Сетевые угрозы

Владимир Борисович Лебедев

ТТИ ЮФУ

Программа

- Риски вторжений в сеть
- Источники вторжений в сеть
- Социотехника и фишинг

Риски вторжений в сеть

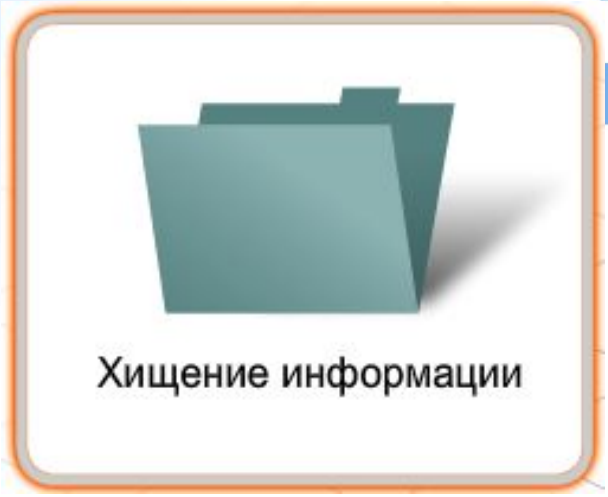
Компьютерные сети – как проводные, так и беспроводные – стремительно приходят в повседневную жизнь. Индивидуальные пользователи и организации в равной мере зависят от надежной работы компьютеров и сетей в таких задачах, как электронная почта, учет, организационное управление и работа с файлами. Несанкционированное вторжение в сеть может привести к чрезвычайно затратным перебоям и потере ценных результатов работы. Атака на сеть может иметь разрушительные последствия с потерей времени и денег в результате повреждения или хищения важной информации и ресурсов.

Злоумышленники могут получить доступ в сеть, эксплуатируя уязвимости в ПО, атакуя оборудование или даже используя такие изящные приемы, как угадывание чужого имени пользователя и пароля. Злоумышленники, которые получают доступ, изменяя программное обеспечение или эксплуатируя уязвимости в программном обеспечении, часто именуются хакерами.

Хакер, получивший доступ в сеть, сразу становится источником четырех видов угроз:
Хищение информации;
Хищение личных данных;
Уничтожение/изменение данных;
Нарушение работы.

Хищение информации

Проникновение в компьютер для получения конфиденциальной информации.
Эта информация может быть использована или продана с различными целями.
Пример:
Хищение конфиденциальной информации, принадлежащей организации, например, сведений о научно-технических разработках.



Потеря данных и манипуляции с ними

Проникновение в компьютер с целью уничтожения или изменения записей данных. Примеры потери данных:
передача вируса, форматирующего жесткий диск компьютера.
Примеры манипуляций с данными: проникновение в систему хранения информации с целью изменения каких-либо данных, например, цены изделия.

Потеря данных и манипуляции с ними

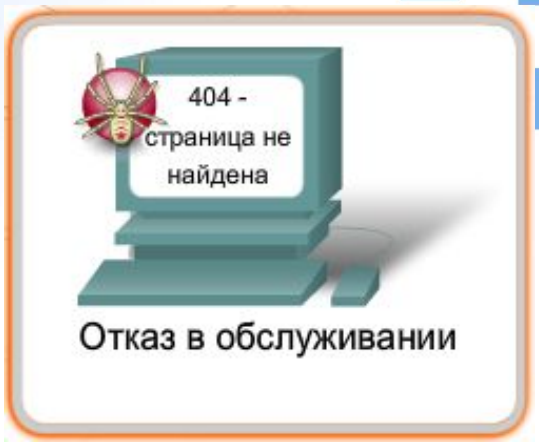
Хищение персональных данных

Вид хищения информации, при котором крадутся личные данные для использования этих данных с целью обмана. С использованием этой информации человек может получить юридические документы, подать заявление на кредит и совершать несанкционированные покупки через Интернет. Проблема хищения персональных данных продолжает обостряться, а финансовые потери составляют миллиарды долларов в год.

Хищение персональных данных

Отказ в обслуживании

Лишение зарегистрированных пользователей возможности доступа к услугам, которыми они имеют право пользоваться.



Внешние угрозы

Внешние угрозы исходят от лиц, находящихся за пределами организации и не обладающих санкционированным доступом к компьютерным системам и сетям. В этом случае атаки совершаются главным образом из Интернета, по беспроводным сетям или через серверы коммутируемого доступа.

Внутренние угрозы

Внутренние угрозы исходят от пользователей, имеющих официально разрешенный доступ в сеть с учетной записью или физический доступ к сетевому оборудованию. Злоумышленники, атакующие сеть изнутри, знакомы с внутренней политикой и персоналом. Кроме того, они обычно знают, какая информация представляет ценность и наиболее уязвима, а также – как получить к ней доступ.

Однако не все атаки являются преднамеренными. В некоторых случаях, внутренняя угроза исходит от добросовестного сотрудника, который, находясь за пределами компании, стал жертвой вируса или нарушения безопасности и, впоследствии, неосознанно принес эту угрозу во внутреннюю сеть.

Многие компании затрачивают значительные ресурсы на защиту от внешних атак, хотя большинство атак исходит из внутренних источников. Согласно данным ФБР, внутренний доступ и нарушение регламента пользования компьютерными системами – причина 70% известных нарушений в области информационной безопасности.

Социотехника и фишинг

Манипуляция другими людьми остается для злоумышленников одним из простейших способов получения доступа как изнутри, так и извне. Широко распространена практика эксплуатации психологических слабостей, называемая социотехникой.

Социотехника

Социотехника – использование внешних факторов для влияния на поведение группы людей. В контексте компьютерной и сетевой безопасности под социотехникой понимаются различные приемы введения в заблуждение внутренних пользователей с подталкиванием к выполнению определенных действий или разглашению конфиденциальной информации.

В результате злоумышленник через неподозревающих внутренних пользователей получает доступ к внутренним ресурсам и личным данным, например, банковским реквизитам и паролям.

Атаки с применением социотехники возможны благодаря тому, что пользователи часто являются самым слабым звеном в системе безопасности. Злоумышленники, применяющие социотехнику, могут находиться как внутри, так и за пределами организации, однако чаще всего они не контактируют с жертвами лицом к лицу.

Три наиболее распространенных приема **социотехники: вымышленный предлог, фишинг и вишинг.**

Социотехника и фишинг

Вымышленный предлог

Одной из форм социотехники является использование вымышленного предлога, побуждающего жертву разгласить информацию или выполнить определенное действие. Контакт с жертвой обычно осуществляется по телефону. Данный прием эффективен в том случае, если злоумышленнику удается завладеть доверием своей цели или жертвы. Злоумышленник во многих случаях изначально должен располагать некоторыми знаниями или наблюдениями. Например, если ему известен номер счета жертвы, он сможет воспользоваться этой информацией для вхождения в доверие к жертве. После этого выудить дополнительную информацию будет проще.

Фишинг

Фишинг представляет собой форму социотехники, в которой злоумышленник маскируется под легитимную внешнюю организацию. Контакт с жертвой фишинга обычно происходит по электронной почте. Злоумышленник может обратиться с просьбой уточнить определенные реквизиты, например пароли или имена пользователей, во избежание крайне нежелательных последствий.

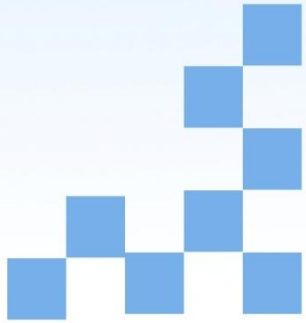
Вишинг / телефонный фишинг

Вишинг – новая форма социотехники, основанная на использовании IP-телефонии (VoIP). Неподозревающий пользователь получает сообщение голосовой почты с указанием перезвонить на номер, принадлежащий легитимной службе банковского самообслуживания. Однако разговор перехватывается мошенником, во владении которого оказываются номера банковских счетов и пароли, сообщаемые по телефону для проверки.

Социотехника и фишинг

Вопросы&Ответы

Сетевые угрозы



ТТИ ЮФУ