УДК 621.311

СЕТЕВАЯ РАЗВЕДКА

Гущин Р.А., Колос К.А.
Научный руководитель – Белова С.В.

При обсуждении проблем сетевой безопасности часто используются термины, изначально применяемые в военной области, например, «атака», «нападение», «защита», «разведка».

Большинство атак на транспортную инфраструктуру сети требуют предварительных знаний об атакуемой сети и составляющих ее хостах. Поэтому, как и в военном деле, при попытке нарушения информационной безопасности перед атакой проводится сетевая разведка, в ходе которой злоумышленник пытается собрать необходимые для атаки сведения. В зависимости от типов атак набор сведений может меняться. Чаще всего для проведения атаки необходимы такие данные, как IP-адреса активных хостов, номера активных TCP/UDP-портов, типы и версии операционной системы и приложений. Из этого следует, что сетевая разведка – это комплекс мероприятий по получению и обработке данных об информационной системе клиента, ресурсах, средствах защиты, используемых устройствах, программном обеспечении и их уязвимостях.

Рассмотрим этапы, которые проходят злоумышленники для получения несанкционированного доступа. Первым является выбор сети, сервера или информационного пространства. Затем проводится сканирование, тестирование и сбор информации о цели. Следующим шагом является обработка полученной информации и выбор уязвимого места для проникновения в систему. За этим следует эксплуатация уязвимости и проникновение в систему, дальнейшие же действия зависят исключительно от поставленной злоумышленником задачи. Этой задачей может быть изменение информации, кража, повышение полномочий или удержание системы.

Для сетевой разведки возможны следующие пути получения данных:

1) сканирование сети;
2) сканирование портов;
3) получение информации от whois-серверов;
4) просмотр информации DNS-серверов исследуемой сети для выявления записей, определяющих маршруты электронной почты.

Наибольший интерес представляют первые два пункта. Под сканированием сети понимают получение IP-адресов активных хостов сети. Под сканированием портов – получение активных и пассивных портов. Существуют различные приемы сканирования сети, такие как пинг TCP SYN, TCP ACK, UDP, ICMP, IP. Похожие методы применяются и для сканирования портов.

Очень вероятно, что средства протоколирования событий ОС и межсетевых экранов зафиксируют процесс сканирования, а администратор сканируемой сети начнёт расследовать инцидент. Тут же возникает вопрос: с какого адреса выполнялось сканирование? Чтобы избежать раскрытия, злоумышленники часто используют спуфинг IP-адреса при атаках. Он возможен и при сканировании. Самый распространённый приём – маскировка IP-адреса среди множества других. В таком случае тестовые сканирующие пакеты будут отправлены с действительного IP-адреса наряду с множеством таких же пакетов, но с поддельными адресами. Это делается с расчётом на то, что при расследовании трудно будет установить, кто являлся истинным организатором сканирования, а кого просто использовали в качестве прикрытия. Ещё более изощрённым способом является так называемое пустое сканирование. При нём истинный адрес никогда не указывается, а результаты оцениваются злоумышленниками по реакции третьего компьютера, чей адрес подделывается.

Полностью избавиться от сетевой разведки невозможно. Если отключить эхо-запрос ICMP и эхо-ответ на периферийных маршрутизаторах, можно избавиться от эхо-тестирования, но при этом теряются данные, необходимые для диагностики сетевых сбоев. Сканировать порты можно без предварительного эхо-тестирования, но это займёт больше времени, так как придётся сканировать и несуществующие IP-адреса. Системы IDS на уровне сети и хостов обычно справляются с задачей уведомления администратора о ведущейся сетевой разведке, что позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера.

Таким образом, сетевая разведка является важным инструментом злоумышленников при организации атак. В целях предотвращения успешной сетевой разведки необходимо изучение различных приемов сканирования и организация мероприятий по технической защите информационных ресурсов.

Литература

1. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е издание / В. Олифер, Н. Олифер. – СПб.: Питер, 2016. – 992 с.

2. Википедия – Свободная энциклопедия [Электронный ресурс] / Сетевая разведка. – Режим доступа: https://ru.wikipedia.org/wiki/ Сетевая разведка, свободный. – Загл. с экрана. – Яз. рус.

3. Безопасник [Электронный ресурс] / Сетевая разведка. Режим доступа: http://bezopasnik.org/article/111.htm, свободный. – Загл. с экрана. – Яз. рус.