Сюжет

Предистория

Ты новый сотрудник в этом офисе и в первый день тебя посадили на место предыдущего работника который не придерживался правил информационной безопасности, он накачал всякую шнягу и использовал только пиратское ПО, но других компьютеров нет поэтому надо работать с чем есть и снести винду нельзя так как нельзя потерять папку анапа 2007, а флешки нет. Наш новенький должен выполнить задачи и завершить рабочий день не дав доступ к своему пк хакеру.

Концепт игры

Игра состоит из трех дней, каждый день есть какое то количесто задач которые должен выполнить игрок, задачи офофрмлены как ярлыки приложений на рабочем столе компьютера, с каждым последующим днем количество задач будет рознится в зависимости от того кто выиграл в прошлый денью. Чтобы победить в дне игроку нужно выполнить какие то определенные задачи, а хакеру добраться до каких то определенных программ.

Каждый ход игрок может выбирать ходить или выполнить задание,хакер делает то же самое и при взломе программы хакер получает себе на руку рандомный вирус, который он может разметистить когда захочет и на тех программах которые он даже не взламывал ,самвирус срабатывает при попытке выполения задания игроком , для выполнения задания нужно использовать ресурсы, а именно байты данных которые можно получить при выполнении задания, также за выполнение задания можно получить способность, с помощью которых можно противодействовать хакеру( проверить приложение на наличие вируса, поставить ограничение на перемещение хакера, отменить эффект от активированного вируса который поставил хакер на какое то из приложений. Так же он знает, что хакер заразил какие – то программы. Допустим, если игрок входит в какие – нибудь проги по типу питона, офисов и тд, то там может быть троян. Если в браузер, то там фишинг сайты, которые воруют данные. Если почта, то всякий спам, типо у вас бонус зайдите и получите. Также если скачать какую то прогу то он может скачать троян, шпион, бэкдор, винлокер, adware.

Чтобы взломать программу которая не требуется хакеру он может использовать брутфорс-атаку и получить при взломе рандомный вирус на руку или троян, который требуется для взлома требующихся для победы программ.

Хакер может ставить вирусы на приложения при активации которых игрок будет терять байты данных которые нужны выполнения задач. среди вирусов которые может поставить хакер есть: фишинг-потеря байтов данных, атаки на цепочку поставок- потеря абилок игрока,эксплойт- игрок пропускает ход, спуффинг-заменяет получение игроком обилки, получением вируса хакером, SQL-узнать все обилки на руке игрока.

Игрок может использовать такие способности как: проверка электронно-цифровой подписи и выявление вируса если он имеется, файерволл для блокировки хода хакера, стойкие пароли - хакеру нужно взламывать эту программу на один ход дольше

Клерк должен выполнить задачи

* internet explorer(День 1: Зайти в интернет браузер для установки браузера амиго.Потенциальная угроза для игрока: сайт с вредоносным ПО. День 2: Покупка какой то вещи в интернет магазине. Потенциальная угроза для игрока: потеря данных банковской карты, фишинговый сайт. День 3: Найти в браузере статью связанную со спецификой работы. Потенциальная угроза: посещение сайта с межсайтовыми скриптами.)
* Mail.ru(Проверка электронной почты на наличие письма от начальства с последующими задачами. Потенциальная угроза: Фишинговое письмо с ссылкой ведущей к вредоноснвм ресурсам.)
* Excel(Работа с таблицами, создание баз данных. Потенциальная угроза: программа-шпион, воровство данных хакером)
* Написать в ворде описание чего – либо(иконка ворд)
* Написать код в питоне(иконка питона)
* Проверить новости(иконка браузера )
* Написать статью в википедии(иконка браузера)
* Вход в мессенджер(иконгка браузера)
* Затестить прогу, а ее надо будет скачать (иконка браузера а также нн иконка проги)
* Нарисовать превьюшку(иконка пайнта)
* Отфотошопить фотку(иконка адоб фотошоп)
* Настроить сервер(иконка проги нн)
* Достать файлы фтп файл(иконка папки)
* Поиск важного файла:

Описание: Клерку нужно найти важный файл на компьютере, который потерялся где-то на рабочем столе. Файл должен быть найден и сохранен до конца рабочего дня.

* Установка обновлений:

Описание: Клерку предстоит установить обновления операционной системы и программ для поддержания безопасности компьютера.

* Антивирусная проверка:

Описание: Клерк должен запустить антивирусную проверку своего компьютера, чтобы обнаружить и удалить вредоносные программы.

* Бекап данных:

Описание: Клерку нужно сделать регулярный резервный копии важных данных на внешний носитель или в облачное хранилище.

* Защита от фишинга:

Описание: Клерк должен обнаружить фишинговые письма в своей почте и избегать открытия вредоносных вложений или перехода по подозрительным ссылкам.

* Создание безопасного пароля:

Описание: Клерк должен создать безопасный пароль для своей учетной записи и изменить старый, чтобы предотвратить взлом.

* Очистка временных файлов:

Описание: Клерк должен очистить временные файлы и кэш браузера для повышения производительности компьютера и уменьшения риска заражения.

* Разблокировка заблокированных файлов:

Описание: Клерку нужно разблокировать файлы, которые были зашифрованы вирусом-вымогателем (рансомваром).

* Поиск и устранение сбоев:

Описание: Клерк должен найти и устранить сбои в работе компьютера, вызванные вирусами или другими проблемами.

* Обучение сотрудников по кибербезопасности:

Описание: Клерк должен провести обучение сотрудников по правилам кибербезопасности, чтобы уменьшить риск возникновения угроз.

* Защита важной информации:

Описание: Клерк должен убедиться, что важная информация и данные остаются в безопасности от хакеров.

* Создание резервных копий базы данных:

Описание: Клерк должен регулярно создавать резервные копии базы данных компании для предотвращения потери данных.

* Обнаружение вторжения:

Описание: Клерк должен мониторить сетевую активность и обнаруживать попытки несанкционированного вторжения в компьютерную систему.

* Аудит безопасности:

Описание: Клерк должен провести аудит безопасности компьютерной системы и выявить уязвимости, которые могут быть использованы хакерами.

* Обнаружение и блокирование сетевых червей:

Описание: Клерк должен обнаружить и блокировать сетевые черви, которые пытаются распространиться по компьютерной сети.