Server (Ubuntu). Ниже приведена сравнительная таблица результатов сетевого сканера для исследуемых конфигураций сканирования тестируемых программ. Сканер «LanState» работает в связке со сканером «10-Страйк Сканирование Сети», ввиду чего не имеет отдельного столбца. Также следует уточнить указанные конфигурации:

- Superscan Fast: Scan Speed Delay = 10 ms; TCP: port scan timeout = 4000, mode = SYN; UDP: port scan timeout =2000, mode = Data+ ICMP; Ports list: standart
- Superscan Intense: Scan Speed Delay = 20 ms; TCP: port scan timeout = 4000, mode = connect; UDP: port scan timeout = 4000, mode = Data+ ICMP. Ports list: 1-65535 both for TCP and UDP.

По итогам сканирования самыми результативными можно считать «Nessus», «Superscan» в конфигурации Fast и «X-Scan». В случае, если требуется детальное сканирование какого-либо хоста, его можно провести с помощью «Nessu»s, либо «Nmap» в конфигурации Intense + UDP. Несмотря на средние результаты, сканер «LanSpy» может рекомендоваться для получения наиболее подробных сведений о сети за оптимальное время, т.к. собирает большое количество дополнительной информации. Рекомендуется использовать его на небольшом размере окружения.

Таблица

Результаты сканирования открытых TCP/UDP портов

ОС	LanSpy	X-Scan	Superscan Standart	Superscan Fast	Superscan Intense	Nmap Intense	Nmap Quick	Nmap Regular	Nmap Int. + UDP	Nessus	10-Страйк Сканир.С.
Win 8	3 / 0	3 / 0	0 / 1	7 / 79	7 / 835	6 / 0	6 / 0	6 / 0	6 / 1	7 / 35	4 / 1
Win 7	6 / 0	6 / 0	0 / 1	9 / 79	9 / 20519	1 / 0	1 / 0	1 / 0	6 / 16	9 / 42	6 / 16
Deb.Slacko	0 / 14	0 / 14	0 / 0	0 / 74	0 / 74	0 / 0	0 / 0	0 / 0	0 / 19	0 / 47	0 / 19
Win XP	3 / 7	3 / 7	0 / 0	4 / 0	4 / 1	3 / 0	3 / 0	3 / 0	3 / 7	4 / 7	3 / 7
Ubun. Server	0 / 14	0 / 14	0 / 0	0 / 74	0 / 74	0 / 0	0 / 0	0 / 0	0 / 3	0 / 62	0 / 3
Ubun. Desk.	0 / 13	0 / 13	0 / 0	0 / 74	0 / 74	0 / 0	0 / 0	0 / 0	0 / 1	0 / 62	0 / 1
Время, с	320	49	51	105	30600	178	1	1	7688	130	250

При тестировании сканеров в корпоративной сети была проверена функция сетевого картографирования, см рис. 1.

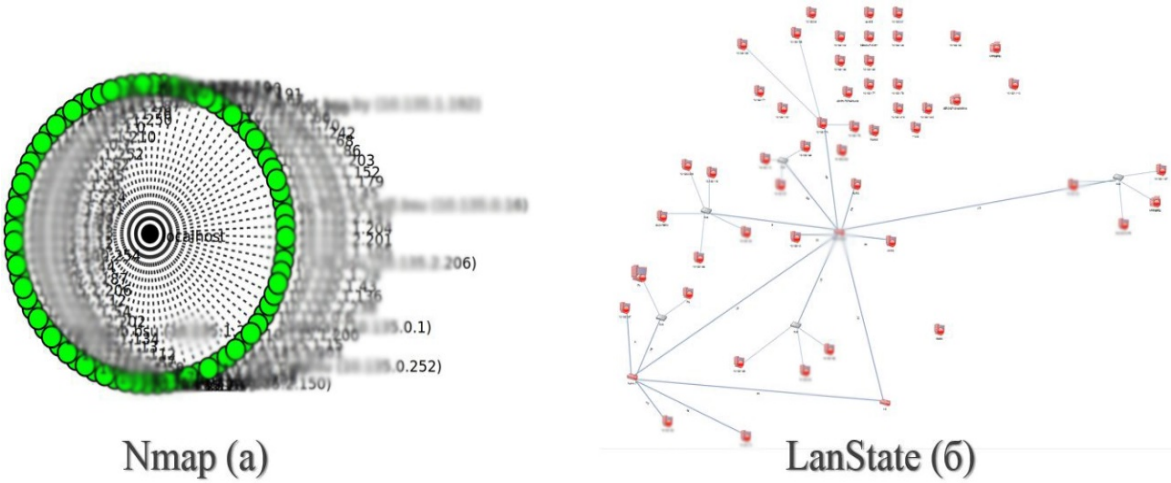

Рис. 1. Результаты построения карты сети для корпоративной сети сканерами Nmap (а) и LanState (б). Для сохранения конфиденциальности часть информации заретуширована

Рекомендуется использовать сканер «LanState» с дополнительным импортом информации из сканера «10-Страйк Сканирование Сети» ввиду возможности получить информацию о таблицах маршрутизации с обнаруженных маршрутизаторов.

УЯЗВИМОСТИ

В результате исследования корпоративной сети можно сделать вывод о наличии в среднестатистической локальной сети некоторых уязвимостей, эксплуатация которых может привести к утечке данных, заражению компьютеров внутри сетевого окружения, удаленному выполнению кода, перехвату почтового трафика, Man-In-The-Middle – атакам на информацию в сети. Обнаруженные уязвимости были классифицированы по международным базам данных CVE [1] и Microsoft, в результате чего можно говорить о следующих уязвимостях: MS17-010, CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148, MS11-030, MS14-066, MS12-020 CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276, CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279, MS09-001 и др. Наиболее распространены MS11-030, MS12-020, MS17-010.Большинство из найденных уязвимостей может быть эксплуатировано через 445 TCP, 3389 TCP, 161 UDP порты.

Рекомендациями по закрытию большинства обнаруженных уязвимостей может служить установка обновлений от компании Microsoft, отключение SNMP-службы в маршрутизаторах, включение принудительной цифровой подписи в политике Microsoft network server, а также использование криптографического протокола SSL при работе с Remote Desktop Protocol Server.

ВЫВОДЫ

В работе проведено исследование механизмов работы сетевых сканеров, их функциональности, скорости, применимости к сетевому картографированию. Изучены особенности работы сканеров в условиях реального и виртуального сетевого окружения на различных операционных системах, определены наиболее опасные и распространенные уязвимости в локальных сетях, указаны порты, через которые возможна их эксплуатация, а также предложены рекомендации по их закрытию.

Библиографические ссылки

1. Международная база уязвимостей CVE. [Электрон. ресурс] / URL: https://cve.mitre.org/ – Дата доступа: 01.05.2018 г.