МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ОБЪЕКТИВНОГО КОНТРОЛЯ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

ДОКЛАДЧИК: заведующий кафедрой Информационной и кибернетической безопасности Учебно-научного института защиты информации д.т.н., профессор БУРЯЧОК В.Л.

План доклада

1. Влияние информации и современных ИТ-технологий на развитие информационного общества
2. Зависимость критически важных отраслей и секторов мировой экономики от угроз антропогенного и техногенного характера
3. Причины утечки данных. Виды информационного ресурса, наиболее подверженного похищению
4. Новая услуга в области информационной безопасности - «тестирование на проникновение» (pentest)
5. Популярные методики и векторы атак при проведении pentest
6. Подходы к проведению pentest
7. Структурно-логическая схема и обобщенный алгоритм проведения pentest
8. Критерии завершения теста на проникновение и ценовая политика его проведения
9. Подготовка специалистов по pentest в Государственном университете телекоммуникаций
10. Перечень специализированных программ для подготовки специалистов по pentest
11. Примеры специализированных инструментов для проведения и подготовки специалистов по pentest

Выводы

История развития информационного общества тесно переплетена с информационными операциями. В последнее время это приводит к тому, что мероприятия по *манипуляции информацией, дезинформации конкурирующих сторон и/или введении их друг друга в заблуждение* являются неотъемлемой частью внутренней и внешней политики подавляющего большинства государств земного шара.

Главную роль в этих процессах в последнее время играет ***Internet - пятая власть мира***. Именно поэтому все чаще знаменитое выражение Н.Ротшильда

«Кто владеет информацией, тот владеет миром»

звучит в новой трактовке:

«Кто владеет *Internet*, тот владеет миром»

Обьективность данного высказывания обьясняется тем, что **именно благодаря новейшим Интернет-технологиям** *доступ к мировым объемам информации получило практически все население планеты Земля,* а **изобретение мощных компьютеров**

позволило, в свою очередь, превратить *современные ИТ системы и сети в «**электронную артерию**» всего человечества.*

Известно, что такое положение дел, в свою очередь, способствует как *глобальной интеллектуализации, развитию промышленности и существенному расширению возможностей международного бизнеса*, так и приводит *к значительной зависимости прежде всего*

Перечень критически важных секторов и отраслей мировой экономики

Отрасль	Сектора
Энергетика	- электричество; - нефть и природный газ
Водоснабжение	- дамбы; - очистные и распределительные системы и т.п.
Транспорт и транспортные перевозки	- судоходство и авиация; - железнодорожный и автомобильный транспорт; - логистика и т.п.
Пищевая промышленность	- торговля продуктами питания; - сельское хозяйство и т.п.
Средства массовой информации и культурные активы	- радио и пресса; - культурное наследие и т.п.
Финансы и страхование	- банки; - фондовые биржи; - страховые компании; - финансовые услуги и т.п.
Здравоохранение	- здравоохранение; - аптечное дело и т.п.
Образование	- дошкольные и школьные учреждения; - профессионально-технические заведения; - высшие учебные заведения и т.п.
Информационно-коммуникационные технологии	- телекоммуникации (включая спутники); - информационно-телекоммуникационные системы; - программное и аппаратное обеспечение и т.п.
Государственное управление и администрирование	- правительство; - парламент; - правовые институты и т.п.

критически важных отраслей и секторов мировой экономики

от *угроз*

антропогенного и техногенного характера, а также природных катаклизмов.

Федеральне бюро розслідувань США запустило у 2001 році програму попередження комп'ютерних злочинів InfraGuard, розроблену Центром захисту національної інфраструктури (National Infrastructure Protection Center, NIPC, http://www.nipc.gov/). Однією з цілей програми є створення захищеної від вторгнення ззовні мережі для обміну інформацією між компаніями та органами забезпечення правопорядку про здійснені атаки та надання відомостей, які можуть попередити такі зазіхання. Однак деякі експерти вважають, що контроль з боку ФБР спричиняє недоступність інформації іншим учасникам. Це зумовлює появу інших подібних програм. Так, американські комп'ютерні корпорації Miscrosoft, Oracle, AT&T, Intel та 15 інших компаній створили центр обміну інформацією по боротьбі з комп'ютерною злочинністю (Information Technology Information Sharing and Analysis Center).

Количество государственных и коммерческих структур, подверженных таким воздействиям в последнее время значительно увеличилось. Этому способствует «продуктивная работа» действующих лиц информационного и киберпространств – легальних пользователей, хакеров, киберпреступников и кибертеррористов, а также подразделений современных кибервойск.

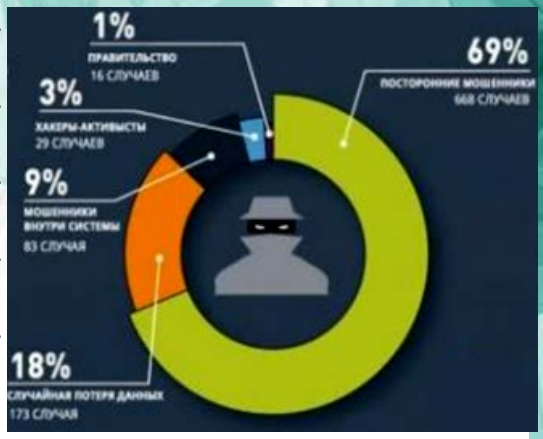
Легальные пользователи, операторы, администраторы и т. П.	На информационную и кибербезопасность негативно не влияют
Хакеры, не имеющие злокачественных намерений	На информационную и кибербезопасность влияют отрицательно, лишь для собственного самоудовлетворения и самовыражения, азарта, так называемого "спортивного интереса"
Хакеры, преследующие корыстные цели	На информационную и кибербезопасность влияют негативно, спланировано ради удовлетворения мести, или с целью решения определенных корыстных намерений
Сетевые комбатанты	На информационную и кибербезопасность влияют опосредованно, имея целью решения собственных целей, тоесть имея собственную мотивацию
Киберпреступники	На информационную и кибербезопасность влияют негативно, преследуя при этом сугубо преступные цели
Кибертеррористи	На информационную и кибербезопасность влияют негативно, преследуя при этом сугубо террористические цели
Подразделения государственных и негосударственных структур, осуществляющих информационные операции	На информационную и кибербезопасность, состояние информационного и киберпространства влияют сугубо в военнополитичний целях
Кибервойська	На информационную и кибербезопасность, состояние информационного и киберпространства влияют комплексно

Степень их влияния на информационную и кибербезопасность

Именно они, будучи подкрепленными новыми возможностями по взлому веб-сайтов, серверов приложений и БД, способны причинить не только прямые финансовые потери, но и парализовать работу критически важных объектов инфраструктуры стран мира

Причины утечки данных:

- 69% инцидентов – результат **внешних атак**
- 18% инцидентов – результат **случайной потери данных**
- 9% инцидентов – результат **деятельности инсайдеров**
- 3% инцидентов – результат **деятельности хакеров**
- 1% инцидентов – результат операций по **кибербразведке**



Хакерство — загроза чи невинна гра?

Секретні служби США поінформували комітет з озброєнь сенату про загрозу безпеці США № 1. '(і становив хакер, який близько 200 разів зламав системи безпеки різного рівня і скопіював десятки секретних файлів, включаючи подробиці досліджень і розробок балістичних ракет. На те щоб його піймати, знадобилось 13 місяців. Хакером виявився англійський 16-річний хлопець, комп'ютерні навички котрого шкільний учитель оцінив у 4 бали. У ході судового засідання адвокат стверджував, що неповнолітній хакер не мав злого наміру і перебував під враженням від фільму «Ігри патріотів».

Виды похищенного ИР:

64% - идентификационная информация
16% - финансовые данные
11% - данные учетных записей
5% - интеллектуальная собственность
4% - другое

Хакери: погоня за славою, розваги чи самореалізація?

У січні 2001 року на сайт! Xakep.ru з'явилось повідомлення про злом сайта ФБР (www.fbi.gov). За неперевіреними зі зрозумілих причин даними, хакери змінили структуру сайту і стерли директорію «wanted» (список найбільш небезпечних злочинців, яких розшукує ФБР), зробивши дублювальні копії файлів,

Учитывая изложенное можно сформулировать следующую гипотезу, ставшую в последнее время обьективной реальностью: **чем больше ИТ технологии развиваются и интегрируются в нашу повседневную жизнь, тем более важными и востребованными в любых сферах человеческой деятельности становятся технологи информационной безопасности. *Подтверждением этому являются***:

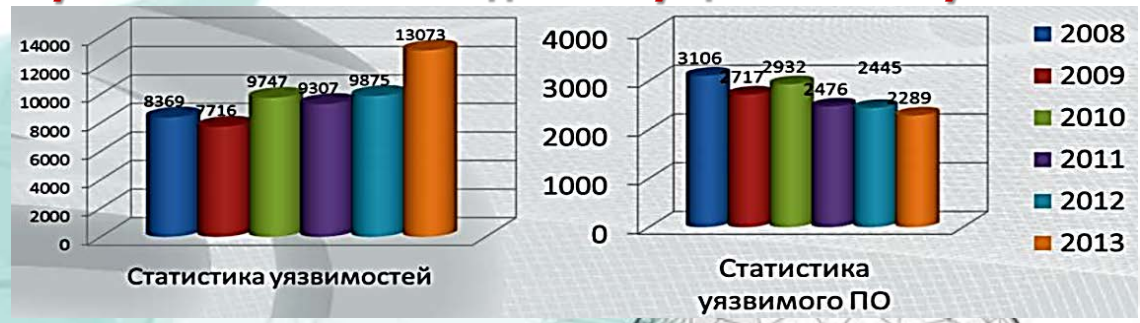
1) *статистические данные, обнародованные корпорацией WASC* (Web Application Security Consortium), согласно которым **уязвимыми к хакерским атакам являются более 96% веб-сайтов, около 74% прикладного и системного программного обеспечения (ПО), приблизительно 68% серверных приложений.**

Типы уязвимостей в компонентах ОС

Типы уязвимостей в серверных приложениях

При этом и те, и другие считают, что как в ПО, так и в серверных приложениях доминируют, в последнее время , одни и те же уязвимости типа: **отказа в обслуживании, компроментации системы и повышения привилегий.**

2) *выводы специалистов из международной организации CERT* (Computer Emergency Response Team), которые **утверждают, что количество инцидентов в инфосфере и количество выявленных уязвимостей ежегодно существенно увеличивается.**



Порушення безпеки ІТ — несанкціоноване використання ресурсів

За результатами розслідування, яке тривало 6 місяців, Центральне розвідувальне управління США (http://www.cia.gov) звільнило 4 співробітників за створення і використання таємного чата безпосередньо в мережі розвідувального підрозділу. Звільнених було визначено як неблагонадійних, щоб їх не могли прийняти на роботу аналогічні організації. Один із них обіймав високу посаду в американській розвідці. Ще 96 осіб понесли різного роду стягнення.

Чат, який було створено в середині 1980-х років, відвідували близько 160 співробітників, щоб пофліртувати, пожартувати або просто побазікати в обхід систем безпеки. В офіційній заяві ЦРУ цей факт було названо «волаючим порушенням цілісності мережі». Цей скандал ще раз засвідчив не лише існування проблем щодо інформаційної безпеки у ЦРУ, а й серйозне ставлення до них. Можна згадати, що наприкінці 1996 року за зберігання секретних матеріалів на домашньому комп'ютері, підімкненому до Інтернет, було звільнено Джона Дейча, директора Управління.

Для предотвращения влияния таких и им подобных уязвимостей на собственную инфраструктуру, а также ее защиты от ряда внешних и внутренних угроз большинство стран мира выделяет нынче колоссальные финансовые средства.

Пример - переполнение буфера в Java JDK и JRE

Серьезная уязвимость
Переполнение буфера
ID: 171936
CVE: CVE-2009-1098
Secunia: 34451, 34489, 34495, 34496, 34632, 34675, 35156, 35223, 35255, 35416, 35776, 36185, 37460
Bugtrack: 34240

Описание

Переполнение буфера в Java SE Development Kit (JDK) и Java Runtime Environment (JRE) позволяет злоумышленникам, действующим удаленно, получить доступ к файлам или выполнить произвольный код, используя специально сформированный GIF-файл изображения.

CVSS

Максимальный уровень риска !

Базовая оценка: 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Ссылки

BID (34240): http://www.securityfocus.com/bid/34240

/data/vulnerabilities/exploits/254570.tgz

Но, довольно часто бывает так, что приобретая дорогое антивирусное ПО и дорогие аппаратные брандмауэры, - подавляющее большинство заказчиков не получает при этом практически ничего, кроме теоретических доказательств того, что вложенные средства делают их сети от хакерских атак более защищенными.

Чтобы уберечься от лишних потерь государственные и коммерческие структуры применяют в настоящее время такую услугу в области информационной безопасности, как

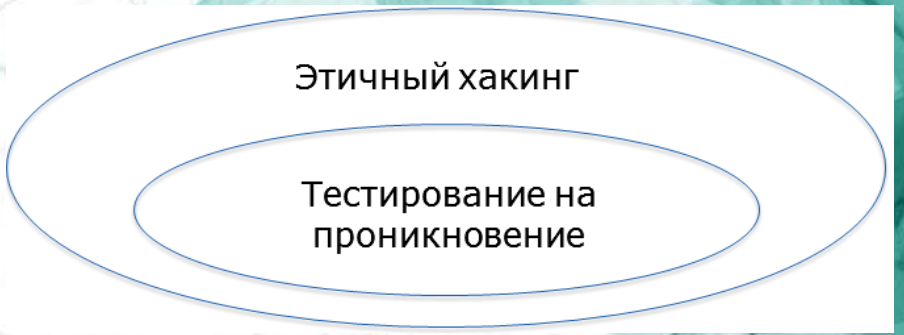
«ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ»

(*pentest*)

Она предполагает *осуществление санкционированного обхода существующего комплекса средств защиты собственных ИТ систем и сетей с целью обнаружить в них слабые места* (путем идентификации максимально возможного количества уязвимостей за ограниченное время при заданных условиях и текущем состоянии) *и убедиться в их эффективности*.

Суть теста: в ходе pentest роль злоумышленника играет специалист, который должен осуществить атаку на веб-сервер, сервер приложений или баз данных, персонал или корпоративную сеть, определить уровень защищенности, выявить уязвимости, идентифицировать наиболее вероятные пути взлома и определить на сколько хорошо работают средства обнаружения и защиты ИС от атак на ОИД.

Тестирование на проникновение является составной частью ***этичного хакинга*** – процесса, ориентированного на поиск и обнаружение уязвимостей ИБ, а также на проведение контролируемых атак, направленных как на отдельные ИТ системы - CMS, CRM, ERP и интернет клиент-банк, так и на инфраструктуру объекта информационной деятельности в целом.



«Знай врага и знай себя, и ты пройдешь сотню битв без поражения» (Сунь Цзи) – *ключевая идея этичного хакинга*

Тестирование на проникновение может проводиться в составе:

Тест на проникновение != аудит информационной безопасности

Тест на проникновение != анализ уязвимостей

Тест на проникновение != аттестация

При проведении ***аудита ИБ*** элементы *pentest* могут использоваться для оценки эффективности реализации таких защитных механизмов, как «защита от злокачественного кода», «обеспечение сетевой безопасности» и других видов атак. Главная задача аудитора состоит в том, чтобы найти ответы на такие вопросы: «как проще попасть в систему, нарушить ее работоспособность или что-нибудь получить» и «какой может быть мнимальная цена взлома».

При ***анализе уязвимостей*** элементы *pentest* могут использоваться для оценки используемого в ИТ системах (сетях) программного и аппаратного обеспечения на предмет попытки их эксплуатации для проникновения в систему.

В ходе ***аттестации объектов информатизации*** элементы *pentest* могут использоваться для демонстрации на практике того, что несоответствие требованиям стандартов или другим нормативно-правовым документам по безопасности информации может привести к успешной компрометации системы.

Для этого аудитор применяет, как правило, ряд стандартных инструментов, представленных на *СЛАЙДЕ №9*

Примеры специализированных инструментов для проведения и подготовки специалистов по *pentest*

Pwn Pad

Устройство предназначено для проведения скрытого pentest. Устройство оснащено мощным четырех ядерным процессором (Qualcomm Snapdragon S4 Pro, 1,5 Ггц), 7-дюймовым экраном с разрешением 1900 x 1200 и мощной батареей, обеспечивающей до девяти часов активной работы (3950 мА/ч), 2 Гб ОЗУ и 32 Гб внутренней памяти. В комплект входят три адаптера: две мощные внешние антенны для пентеста 802.11 b/g/n беспроводных сетей и Bluetooth, а также переходник USB - Ethernet, позволяющий проверять проводные сети.

Главной составляющей устройства является программная компонента: Metasploit, SET, Kismet, Aircrack-NG, SSLstrip, Ettercap-NG, Bluelog, Wifite, Reaver, MDK3, FreeRADIUS-WPE, Evil AP, Strings Watch, Full-Packet Capture, Bluetooth Scan и SSL Strip.

CreepyDOL

Специальное ПО и устройство на базе Raspberry Pi с помощью которых можно создать сеть, перехватывающую Wi-Fi трафик и собирающую конфиденциальную Информацию о пользователях. Как результат, устройство позволяет позициони-ровать владельца устройства. Вся информация обрабатывается на центральном Сервере. Там же можно в реальном времени отслеживать передвижения владель ца телефона и его перехваченные данные.

Причем от слежки не спасет даже использование VPN, так как, например, на iOS устройствах подключиться к VPN можно только после подключения к Wi-Fi.

Demy[illegible]

Устройство предназначено для проверки на прочность Ethernet-, Wi-Fi - и Bluetooth-сетей. Построено оно на базе популярного одноплатного компьютера Raspberry Pi и оснащено ARM-процессором 700 МГц, который можно разогнать до 1 ГГц. Также на борту имеется 512 Мб оперативной памяти, SD-карта на 32 Гб, Ethernet, Bluetooth, Wi-Fi адаптеры. В качестве ОС используется Debian Linux с набором предустановленных security-тулз: Nmap, OpenVPN, w3af, aircrack-ng, btscanner, ophcrack, John the Ripper и другие.

Отсутствующие, но необходимые пользователю инструменты можно доустановить самостоятельно.

Популярные методики и векторы атак при проведении *pentest*

Кроме навыков использования огромного количества техник и инструментов, приведенных на слайде №9, аудитор для реализации пентеста должен понимать ***все нюансы технической и организационной составляющей ИБ, владеть навыками социальной инженерии, придерживаться определенных методик:***

- Penetration Testing Model (**BSI**);
- Payment Card Industry Data Security Standard (**PCI DSS**);
- Information System Security Assessment Framework (**ISSAF**);
- Penetration Testing Execution Standard (**PTES**);
- Open Source Security Testing Methodology Manual (**OSSTMM**);
- Open Web Application Security Project Testing Guide (**OWASP**);
- **NIST Special Publication** 800-115: Technical Guide to Information Security Testing and Assessment

Вектор атаки	Описание
Физический	Атаки с использованием непосредственного физического доступа внутрь периметра корпоративной сети, что защищается
Сетевой	Дистанционные атаки на сетевые ресурсы и протоколы
Электронная почта	Атаки с использованием электронной почты (в том числе с элементами социальной инженерии)
Приложения	Атаки с использованием специфических приложений используемых Заказчиком (например, web портал)
Беспроводные сети	Атаки направлены на беспроводные протоколы передачи данных 802.11 (Wi-Fi), 802.15 (Bluetooth), 802.16 (Wi-Max)
Клиентские приложения	Атаки на клиентские программы
Мобильные устройства	Атаки на мобильные устройства (мобильные и переносные компьютеры, смартфоны и т.д.)
Социальная инженерия	Атаки на пользователей с использованием методов соц. инженерии

а также ***определенных векторов атак, которые могут быть направлены прежде всего на:***

1) ***пользователей корпоративных систем*** (соц.инженерия),

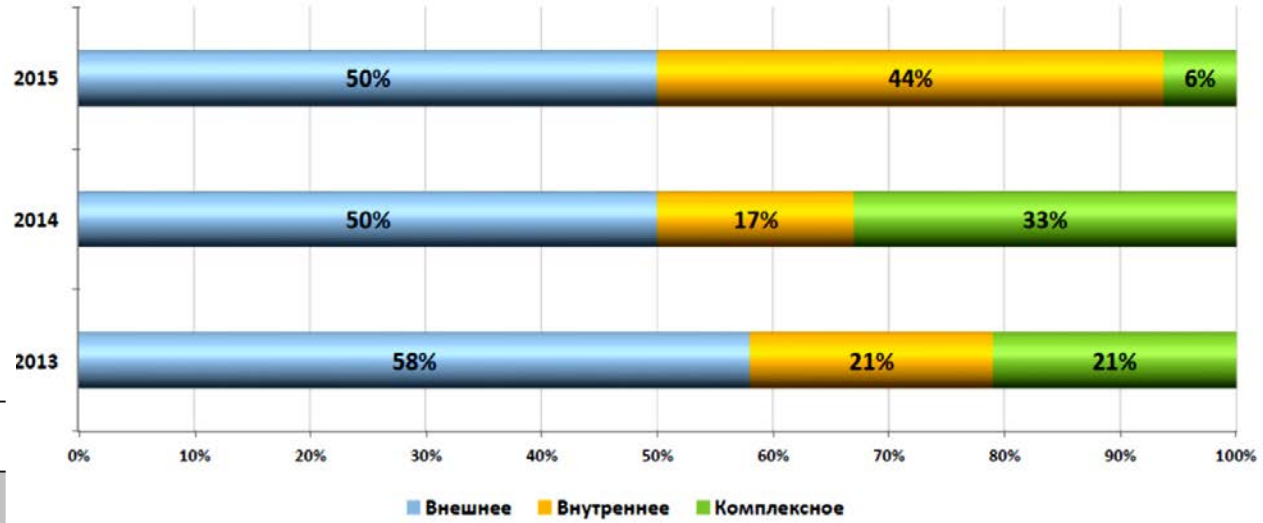
2) ***внешний периметр сети*** (периметр IP-адресов и Web-сайтов),

3) ***беспроводные сети*** IEEE 802.11(Wi-Fi), 802.15(Bluetooth) и 802.16(Wi-Max),

4) ***переносимые компьютеры и мобильные устройства***

Подходы к проведению *pentest*

По ***месту расположения аудитора*** относительно сетевого периметра корпоративной системы *pentest* может быть **внутренним, внешним** или **комплексным**.



Внешнее тестирование на проникновение

Тип тестирования	Описание
Тестирование внешнего периметра сети	Анализ включает только внешние IP-адреса компании, доступные из Інтернет
Тестирование WEB сайтов	Анализ включает только WEB-сайты и сервисы компании, доступные неограниченному круга внешних пользователей
Тестирование специализированных приложений	Анализ включает разные приложения, доступные внешним пользователям, которые используют сервера компании
Тестирование сотрудников на устойчивость к методам социальной инженерии	Попытка получения доступа к системе компании с использованием методов социальной инженерии. Оценка уровня знаний сотрудников по вопросам ИБ
Тестирование беспроводных сетей	Анализ возможностей преступника, находящегося в зоне радионаблюдаемости беспроводных сетей компании, но не имеющего к ним санкционированного подключения
Имитация «потерянного» корпоративного устройства	Анализ возможностей потенциального преступника, овладевшего корпоративным мобильным устройством

Внутреннее тестирование на проникновение

Тип тестирования	Описание
Тестирование внутреннего периметра	Оценка возможностей преступника, имеющего санкционированный ограниченный доступ к корпоративной сети, аналогичный уровню доступа рядового пользователя или гостя, имеющего доступ только к гостевому сегменту или же только к сетевой розетке
Тестирование отдельного компонента/системы	WEB-приложения, ERP, СУБД

Внешний pentest предполагает прежде всего тестирование внешнего периметра сети, web-сайтов и спецприложений и т.д. ***Внутренний*** – ориентирован главным образом на внутренние ресурсы

Подходы к проведению *pentest*

По ***объему информации***, предоставляемой аудитору о тестируемой системе *pentest* может проводиться с использованием методов черного (**Black Box**) или белого (**White Box**) ящиков.

По ***уровню информированности*** заказчика о об испытаниях *pentest* может проводиться:

Black Box	**Исполнитель имитирует группу хакеров, которые имеют только название компании и практически нулевые сведения о системе, что является целью исследования. Для реализации поставленной задачи ему необходимы лишь диапазон внешних IP-адресов и, возможно, e-mail адреса внутренних пользователей системы.**
White box	Исполнитель имеет доступ к системам и полную информацию о них. Такая модель тестирования используется как часть организационно-технического аудита организации ИТ и предполагает анализ процессов и процедур.

– с уведомлением администраторов тестируемого объекта (режим **White hat**);

– без уведомления администраторов и специалистов по безопасности тестируемого объекта (режим **Black hat**).

В режиме ***Black Hat*** о проведении работ знают только руководители службы ИБ. При этом задача группы тестировщиков – полностью имитировать действия злоумышленника, действуя максимально незаметно и не оставляя следов. В таком случае удается проверить уровень оперативной готовности к атакам сетевых администраторов и администраторов ИБ.

В режиме ***White Hat*** каких-либо мер для сокрытия атакующих действий не применяется, а исполнители тестов работают в постоянном контакте с ИБ-службой заказчика. Их основная задача сводится к выявлению возможных уязвимостей и оценке риска проникновения в систему.

Структурно-логическая схема и обобщенный алгоритм проведения *pentest*

I этап: состоит в *получении предварительной информации о сети заказчика и планировании проведения теста на проникновение.*

Результатом первого этапа может быть – **формирование карты сети, определение типов устройств, ОС и приложений путем оценки их реакции на внешнее воздействие**

Пассивные методы :

- Google Hacking & Google Cache;
- Shodan и WHOIS інформація;
- Wayback Machine;
- публикации о компании и ее сотрудниках в СМИ;
- сайты поиска работы, пресс-релизы интеграторов;
- страницы сотрудников в социальных сетях, блоги и форумы;
- поиск в физическом мусоре компании – Dumpster Diving.

Активные методы :

- Ping Sweep;
- Fingerprint;
- сканирование портов;
- NetBios Enumeration и SNMP Enumeration;
- LDAP Enumeration и NTP Enumeration;
- SMTP Enumeration и DNS Enumeration;
- социальная инженерия.

II этап: состоит в *поиске, идентификации и проверке возможности использования уязвимостей сетевых служб и приложений*.

При этом проверяется наличие и возможность использования таких уязвимых мест, как:

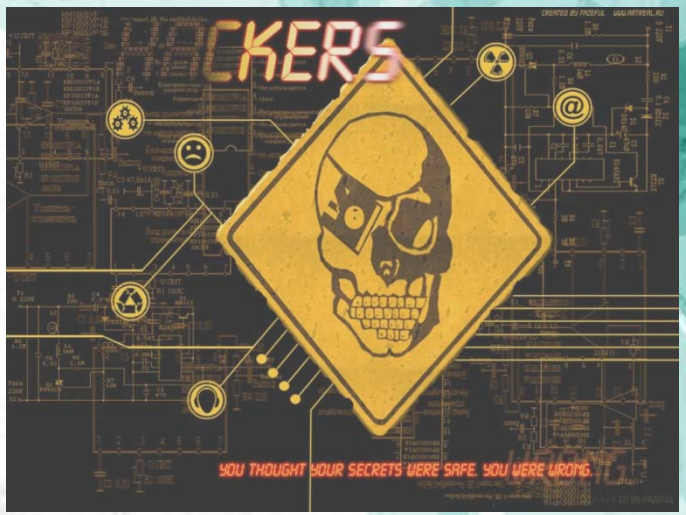
- ✓ SQL Injection (использование операторов SQL);
- ✓ Source code injection (выполнение произвольного кода);
- ✓ OS Commanding (выполнение команд ОС);
- ✓ Client-side Attacks (атак на клиентов);
- ✓ Cross-Site Scripting, XSS (межсайтовое выполнение сценариев);
- ✓ Content Spoofing (подмены содержимого);
- ✓ Buffer Overflow (переполнение буфера);
- ✓ механизмов авторизации и аутентификации и прочее.

Уязвимости, характерные для проведения внутренних тестов

Проверка производится как вручную, так и с использованием различных сканеров уязвимости от компаний MaxPatrol, Nessus, OpenVAC и других (***СЛАЙД № 15***).

Сканеры уязвимостей

Инструмент	Предназначение
Metasploit Framework	Платформа с открытым исходным кодом для разработки, тестирования и эксплуатирования кода
OpenVAS	Фреймворк нескольких служб и инструментов, предлагающих всестороннее и мощное решение по управлению сканированием уязвимостей
Nessus	Выявляет, сканирует и профилирует многочисленные устройства и источники для увеличения безопасности и соответствия в вашей сети
Porkbind	Многопоточный сканер серверов имён, который может рекурсивно делать запросы на сервера имён поддоменов
Canvas	Надёжный фреймворк по разработке эксплойтов для тестеровщиков на проникновение и профессионалов по безопасности
Social-EngineerToolkit (SET)	Стандартный инструментом в арсенале пентестеров, созданный для продвинутых атак на "человеческий фактор
Acunetix	Инструмент созданный для выявления дыр в безопасности веб-приложений. Ищет множество уязвимостей, включая SQL-инъекции, межсайтовый скриптинг и слабые пароли
RIPS	Инструмент, использующий методы статического анализа кода, для поиска уязвимостей в PHP приложениях
Rapid7 NeXpose	Сканер уязвимостей, цель которого поддержать полный жизненный цикл управления уязвимостями, включая обнаружение, выявление, верификацию, классификацию риска, анализ влияния, описание и смягчение
VulnDetector	Нацелен на сканирование веб-сайта. В настоящее время может выявить такие уязвимости как межсайтовый скриптинг (XSS) и SQL-инъекции (SQLI) в веб-скриптах
CAT.NET	Анализатор исполнимого кода. Помогает выявить распространённые варианты определённых преобладающих уязвимостей, которые могут привести к атакам общего вектора, таким как межсайтовый скриптинг (XSS), SQL-инжекты и XPath инжекты.
GFI LanGuard	Сканер безопасности сети и уязвимостей, созданный для помощи в управлениями патчами и сетью, проведения аудита программного обеспечения и оценки уязвимостей
MBSA	Простой в использовании инструмент, предназначенный для IT профессионалов. Помогает малым и средним бизнесам определять состояние их безопасности в соответствии с рекомендациями по безопасности Microsoft и предлагает конкретные рекомендации по итогу проверки.



Веб сканеры

Веб сканеры	
Arachni	Автоматизированная система, которая в полную силу проверяет веб-сайт "на вшивость"
Burp Suite	Интегрированная платформа для выполнения тестирования безопасности веб-приложений
CAL9000	Коллекция инструментов тестирования безопасности веб-приложений, дополненная функциями установки веб-прокси и автоматических сканеров
CAT	Система проведения ручного тестировании на проникновение веб-приложений для более комплексных, требовательных задач в тестировании приложений
DIRB	Сканер веб контента. Он ищет существующие (и/или скрытые) веб объекты. В основе его работы лежит поиск по словарю, он формирует запросы к веб-серверу и анализирует ответ
Fiddler	Отладочный веб-прокси, который записывает весь трафик HTTP(S) между вашим компьютером и Интернетом. Fiddler позволяет инспектировать весь HTTP(S) трафик, устанавливать точки прерывания и "играться" с входящими и исходящими данными
Gamja	Ищет слабые точки — XSS(межсайтовый скриптинг) и SQL-инъекции — а также ошибки валидации URL параметра
Grendel-Scan	Инструмент для автоматического сканирования безопасности веб-приложений. Может быть использован для проведения ручного тестирования на проникновение
HTTrack	Бесплатная и простая в использовании утилита оффлайн браузера. Позволяет загружать сайт из Всемирной Сети на локальный диск, создавать рекурсивную структуру каталогов, получать HTML, картинки и другие файлы с сервера на ваш компьютер
LiLith	Инструмент анализирует веб-страницы в поиска тэга <form>, который обычно перенаправляет на динамичные страницы, на которых можно искать SQL-инъекции и другие слабости
Nikto2	Сканер веб-серверов с открытым исходным кодом (GPL). Выполняет полное тестирование веб-серверов по множеству параметров, включая более 6500 потенциально опасных файлов/CGI
ProxyScan.pl	Инструмент безопасного тестирования на проникновение для сканирования хостов и портов через веб прокси сервер
ScanEx	Утилита, которая запускается против целевого сайта и ищет внешние ссылки и вредоносные кроссдоменные инжекты (выявляет сайты, которые уязвимы к XSS и в которых подложен инжект)
Springenwerk	Сканер безопасности кроссайтового скриптинга (XSS)
Sqlmap	Инструмент для тестирования на проникновение, который автоматизирует процесс выявления и эксплуатирования бреши SQL-инъекций, при этом позволяет получить все данные с сервера БД
Wapiti	Инструмент для аудита безопасности веб-приложений. Выполняет сканирование "чёрный ящик", т.е. он не изучает исходный код приложения, а работает с уже развернутыми сайтами

III этап: состоит в *эксплуатации уязвимостей*

Уязвимости, характерные для проведения внешних тестов по данным компании Positive Technologies

Получив перечень возможных уязвимостей аудитор проводит их эксплуатацию. Методы и инструментарий выбираются индивидуально для каждого типа уязвимости.

TOP 10 наиболее часто используемых паролей

Пароль	Позиция	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Пустая строка	4	0,72%
12345	5	0,47%
7654321	6	0,31%

Особое внимание при этом уделяется :

- подбору паролей в разных сетевых сервисах;
- проведению атак типа «человек по средине» для перехвата паролей пользователей.

Хакерские инструменты для раскрытия паролей

Инструмент	Предназначение
Cain & Abel	Инструмент по восстановлению пароля для операционной системы Microsoft. Позволяет восстановить пароли различного рода посредством прослушивания сети
John the Ripper	Быстрый взломщик паролей. В настоящее время доступен на разного рода Unix, Windows, DOS, BeOS и OpenVMS
Hydra	Очень быстрый взломщик входа по сети. Программа поддерживает множество различных служб
Ncrack	Высокоскоростной инструмент взлома паролей аутентификации. Создан с целью оказания помощи в ходе обеспечения сетевой безопасности
Ophcrack	Взломщик паролей Windows, основанный на радужных таблицах
phrasen|drescher	Модульный и мульти процессный обходчик паролей для их взлома. Поставляется с рядом плагинов, а простые API позволяют простую разработку новых плагинов
Fcrackzip	программа для взлома паролей zip
Enumiax	Инструмент для брут-форса имени пользователя протокола Inter Asterisk Exchange версии 2 (IAX2)
Bruter	Параллельный брутфорсер сетевого входа для Win32. Цель этого инструмента — продемонстрировать важность выбора сильного пароля
The ssh bruteforcer	Инструмент для выполнения атаки по словарю на SSH серверы
Lodowep	Инструмент для анализа стойкости пароля аккаунта в веб-серверной системе Lotus Domino. Инструмент поддерживает как сессионную, так и базовую аутентификацию.
SSHatter	Использует техники брут-форса для определения, как зайти на сервер SSH.

Дополнительные услуги в ходе III-го этапа

По согласованию с заказчиком при тестировании на проникновение, дополнительно, может проводиться проверка:

- базовых работ по контролю защищенности беспроводных сетей;
- внешнего периметра и открытых ресурсов на возможность DOS (DDOS) атак, а также оценки степени устойчивости сетевых элементов и возможного ущерба при их проведении;
- устойчивости сети, путем моделирования атак на протоколы канального уровня STP, VTP, CDP, ARP;
- устойчивости маршрутизации, путем моделирования фальсификации маршрутов и проведение DOS (DDOS) атак против используемых протоколов маршрутизации;
- сетевого трафика, с целью получения, например, паролей пользователей, конфиденциальных документов и пр.;
- возможности получения злоумышленником НСД к конфиденциальной информации или информации ограниченного доступа заказчика (проводится проверкой прав доступа к различным ИР заказчика с привилегиями, полученными на различных этапах тестирования) и.т.д.

IV этап: состоит в *оформлении отчета*

Полученная в ходе анализа уязвимостей и попыток их эксплуатации информация документируется и анализируется с целью выработки рекомендаций в форме отчета, направленного на улучшение защищенности ИТ систем (сетей).

Практика ведения бизнеса в Украине показывает, что наиболее оптимальной структурой отчета является его разбиение на три уровня: для высшего руководства, для менеджеров ИБ и для технических специалистов.

Отчет должен содержать :

- методику проведения теста;
- выводы для руководства, содержащие общую оценку уровня защищенности;
- описание выявленных недостатков системы управления ИБ;
- описание хода тестирования с информацией по всех обнаруженных уязвимостях и результатам их эксплуатации;
- рекомендации по устранению выявленных уязвимостей.

Примеры отчетов о результатах тестирования на проникновение и рекомендаций по их формированию приведены на таких сайтах:

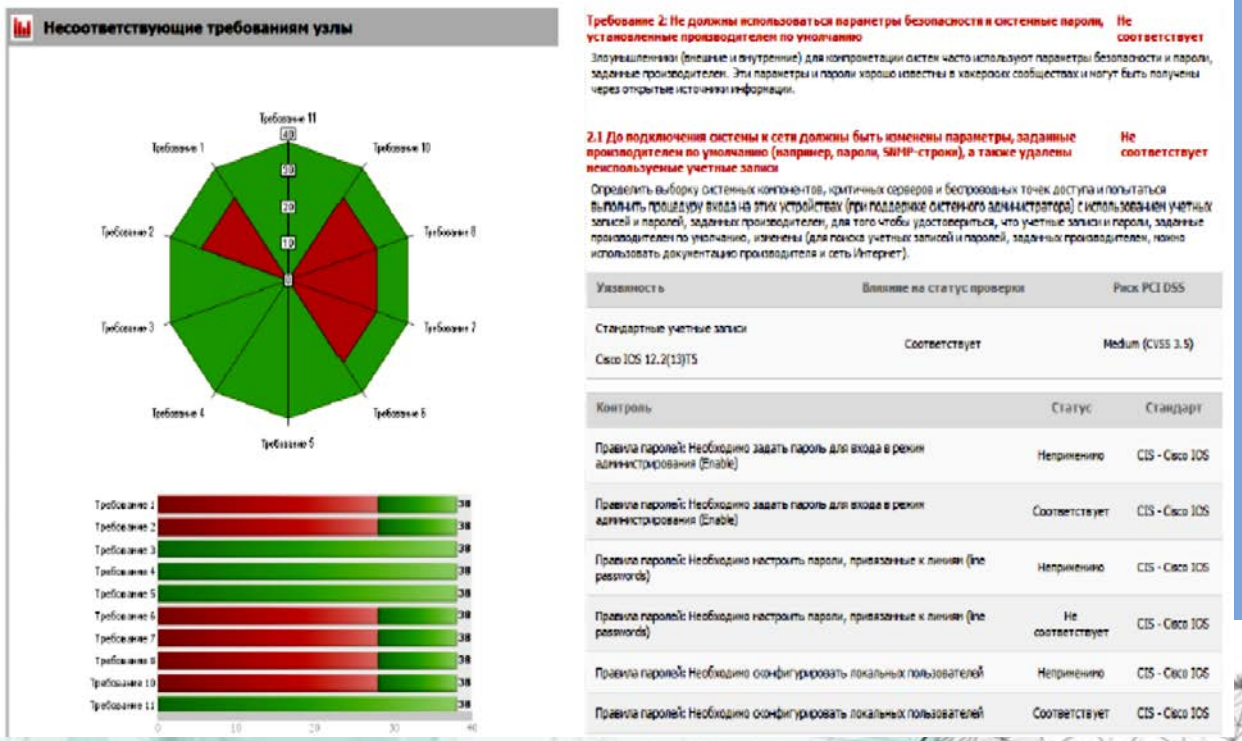
https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf (від Offensive Security, ENG);

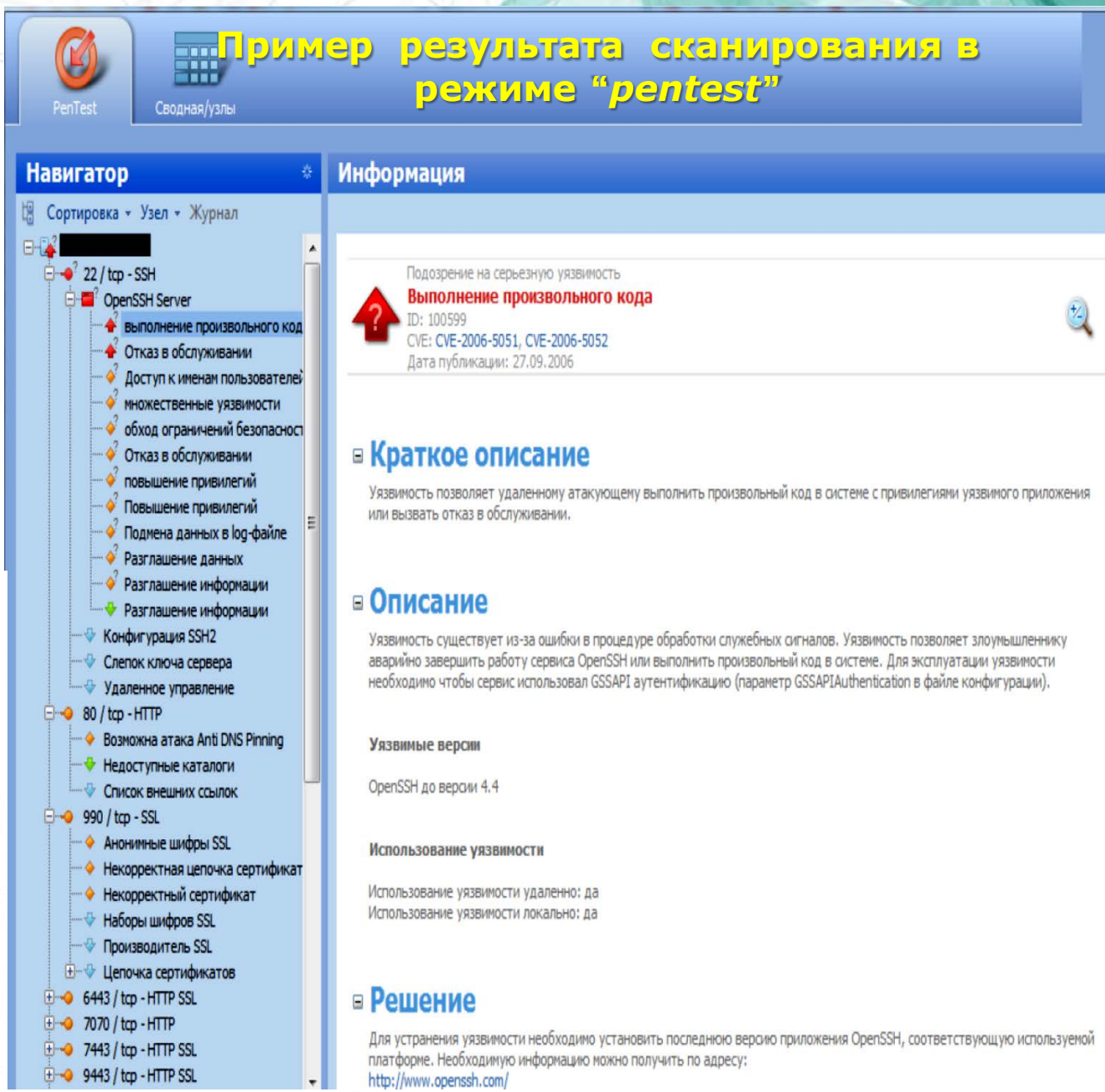
http://www.slideshare.net/devteev/pt-penetration-testing-report-sample (від Positive Technologies, RUS);

https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343 (від Writing a Penetration Testing Report - SANS Institute);

http://resources.infosecinstitute.com/writing-penetration-testing-reports/ (від The Art of Writing Penetration Test Reports).

Вариант отчета о результатах *pentest*, выполненного по методике PCI DSS





с использованием ПО контроля защищенности и соответствия стандартам от компании ***MAXPATROL***

Завершение теста на проникновение и ценовая политика его проведения

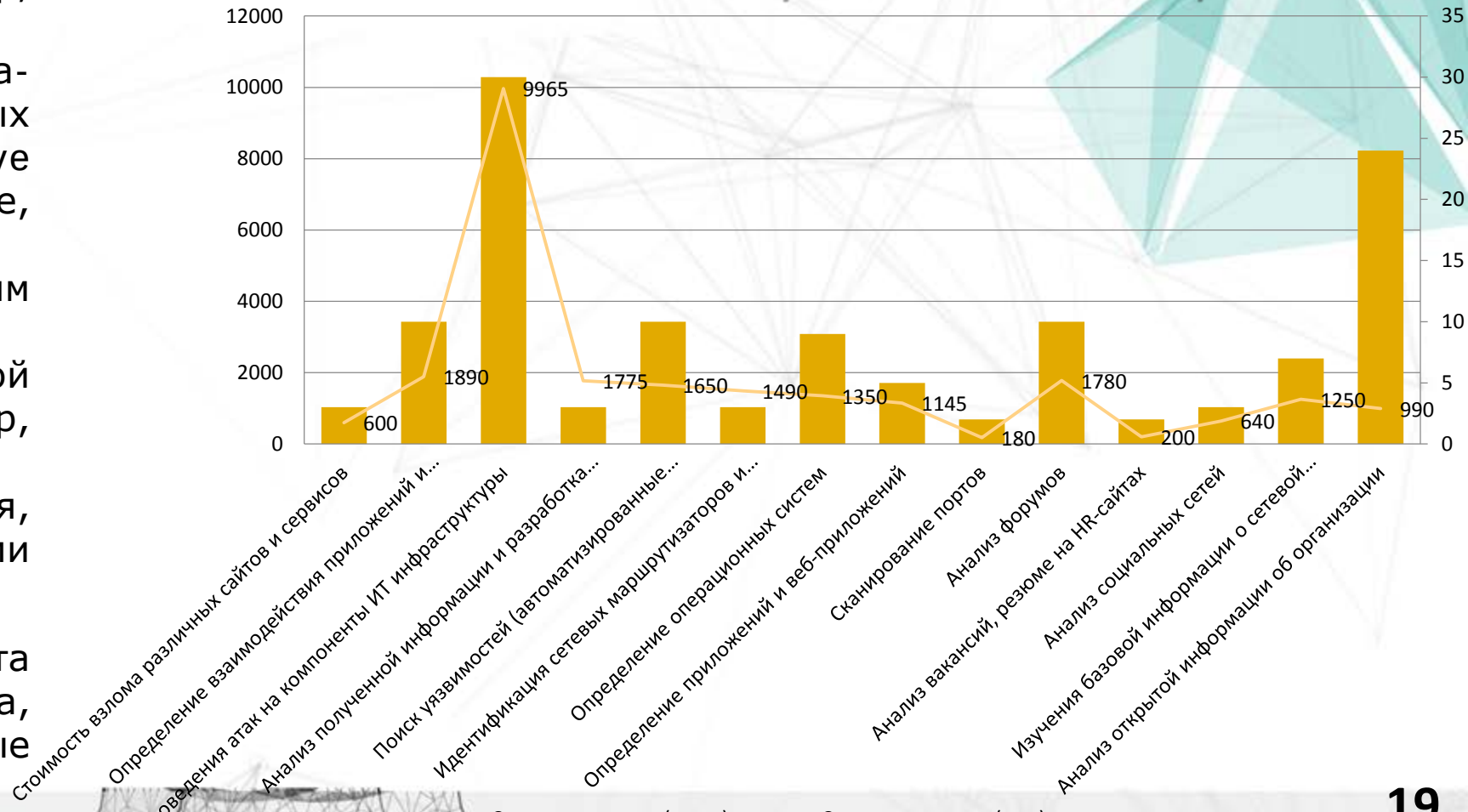
Критерием завершения теста на проникновение является получение:

- ✓ доступа к внутренней сети со стороны сети Интернет;
- ✓ доступа к определенному сегменту сети (например, сегмент АСУ ТП);
- ✓ привилегий в основных инфраструктурных и информационных системах/сервисах (Active Directory, сетевое оборудование, СУБД, ERP и т.п.);
- ✓ доступа к определенным информационным ресурсам;
- ✓ доступа к определенной информации (например, электронная почта директора);
- ✓ первого серьезного сбоя, вызванного действиями аудитора.

После проведения теста возможные остаточные следы теста, так называемые артефакты, которые необходимо устранить.

По состоянию на май - июнь 2016 средняя цена первоначального *pentest* колеблется в районе 50 $, что положительно сказывается для конечного заказчика. Если же компания обращается за проведением информационного аудита - *pentest* всей информационной среды, сумма может достигать сотен тысяч, а для начального корпоративного сайта - тысяч долларов.

Стоимость взлома различных сайтов и сервисов



Подготовка специалистов по *pentest* в Государственном университете телекоммуникаций

№	КУРС	ВИМОГИ (Що студенти мають знати?)	РЕЗУЛЬТАТИ (Що студенти будуть знати?)
1.	**Adv. Network & Cloud security** (secure protocols, network security software, network aspects of clouds, VPN, protocol) *Безпека мережевої інфраструктури*	Стек протоколів OSI, структуру кадрів протоколів TCP, UDP, IP. Ethernet пакет й пакети основних телекомунікаційних технологій. Адресацію. Принципи побудови мереж. Мережеве обладнання. Протоколи сигналізації. Концепцію побудови Cloud систем. Основи криптографії.	Знати уразливості й методи їх застосування в різних телекомунікаційних технологіях. Знати способи боротьби з даними дразливостями, ат також спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки корпоративних мереж. Вміти проектувати захищені (з урахуванням загроз) проводові ТКС. Знати методи організації захищеної передачі даних у незахищеному середовищі.
2.	**Wireless&Mobile security** (Wi-Fi, LTE, Bluetooth ,Alarm system, Broadband system) *Безпека безпроводових і мобільних мереж*	Основні безпроводові технології (Wi-Fi, LTE, Bluetooth, WiMAX, CDMA, GSM, UMTS). Принципи формування й кодування каналів в даних технологіях. Використовувані в них протоколи. Принципи організації доступу до мережі в різних технологіях	Знати уразливості й методи їх застосування в безпроводових і мобільних мережах. Вміти виявляти загрози проникнення або доступу зловмисників до таких мереж. Знати спеціалізоване мережеве обладнання, що застосовується для забезпечення безпеки безпроводових і мобільних мереж. Вміти проектувати захищені (з урахуванням загроз) безпроводові мережі.
3.	**Secure software** (firewalls, software aspect sofclouds, etc) *Програмне забезпечення мережевої безпеки*	Протоколи транспортного й мережевого рівнів системи OSI та структуру їх кадрів. Мови програмування (C++, Java, Assembler). Архітектуру операційних систем. Принципи побудови ТКС.	Знати методи і способи розробки та тестування програмного забезпечення з виявлення і усунення активності, що загрожує безпеці системи (антивіруси, firewalls, сніфери, сканери портів)
4.	**Malware** (OS, AV, malwareanalysis) *Злоякісне програмне забезпечення*	Мови програмування (C++, Java, Assembler). Архітектуру операційних систем.	Вміти проводити семантичний аналіз файлів. Вміти виявляти злоякісне програмне забезпечення й файли за їх структурою та поведінкою. Вміти відновлювати пошкоджену інформацію. Вміти моделювати уразливості ПЗ та використовувати шаблони проектування для захисту ПЗ.
5.	**Websecurity** (PHP, SQL, Server&Client, etc) *Безпека Web*	Архітектуру побудови Web ресурсів. Мови програмування та протоколи, що використовуються при розробці та експлуатації Web ресурсів (PHP, SQL, HTML, HTTP, IP, TCP, UDP, IP, JAVA, JAVAScript).	Знати існуючі уразливості Web ресурсів (sql ін'єкції, брутфорс, xss й т.д) та способи боротьби з ними на етапі розробки та в процесі експлуатації. Знати шаблони проектування безпечних Web додатків.
6.	**Pentest and ethical hacking** (practical aspects) *Тести на проникнення та етичний хакінг*	Існуючі уразливості Web ресурсів (sql ін'єкції, брутфорс, xss й т.д). Архітектуру побудови Web ресурсів, мови та протоколи, що використовуються при розробці та експлуатації Web ресурсів (PHP, SQL, HTML, HTTP, IP, TCP, UDP, IP, JAVA, JAVAScript).	Знати методи і способи тестування мережевих ресурсів на наявність уразливостей безпеки. Вміти знаходити шляхи для їх усунення
7.	**Digital forensic** *Розслідування інцидентів інформаційної безпеки*		Вміти організовувати процеси розслідування інцидентів у відповідності зі стандартами ISO 27001, ISO 20000, ISO/IEC TR 18044, NIST SP 800-61, CMU/SEI-2004-TR-015, ISO 27035, ISO 27037. ISO 27031

В Государственном университете телекоммуникаций подготовка специалистов по *pentest* открыта в 2016 году в рамках международного проекта

"МАГИСТЕРСКАЯ ПРОГРАММА ПОДГОТОВКИ НОВОГО ПОКОЛЕНИЯ ЭКСПЕРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ"

(проект 544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR, 2013 – 2016)

Основанием для этого является соглашение 2013-5084/001-001 о сотрудничестве, заключенное между Украиной и Евросоюзом в 2013 году при поддержке Европейской комиссии: агентства по образованию, культуре и аудиовизуальным средствам (EACEA, Tempus IV).

Целевой группой проекта являются:

1) студенты и преподаватели ведущих высших учебных заведений Германии, Греции, Польши, Украины и Швеции;

2) общественные, государственные и частные организации, которые имеют отношение к отраслям "информационные технологии" и "информационная безопасность".

Цель проекта: создание новой магистерской программы в области информационной безопасности для студентов Европейского союза, как ответа на актуальные проблемы, связанные с киберугрозами, которая основывается на успешном опыте воплощения двойных дипломов среди студентов ЕС, Европейской кредитно-трансферной системы и взаимном признании ученых степеней.

Перечень специализированных программ для подготовки специалистов по *pentest*

Обучение проведению *pentest* в Университете осуществляется как по специализированным программам, так и путем проведения командных соревнований (CTF).

По *первому сценарию* наиболее отработанными являются курсы от компаний EC-Council, Offensive Security и SANS. Они позволяют проводить обучение процедуре проведения *pentest* всех заинтересованных в обеспечении безопасности сетей.

Целью *второго сценария* является обучение участников атаковать чужие и защищать свои ИТ системы (сети) в ходе проведения командной игры.

Обучение и сдача экзаменов – online, кроме обучения по программам AWE и AWAE.

Все экзамены – практические задания.

По завершению обучения обязательным является отчет, составленный на англ.языке.

Сборник ссылок по тематике тестирования на проникновение можно найти в источнике «The Open Penetration Testing Bookmarks Collection». Mind-карту с подбором большого количества online-мест (EnigmaGroup, hACME Game, Hax.Tor, Exploit Exercises и т.д.), а также специализированных образов, виртуальных машин с уязвимостями (Damn Vulnerable Linux, Metasploitable, pWnOS т. д) для обучения – на сайте http://www.amanhardikar.com/mindmaps/Practice.png.

СПЕЦИАЛИЗИРОВАННАЯ ПРОГРАММА	СЕРТИФИКАЦИОННЫЙ ЭКЗАМЕН
Программное обеспечение от компании EC-Council	
Certified Ethical Hacker (CEH)	CEH, тест
Certified Security Analyst (ECSA)	ECSA, тест
Программное обеспечение от компании Offensive Security	
Penetration Testing with Kali Linux (PWK)	Offensive Security Certified Professional (OSCP)
Offensive Security Wireless Attacks (WiFu)	Offensive Security Wireless Professional (OSWP)
Cracking the Perimetr (CTP)	Offensive Security Certified Expert (OSCE)
Advanced Windows Exploitation (AWE)	Offensive Security Exploitation Expert (OSEE)
Advanced Web Attacks & Exploitation (AWAE)	Offensive Security Web Expert (OSWE)
Metasploit Unleashed (MSFU)	---
SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	GIAC Certified Incident Handler (GCIH)
SEC542: Web App Penetration Testing and Ethical Hacking	GIAC Web Application Penetration Tester (GWAPT)
SEC560: Network Penetration Testing and Ethical Hacking	GIAC Penetration Tester (GPEN)
SEC567: Social Engineering for Penetration Testers	---
SEC573: Python for Penetration Testers	---
SEC580: Metasploit Kung Fu for Enterprise Pen Testing	---
SEC617: Wireless Ethical Hacking, Penetration Testing, and Defenses	GIAC Assessing and Auditing Wireless Networks (GAWN)
Программное обеспечение от компании SANS	
SEC642: Advanced Web App Penetration Testing and Ethical Hacking	---
SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
SEC760: Advanced Exploit Development for Penetration Testers	GIAC Penetration Tester (GPEN)
SEC561: Immersive Hands-On Hacking Techniques	---
SEC575: Mobile Device Security and Ethical Hacking	GIAC Mobile Device Security Analyst (GMOB)

Литература для самостоятельной подготовки

ВЫВОДЫ:

1) Согласно выводов, сделанных украинской компанией «Инком» в процессе реализации проектов по созданию / модернизации корпоративных сетей, в ходе *pentest* тестировщикам удается, как правило, получить доступ к:

веб-сайтам – в 50% случаев;
электронной почте – в 40% случаев;
бизнес-программам – в 35% случаев;
IP телефонии – в 10% случаев;
систем дистан.банк.обслуж. – в 29%.

Полный контроль над инфраструктурой может быть получен ими не более чем в 25% проектов, а в 5% – тестировщикам вообще не удается преодолеть периметр.

2) К самым популярным эксплойтам эксперты в области информационной безопасности в последнее время относят:

–межсетевое выполнение сценариев (50%);
–наличие интерфейса удален.управл(47%);
–доступная информация о приложениях (45%);
–внедрение SQL кода (63%)

ВЫВОДЫ:

3) *Самой популярной уязвимостью по выводам экспертов сейчас являются простые пароли администраторов*. Они встречаются в 80% проектов, иногда даже в тех случаях, когда в организациями были внедрены политики по обеспечению сложности паролей для рядовых пользователей.

Уязвимости веб-приложений и *некорректно настроенное оборудование* несут за собой значительно меньшие риски, и поэтому являются ключом к взлому соответственно в 46% и 38% случаях.

Отсутствие обновлений способствует успешному проведению тестовых атак в 25% компаний, а *недостатки архитектуры* – в 9 %.

4) Учитывая такое, именно проведение *pentest* позволит:

– *узнать возможности осуществления угроз безопасности информации;*
– *оценить последствия направленной хакерской атаки;*
– *определить уязвимости в защите информационной системы;*
– *оценить эффективность средств защиты информации;*
– *оценить эффективность менеджмента информационной безопасности;*
– *оценить вероятный уровень квалификации нарушителя для успешной реализации атаки;*
– *получить аргументы для обоснования дальнейшего вложения ресурсов в ИБ;*
– *выработать список контрмер, с тем чтобы снизить возможность реализации атак.*

5) Несмотря на довольно частую критику *pentest*, технология реализации которого не может гарантировать заказчику того, что:

– тестировщик обнаружил все «дыры» в системе его безопасности;
– найденные тестировщиком «дыры» не будут впоследствии использованы для завладения его информацией;
– деятельность тестировщика может быть им полностью проконтролирована,

- в условиях современной информационной и кибервойны, которая ведется против нашей страны, **задача по обеспечению безопасности информационных систем на объектах информационной деятельности и, прежде всего, ИТ систем (сетей) органов власти и критических инфраструктур** (социальных фондов и различных государственных реестров), **а также объективной оценки уровня безопасности этих структур без проведения *pentest* практически НЕ ВЫПОЛНИМА**.

Спасибо за внимание!

Список использованной литературы:

1. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Складанний П.М., Бурячок В.Л., Гулак Г.М., Козачок В.А./ Науковий журнал «Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №3(43). с. 48 – 61
2. Статистика уязвимостей web-приложений за 2015 год. [Электрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/ru-ru/download/WASS-SS-2015-ru.pdf
3. Безопасность АСУ ТП в цифрах. [Электрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf
4. Дмитрий Каталков. Уязвимости корпоративных информационных систем в 2015 году. [Электрон. ресурс]: – Режим доступа: https://www.ptsecurity.com/ru-ru/ics /Webinar_14042016.pdf
5. Бурячок В.Л. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах / Козачок В.А, Бурячок Л.В., Складанний П.М./Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. №3, 2015, с.4–12
6. Контроль защищенности и соответствия стандартам Positive Technologies. [Электрон. ресурс]: – Режим доступа: ftp://ftp.software.ibm.com/software/security/ products/qradar/documents /iTeamaddendum/m_vuln_MaxPatrol.pdf
7. Бурячок В.Л. Аналіз сучасних вимог до створення парольних політик корпоративних користувачів /Борсуковський Ю.В., Складанний П.М./ Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 3, 2016, с. 72 – 76
8. Впровадження європейської кібербезпеки:загальний огляд. [Электрон. ресурс]: – Режим доступа: http://www.isaca.org/Knowledge-Center/Research/Documents /European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf
9. А.Дорофеев. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? [Электрон. ресурс]: – Режим доступа: http://elibrary.ru/item.asp?id=23143917
10. В.Лепихин. Сравнительный анализ сканеров безопасности. [Электрон. ресурс]: – Режим доступа: http://www.itsecurity.ru/news/reliase/2008/12_22_08.htm
11. Бурячок В.Л. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 C MIMO / Астапеня В. М., Соколов В. Ю. / Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 2, 2016, с. 60 – 68