УДК 621.372

АНАЛИТИЧЕСКИЕ ВЕРОЯТНОСТНЫЕ МОДЕЛИ РЕАЛИЗАЦИИ АТАК НА DNS - СЕРВЕРЫ

Е.Е. Смолькина, А.Г. Остапенко, Н.И. Баранников, И.Л. Батаронов

В работе рассматриваются риск-модели атак типа «DNS Amplification» на основе аппарата сетей Петри-Маркова. Приводятся сравнительные характеристики вероятности реализации рассматриваемой атаки от времени, количества инфицированных хостов и различных типов компьютеров

Ключевые слова: сеть Петри-Маркова, вероятность, DNS – атаки, пуассоновский поток

Рассматривая атаки на DNS-сервера [1-5] как пуассоновский поток реализации угроз в компьютерных системах, можно смоделировать рассматриваемые процессы с использованием аппарата сетей Петри-Маркова [3]. Особенность такой сети, отличающая ее от обычной сети Петри, заключается в том, что каждый переход срабатывает только с определенной вероятностью. При этом наиболее часто имеет место одно из двух логических условий: условие "И" и условие "ИЛИ" [1,3].

На рис. 1 представлена классификация разновидностей атак на DNS-серверы. В [1] рассматриваются процессы внедрения ложного DNS – сервера (DNS-атаки первой категории). В настоящей работе рассмотрению подлежат атаки типа «DNS Amplification»

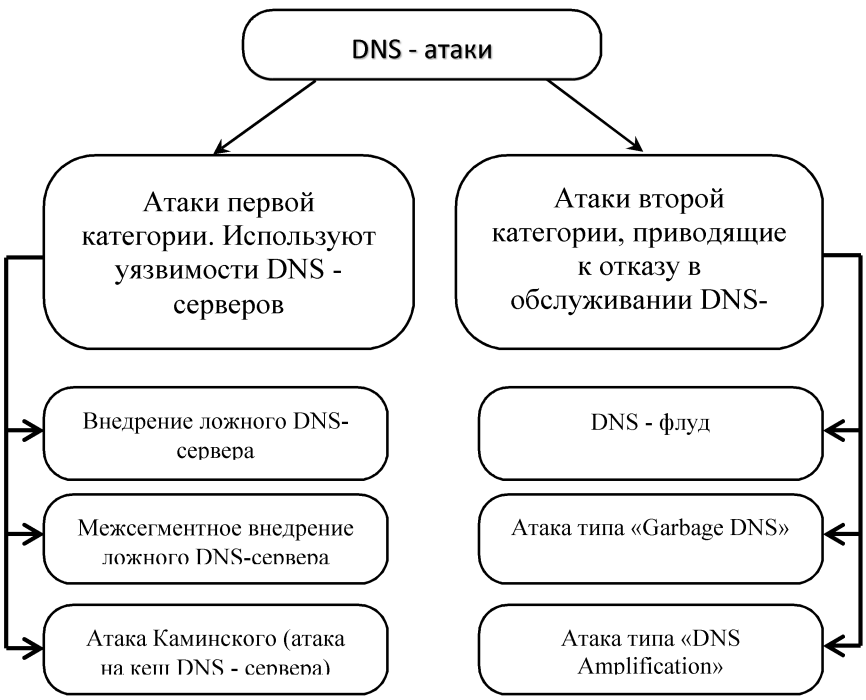

Рис. 1. Классификация DNS-атак

Смолькина Екатерина Евгеньевна – ВГТУ, студент, e-mail: mnac@comch.ru
Остапенко Александр Григорьевич – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru
Баранников Николай Ильич – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru
Батаронов Игорь Леондович – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru

Построим модель атаки типа «DNS Amplification», учитывая, что злоумышленник уже имеет достаточное количество инфицированных компьютеров.

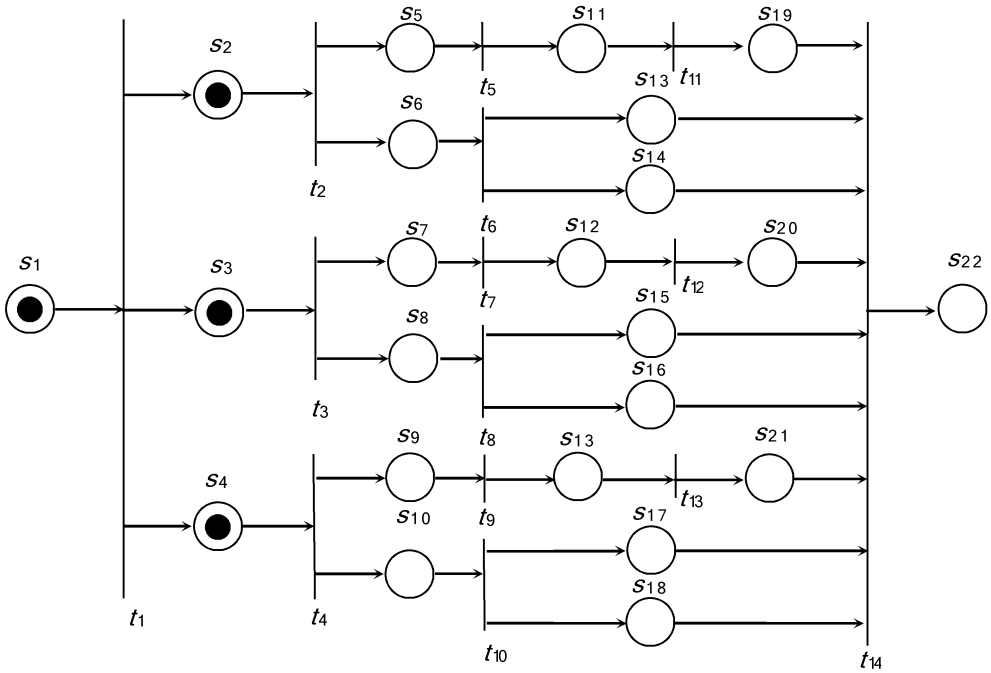

Рис.2. Вид сети Петри-Маркова процесса реализации атаки типа «DNS Amplification»

Сеть Петри-Маркова, изображенная на рис.2, отражает суть атаки типа «DNS Amplification». Чтобы рассчитать зависимость вероятности реализации атаки от времени, разобьем эту сеть на 2 типовых случая реализации атаки. Первый подразумевает атаку без усиления, т.е. DNS-сервер не обрабатывает рекурсивные запросы (атака посредством отраженных DNS-запросов). Второй – это атака с усилением, т.е. с помощью рекурсивных DNS-запросов.

Моделирование атаки типа «DNS Amplification» без усиления (DNS – сервера не обрабатывают рекурсивные запросы)

Рассмотрим принцип атаки без использования «плеча». Получив команду от злоумышленника на атаку определенного хоста, инфицированный компьютер рассылает DNS-запросы по имеющемуся у него списку серверов DNS, подменяя свой IP-адрес на IP-адрес атакуемого хоста. В свою очередь, серверы DNS отправляют свои ответы атакуемому хосту, заполняя его канал UDP-пакетами. Простейший ответ DNS SERVFAIL, отправляемый на запрос чужой зоны, обеспечит UDP Flood канала жертвы. Коэффициента усиления в этом случае не будет (60 байт запрос — 60 байт ответ). Таким образом, благодаря этому факту и использованию UDP-протокола, стала возможна следующая схема атаки на произвольный хост в Интернете:

s_1 —атакующий готов,

t_1 — отправление команды на начало атаки определенного хоста,

s_2 — компьютер находится под удаленным управлением злоумышленника («компьютер-зомби»), ожидает команды на атаку,

s_3 — «компьютер-зомби» получил команду и начал рассылку DNS-запросов,

t_2 — отправление DNS-запросов по имеющимся адресам, подменяя сой IP-адрес на IP-адрес жертвы,

s_4 — большое количество DNS-серверов обрабатывает запрос и отправляют ошибку, так как не являются авторитативными для запрашиваемой зоны,

s_5 — большое количество DNS-серверов обрабатывают запрос и отправляют реальный IP-адрес,

t_3 — отправление ответа компьютеру-

жертве,

s_6 — приём огромного количества ответов (UDP-пакетов) компьютером-жертвой, переполнение канала – UDP flood–атака осуществилась.

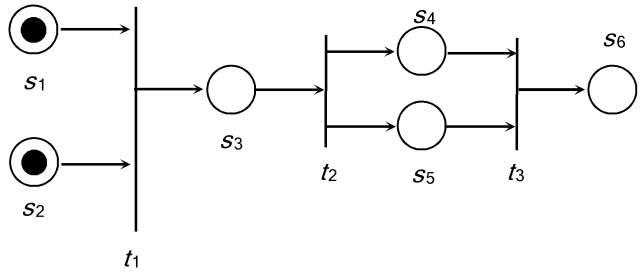

Рис. 3. Вид сети Петри-Маркова процесса реализации атаки типа «DNS Amplification» без усиления приходящего траффика

На этой сети позиции не имеют инцидентные дуги, поэтому вероятности перемещения из них в переходы равны единице.

Элементы матрицы, определяющие логические функции срабатывания сети, могут быть записаны (без учета направленности дуг графа) следующим образом:

$$v_{s_1 t_3} = \begin{array}{c|ccc} & t_1 & t_2 & t_3 \\ s_1 & 1 & 0 & 0 \\ s_2 & 1 & 0 & 0 \\ s_3 & s_1 t_1 \cap s_2 t_1 & 1 & 0 \\ s_4 & 0 & 0 & 0 \\ s_5 & 0 & 0 & 0 \\ s_6 & 0 & 0 & 0 \end{array}$$

Поскольку полушаг из перехода в позицию срабатывает мгновенно, то динамика срабатывания сети определяется только вероятностями срабатывания сети (перемещения из состояния в переход) и плотностями распределения времени нахождения процесса в каждом состоянии. Тогда в данной сети достаточно рассмотреть процесс перехода из начального состояния s_1 в конечный переход t_2.

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений [1]:

$$\Phi_{s_1 t_1}(t) = \pi_{11} \int_0^t f_{s_1 t_1}(\tau)\, d\tau, \qquad \Phi_{s_2 t_1}(t) = \pi_{21} \int_0^t f_{s_2 t_1}(\tau)\, d\tau,$$

$$\Phi_1(t) = \int_0^t f_{s_1 t_1}(\tau)\, \Phi_{s_2 t_1}(\tau) + f_{s_2 t_1}(\tau)\, \Phi_{s_1 t_1}(\tau) d\tau,$$

$$\Phi_{s_3 t_2}(t) = \pi_{32} \int_0^t f_{s_3 t_2}(\tau)\, \Phi_1(t-\tau)\, d\tau,$$

$$\Phi_{s_4 t_3}(t) = \pi_{43} \int_0^t f_{s_4 t_3}(\tau)\, \Phi_{s_3 t_2}(t-\tau)\, d\tau,$$

$$\Phi_{s_5 t_3}(t) = \pi_{53} \int_0^t f_{s_5 t_3}(\tau)\, \Phi_{s_3 t_2}(t-\tau)\, d\tau,$$

$\Phi_2(t) = \Phi_{s_4 t_3}(\tau)\Phi_{s_5 t_3}(\tau) d\tau$, где $f_{s_i t_j}(t)$ — плотность вероятности времени перемещения из состояния s_i к переходу t_j, $\Phi_{s_i t_j}(t)$ — соответствующий закон распределения, π_{ij} — вероятность срабатывания перехода, причем вероятности срабатывания всех переходов на данной траектории не зависят от времени, вероятность перемещения по всей сети рассчитывается по формуле $\pi_{\text{рез}} = \prod_{d_{ij}} \pi_{ij}$, d_{ij} — все полушаги сети.

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид:

$$f_{s_i t_j} = \lambda_{ij} e^{-\lambda_{ij} t}, \qquad (1)$$

где $\lambda_{ij} = 1/\tau_{ij}$, τ_{ij} $(i=1,\ldots,4;\ j=1,\ldots,3)$ — средние времена вышеперечисленных действий соответственно.

Расчет с применением прямого и обратного преобразования Лапласа получается весьма громоздким, поэтому целесообразно применять пуассоновское приближение для плотностей распределения вероятностей времени перемещения в переходы сети Петри-Маркова. Докажем, что процесс реализации атаки типа «DNS

Amplification» можно считать процессом (потоком) Пуассона. Для многих реальных процессов поток событий (требований) достаточно хорошо описывается законом распределения Пуассона. Такой поток называется простейшим. Простейший поток обладает несколькими важными свойствами [1, 2]:

- *стационарности*. Свойство выражает неизменность вероятностного режима потока по времени. Это значит, что число событий, поступающих в равные промежутки времени, в среднем должно быть постоянным. DNS-запросы поступают на DNS-сервер жертвы с постоянной интенсивностью, следовательно, поток стационарен.

- *отсутствие последействия*. Свойство обуславливает взаимную независимость поступления того или иного числа событий в непересекающиеся промежутки времени. Запросы, поступающие на DNS-сервер не зависят от числа поступивших в предыдущем промежутке времени, следовательно, поток без последствий.

- *ординарности*. Свойство выражает практическую невозможность одновременного поступления двух или более событий. DNS-запросы обрабатываются в порядке очереди, поэтому не могу поступать парами, тройками и т.д., следовательно, поток является ординарным.

Если поток удовлетворяет требованиям стационарности, ординарности и без последствия он называется простейшим, пуассоновским потоком. Таким образом, результирующий поток является экспоненциальным, так как экспоненциальный поток и есть простейший. На практике условия простейшего потока не всегда строго выполняются. Часто имеет место нестационарность процесса (в различные часы дня и различные дни месяца поток событий может меняться, он может быть интенсивнее утром или в последние дни месяца). Существует также наличие последействия, когда количество атак в конце интервала времени зависит от их эффективности в начале интервала. Наблюдается и явление неоднородности, когда несколько злоумышленников одновременно реализуют однотипные атаки. Однако в целом пуассоновский закон распределения с достаточно высоким приближением отражает многие процессы массового обслуживания, а, следовательно, применим для использования при распределении вероятностей возникновения атак. Применяя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения[1-3]:

$$\tau_1 = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}},\ \tau_2 = \tau_1 + \tau_{32} + \tau_{43},\ \tau_3 = \tau_1 + \tau_{32} + \tau_{53},\qquad \tau = \frac{\tau_2^2 + \tau_2\tau_3 + \tau_3^2}{\tau_1 + \tau_2},\ P(t) = 1 - e^{-\frac{1}{\tau}t},$$

где исходные параметры атаки принимают следующие значения: τ_{11}=2 с — среднее время отправления сигнала на начало атаки и приёма сигнала инфицированными компьютерами (время определено экспериментально), τ_{21} = 0,1 с – ожидание сигнала инфицированными компьютерами, τ_{32} =2 с - среднее время передачи запроса DNS-серверу, $\tau_{43}=\tau_{53}=2\cdot n$ с, где n-количество DNS-серверов, к которым отправляется запрос от «компьютера зомби». Таким образом, среднее время перехода по всей сети есть τ=1,5(4,005+2n) с. Чем больше будет «опрошено» DNS-серверов, не обрабатывающих рекурсивные запросы, тем эффективнее будет атака типа «DNS Amplification». Важно отметить, что при такой атаке источник атаки отследить весьма затруднительно.

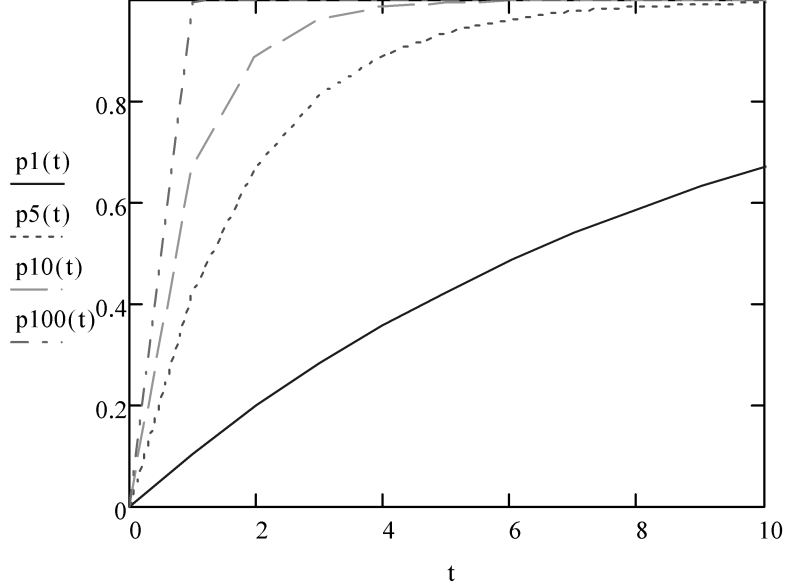

Рис. 4. Зависимость вероятности реализации атак типа «DNS Amplification» без усиления приходящего траффика от времени и для разного количества DNS -серверов

Моделирование атаки типа «DNS Amplification» с усилением (DNS – сервера обрабатывают рекурсивные запросы)

Атака посредством рекурсивных запросов является наиболее сложным и асимметричным методом атаки на DNS-сервер, для ее организации требуются минимальные вычислительные ресурсы, а результат приводит к интенсивному потреблению ресурсов DNS-сервера, который подвергается нападению. При такой атаке используются особенности работы рекурсивных DNS-запросов: когда DNS-клиент делает запрос с именем, которое отсутствует в кэш-памяти DNS-сервера, сервер отправляет повторяющиеся запросы другим DNS-серверам до тех пор, пока нужный ответ не будет отправлен клиенту. Воспользовавшись особенностями данного процесса, злоумышленник отправляет рекурсивные запросы с использованием фальшивых имен, которые, как он знает, не существует в кэш-памяти сервера. Чтобы разрешить такие запросы, DNS-сервер должен обработать каждую запись, временно сохраняя ее, и отправить запрос другому DNS-серверу, затем дождаться ответа. Другими словами, потребляется все большее количество вычислительных ресурсов (процессора, памяти и пропускной способности), до тех пор, пока ресурсы не заканчиваются [4]. Модель данной атаки, построенная с помощью аппарата сетей Петри-Маркова, изображена на рис. 3. Рассматриваются параллельные действия трёх типов инфицированных хостов. К первому типу (I) относятся компьютеры с ширококанальным подключением к интернету – способные отправлять запросы наибольшему количеству DNS – серверов, находящихся в их списке, ко второму (II) – компьютеры с выходом в Интернет, который предоставляют местные провайдеры (городские), к третьему (III) – компьютеры с подключением к Интернету через сети сотовой связи. Скорость подключения компьютеров первого типа - υ_I Мб/с, второго - $\upsilon_{II} = 0{,}27\upsilon_I$ Мб/с, третьего - $\upsilon_{III} = 0{,}024\upsilon_I$ Мб/с.

s_1 — злоумышленник имеет непосредственный доступ к необходимым ему компьютерам (заранее создана компьютерная сеть, состоящая из некоторого количества хостов, с запущенными специальными программами с автономным программным обеспечением),

t_1 — отправка сигнала «компьютеру-зомби» на начало атаки,

s_2 —«компьютеры-зомби» (I) получили сигнал и начали рассылку запросов к своим DNS-серверам, подменив свой IP-адрес на IP-адрес жертвы,

s_3 —«компьютеры-зомби» (II) получили сигнал и начали рассылку запросов к своим

DNS-серверам, подменив свой IP-адрес на IP-адрес жертвы,

s_4 — «компьютеры-зомби» (III) получили сигнал и начали рассылку запросов к своим DNS-серверам, подменив свой IP-адрес на IP-адрес жертвы,

t_2, t_3, t_4 — передача запросов к своим DNS-серверам,

s_5, s_6, s_7 — DNS-сервер не авторитативный для запрашиваемого домена и не содержит адрес в своём временном кэше передаёт подсказку для запроса к одному из корневых DNS-серверов,

t_5, t_6, t_7 — передача запроса к одному из корневых DNS-серверов,

s_8, s_9, s_{10} — корневой DNS-сервер не обладает запрашиваемым соответствием, возвращает подсказку – адрес другого DNS-сервера, который является управляющим для запрашиваемой зоны,

t_8 —итеративный запрос к указанному в ответе DNS-серверу, который является управляющим для запрашиваемого домена,

s_{11} — получение адреса авторитативного сервера для запрашиваемого домена от управляющего сервера для указанной зоны,

t_9 — запрос у авторитативного сервера,

s_{12} — авторитативный сервер для запрашиваемой зоны возвращает искомое соответствие IP-адреса,

t_{10} – отправление ответов для всех «компьютеров-зомби» с искомым IP-адресом одному «компьютеру-жертве»,

s_{13} — DNS - сервер жертвы подвергся DNS-атаке методом DNS Amplification и стал временно не работоспособным.

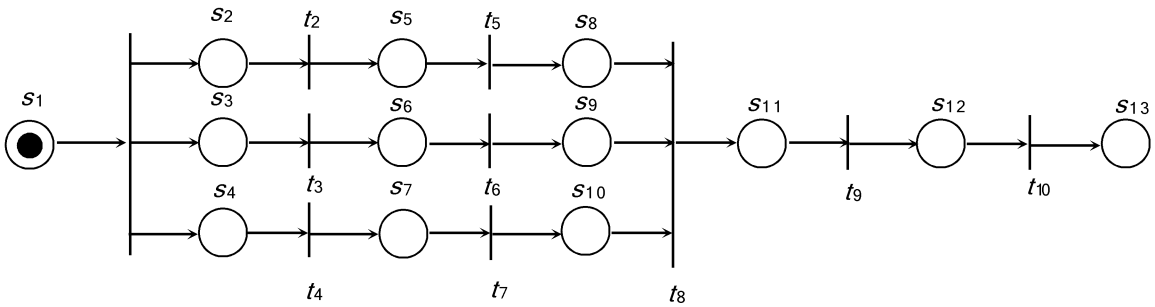

Рис.5. Вид сети Петри-Маркова процесса реализации атаки методом DNS Amplification с усилением

Элементы матрицы, определяющие логические функции срабатывания сети, могут быть записаны (без учета направленности дуг графа) следующим образом:

$v_{s_1 t_{10}} =$

	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}
s_1	1	0	0	0	0	0	0	0	0	0
s_2	$s_1 t_1 \bigcap s_2 t_1$	1	0	0	0	0	0	0	0	0
s_3	$s_1 t_1 \bigcap s_3 t_1$	0	1	0	0	0	0	0	0	0
s_4	$s_1 t_1 \bigcap s_4 t_1$	0	0	1	0	0	0	0	0	0
s_5	0	1	0	0	1	0	0	0	0	0
s_6	0	0	1	0	0	1	0	0	0	0
s_7	0	0	0	1	0	0	1	0	0	0
s_8	0	0	0	0	1	0	0	1	0	0
s_9	0	0	0	0	0	1	0	1	0	0
s_{10}	0	0	0	0	0	0	1	1	0	0
s_{11}	0	0	0	0	0	0	0	1	1	0
s_{12}	0	0	0	0	0	0	0	0	1	1
s_{13}	0	0	0	0	0	0	0	0	0	1

Для данной сети Петри-Маркова имеет место следующая система интегро-дифференциальных уравнений [1]:

$$\Phi_{s_1t_1}(t)=\pi_{11}\int_0^t f_{s_1t_1}(\tau)\,d\tau,\ \Phi_{s_2t_2}(t)=\pi_{22}\int_0^t f_{s_2t_2}(\tau)\Phi_{s_1t_1}(t-\tau)\,d\tau,\quad \Phi_{s_5t_5}(t)=\pi_{55}\int_0^t f_{s_5t_5}(\tau)\Phi_{s_2t_2}(t-\tau)\,d\tau,$$

$$\Phi_{s_8t_8}(t)=\pi_{88}\int_0^t f_{s_8t_8}(\tau)\Phi_{s_5t_5}(t-\tau)\,d\tau,\quad \Phi_{s_3t_3}(t)=\pi_{33}\int_0^t f_{s_3t_3}(\tau)\Phi_{s_1t_1}(t-\tau)\,d\tau,$$

$$\Phi_{s_6t_6}(t)=\pi_{66}\int_0^t f_{s_6t_6}(\tau)\Phi_{s_3t_3}(t-\tau)\,d\tau,\quad \Phi_{s_9t_8}(t)=\pi_{98}\int_0^t f_{s_9t_8}(\tau)\Phi_{s_6t_6}(t-\tau)\,d\tau,$$

$$\Phi_{s_4t_4}(t)=\pi_{44}\int_0^t f_{s_4t_4}(\tau)\Phi_{s_1t_1}(t-\tau)\,d\tau,\quad \Phi_{s_7t_7}(t)=\pi_{77}\int_0^t f_{s_7t_7}(\tau)\Phi_{s_4t_4}(t-\tau)\,d\tau,$$

$$\Phi_{s_{10}t_8}(t)=\pi_{108}\int_0^t f_{s_{10}t_8}(\tau)\Phi_{s_7t_7}(t-\tau)\,d\tau,\ \Phi_1(t)=\Phi_{s_8t_8}(t)\Phi_{s_9t_8}(t)\Phi_{s_{10}t_8}(t),$$

$$\Phi_{s_{11}t_9}(t)=\pi_{119}\int_0^t f_{s_{11}t_9}(\tau)\,\Phi_1(t-\tau)\,d\tau,\ \Phi_{s_{12}t_{10}}(t)=\pi_{1210}\int_0^t f_{s_{12}t_{10}}(\tau)\,\Phi_{s_{11}t_9}(t-\tau)\,d\tau.$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид (1) при $i=1,\ldots,5$; $j=1,\ldots,3$: $f_{s_it_j}=\lambda_{ij}e^{-\lambda_{ij}t}$.

Применяя пуассоновское приближение (выше доказано, что процесс реализации атаки типа «DNS Amplification» является процессом Пуассона), получим среднее время перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения. Рассмотрим время реализации атаки отдельно для каждого рассматриваемого типа инфицированных компьютеров. Атака типа «DNS Amplification» должна быть завершена, когда ото всех зараженных хостов придут DNS – ответы жертве, поэтому время реализации атаки прямо пропорционально самому медленному третьему типу компьютеров.

I: $\tau_{\text{ср.}I}=\tau_{11}+\tau_{22}+\tau_{55}+\tau_{88}+\tau_{119}+\tau_{1210}$,

II: $\tau_{\text{ср.}II}=\tau_{11}+\tau_{33}+\tau_{66}+\tau_{98}+\tau_{119}+\tau_{1210}$,

III: $\tau_{\text{ср.}III}=\tau_{11}+\tau_{44}+\tau_{77}+\tau_{108}+\tau_{119}+\tau_{1210}$, где исходные параметры атаки принимают следующие значения: $\tau_{11}=2$ с — среднее время отправления сигнала на начало атаки и приёма сигнала инфицированными компьютерами (время определено экспериментально для рассматриваемых типов зараженных компьютеров), $\tau_{55}+\tau_{88}+\tau_{119}+\tau_{1210}=\tau_{66}+\tau_{98}+\tau_{119}+\tau_{1210}=\tau_{77}+\tau_{108}+\tau_{119}+\tau_{1210}=$ 15 с (по умолчанию время рекурсивного запроса в службе DNS равен 15 секундам, после чего рекурсивный запрос завершается со сбоем) [5], $\tau_{22}=0{,}5$ с – среднее время передачи запроса DNS-серверу для I, $\tau_{33}=0{,}5\cdot3{,}75=1{,}875$ с (т.к. $\upsilon_{II}\cdot\tau_{33}=\upsilon_I\cdot\tau_{22}$, где $\upsilon_{II}=0{,}27\upsilon_I$) - среднее время передачи запроса DNS-серверу для II, $\tau_{44}=0{,}5\cdot41{,}6=20{,}8$ с (т.к. $\upsilon_{III}\cdot\tau_{44}=\upsilon_I\cdot\tau_{22}$, где $\upsilon_{III}=0{,}024\upsilon_I$).

Таким образом, среднее время перехода по всей сети для I есть $\tau_{\text{ср.}I}=17{,}5$ с, для II - $\tau_{\text{ср.}II}=18{,}875$ с, для III - $\tau_{\text{ср.}III}=37{,}8$ с, а зависимость вероятности реализации атак рассматриваемых типов компьютеров от времени приобретает вид, представленный на рис. 4.

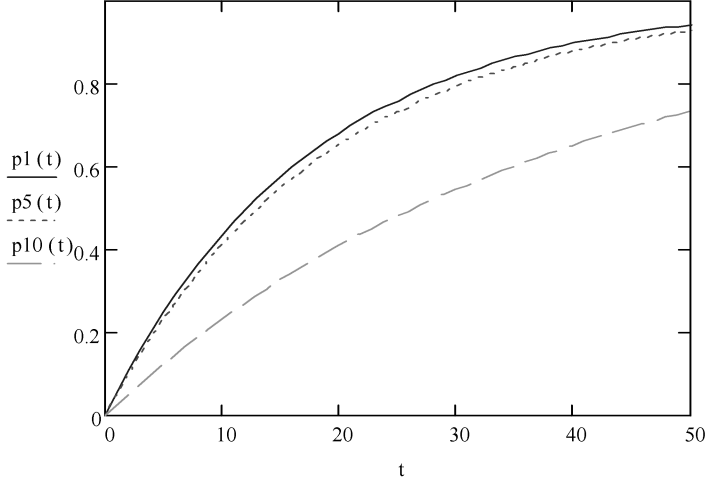

Рис. 4. Зависимость вероятности реализации атаки типа «DNS Amplification» с усилением приходящего траффика для разных типов компьютеров (I, II, III типа соответственно)

Очевидно, что атака будет реализована быстрее, если использовать только компьютеры I и/или II типа. Среднее время от количества зараженных хостов сильно меняться не будет, особенно, если использовать компьютеры I типа, т.к. время на отправление сигнала будет компенсировано временем DNS-запроса. Как правило, злоумышленники готовятся к данной атаке заранее, поэтому хосты с выходом в Интернет через сети сотовой связи не используются из-за низкой скорости передачи DNS-запросов. Злоумышленники предварительно регистрируют собственную зону с записями максимальной длины — длинными именами хостов — и полностью заполненной записью TXT, содержимым которой может быть произвольный текст.

Асимметричный характер рекурсивной атаки и низкая скорость затрудняют борьбу с такими атаками. Рекурсивная атака может быть пропущена как системами защиты, так и людьми, которые больше сосредоточены на выявлении атак с большим объемом.

Литература:

1. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа/ Н.М. Радько, И.О. Скобелев - М.: РадиоСофт, 2010. - 230 с.

2. Тихонов В.И. Статистическая радиотехника/ В.И. Тихонов – Москва «Радио и связь», 1982.- 625 с.

3. Язов Ю.К. Основы методологии количественной оценки защищенности и эффективности защиты информации в компьютерных системах/ Ю.К. Язов– Северо-Еавказский научный центр высшей школы, 2006. – 234 с.

4. SecurityLab. – Электрон. дан. – Режим доступа:
http://www.securitylab.ru/

5. TechNet. Microsoft. – Электрон. дан. – Режим доступа:
http://www.technet.microsoft.com/

Воронежский государственный технический университет
Voronezh State Technical University

ANALYTICAL IMPLEMENTATION probabilistic model attacks on DNS – SERVERS

E.E. Smolkina, A.G. Ostapenko, N.I. Barannikov, I.L. Bataronov

In this paper we consider the risk-model-type attacks «DNS Amplification» based on Petri nets, Markov. The comparative characteristics of the probability of an attack on the time under consideration, number of infected hosts and different types of computers

Key words: Petri net-Markov probability, DNS - attack, Poisson flow