

Лабораторная работа №4

Администрирование межсетевого экрана



ПОЛИТЕХ

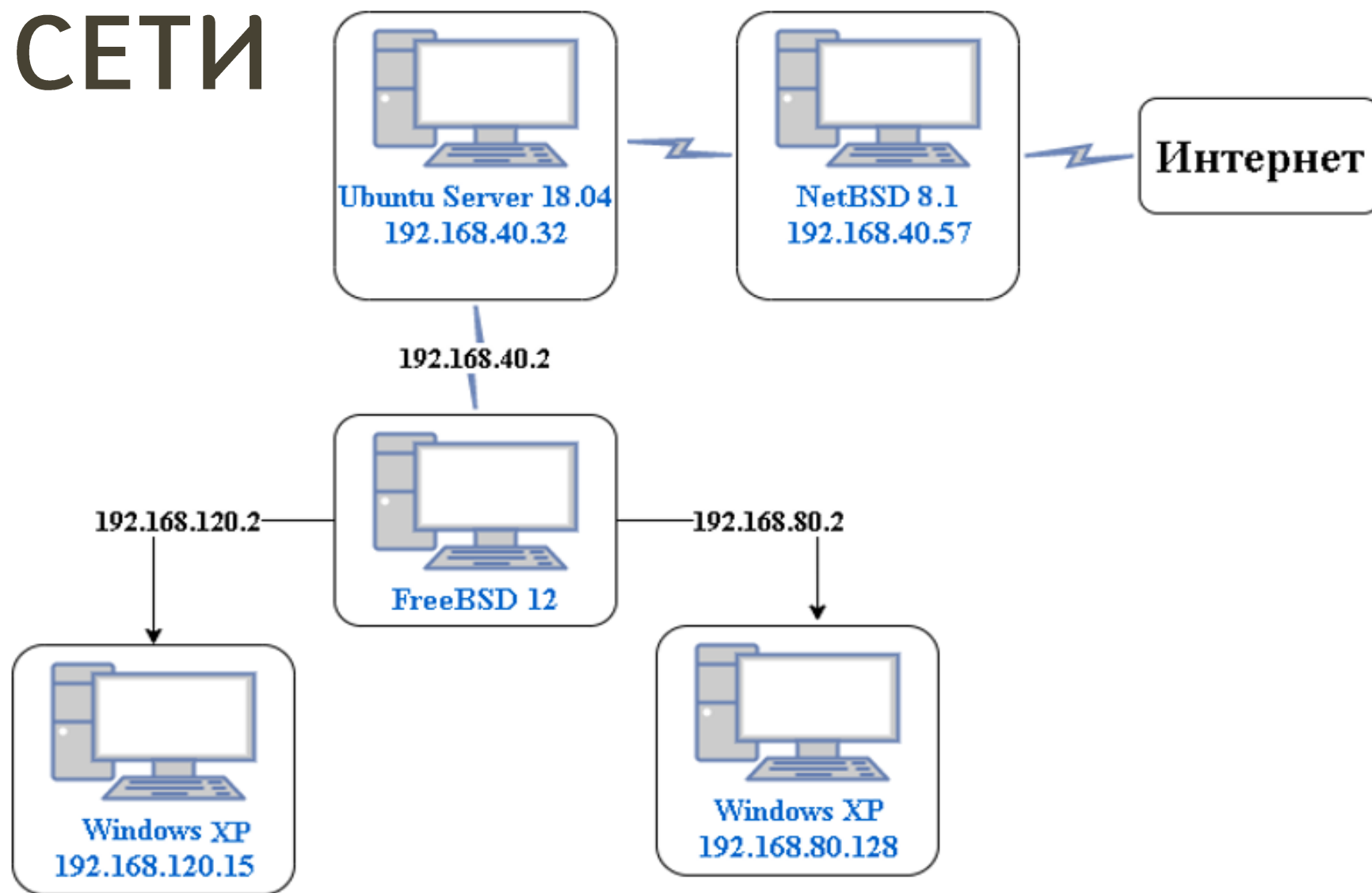
Санкт-Петербургский
политехнический университет
Петра Великого

Бараев Дамир
Группа: 3540901/02001

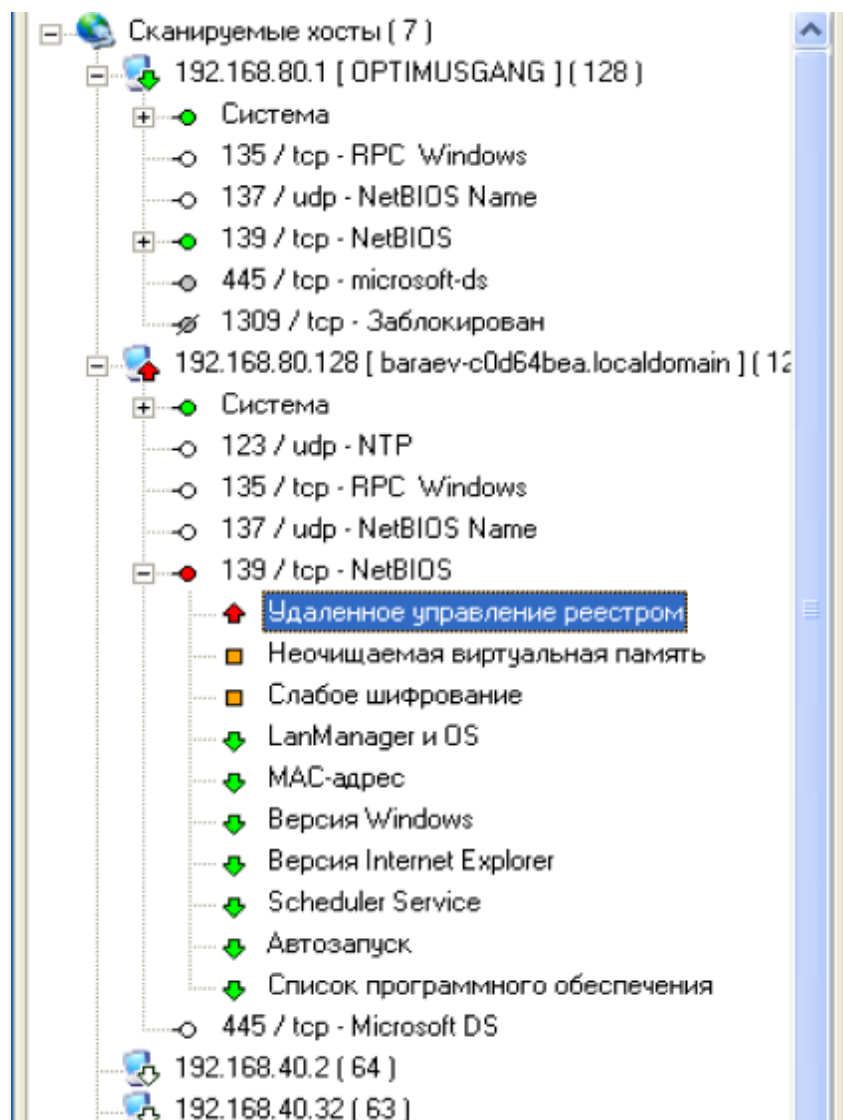
ЦЕЛИ РАБОТЫ

1. Устранение уязвимостей сетей
2. Установка межсетевого экрана

СХЕМА СЕТИ



XSPIDER. РЕЗУЛЬТАТЫ СКАНИРОВАНИЯ



серьезная уязвимость

Удаленное управление реестром

Описание

Эта уязвимость существует только в том случае, если Вы не являетесь Администратором на проверяемом хосте.

Возможен полный доступ к реестру хоста.

Решение

Отключить возможность удаленного управления реестром.

ОТКЛЮЧЕНИЕ УДАЛЕННОГО УПРАВЛЕНИЯ РЕЕСТРОМ

Службы (локальные)

Удаленный реестр

[Остановить](#) службу
[Перезапустить](#) службу

Описание:

Позволяет удаленным пользователям изменять параметры реестра на этом компьютере. Если эта служба остановлена, реестр может быть изменен только локальными пользователями, работающими на этом компьютере. Если эта служба отключена, любые службы, которые явно зависят от нее, не могут быть запущены.

Имя	Описание	Состояние	Тип запуска	Вход от имени
Служба времени ...	Управле...	Работает	Авто	Локальная сис...
Служба загрузки ...				
Служба индексир...				
Служба обеспече...				
Служба обнаруже...				
Служба протокол...				
Служба регистра...				
Служба серийных ...				
Служба сетевого ...				
Служба сетевого ...				
Служба сообщений				
Служба управлен...				
Служба шлюза ур...				
Службы IPSEC				
Службы криптогр...				
Службы терминалов				
Смарт-карты				
Совместимость бы...				
Справка и поддер...				
Съемные ЗУ				
Телефония				
Темы				
Теневое копирова...				
Уведомление о си...				
Удаленный вызов...				
Удаленный реестр				
Узел универсальн...				
Управление прило...				
Фоновая интелле...				

Удаленный реестр (Локальный компьютер) - свойства

Общие | Вход в систему | Восстановление | Зависимости

Имя службы: RemoteRegistry

Выводимое имя: Удаленный реестр

Описание: Позволяет удаленным пользователям изменять параметры реестра на этом

Исполняемый файл: C:\WINDOWS\system32\svchost.exe -k LocalService

Тип запуска: Отключено

Состояние: Работает

Пуск | **Стоп** | Пауза | Продолжить

Можно указать параметры запуска, применяемые при запуске службы из этого диалога.

Параметры запуска:

OK | Отмена | Применить

ОЧИСТКА ВИРТУАЛЬНОЙ ПАМЯТИ

The screenshot shows the 'Локальные параметры безопасности' (Local Security Policy) window. The left sidebar shows the tree structure with 'Политики безопасности' (Security Policies) expanded. The main pane displays a list of policies. The policy 'Завершение работы: очистка страничного файла виртуальной памяти' (End task: cleanup of the virtual memory pagefile) is selected and highlighted. A right-hand pane titled 'Свойства: Завершение работы: очистка страничного файла виртуальной памяти' (Properties: End task: cleanup of the virtual memory pagefile) shows the policy status as 'Отключен' (Disabled) and provides options to 'Включить' (Enable) or 'Отключить' (Disable).

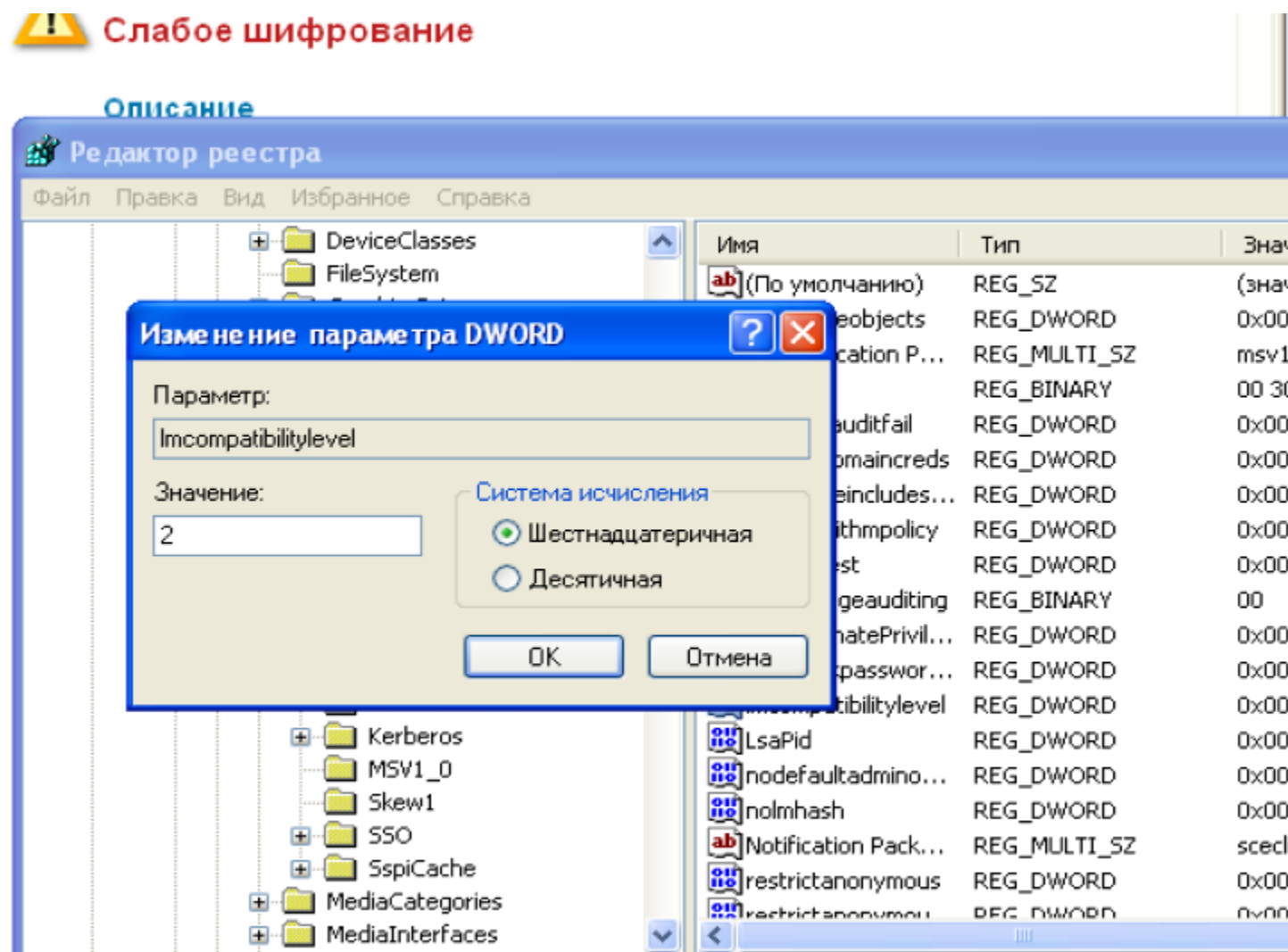
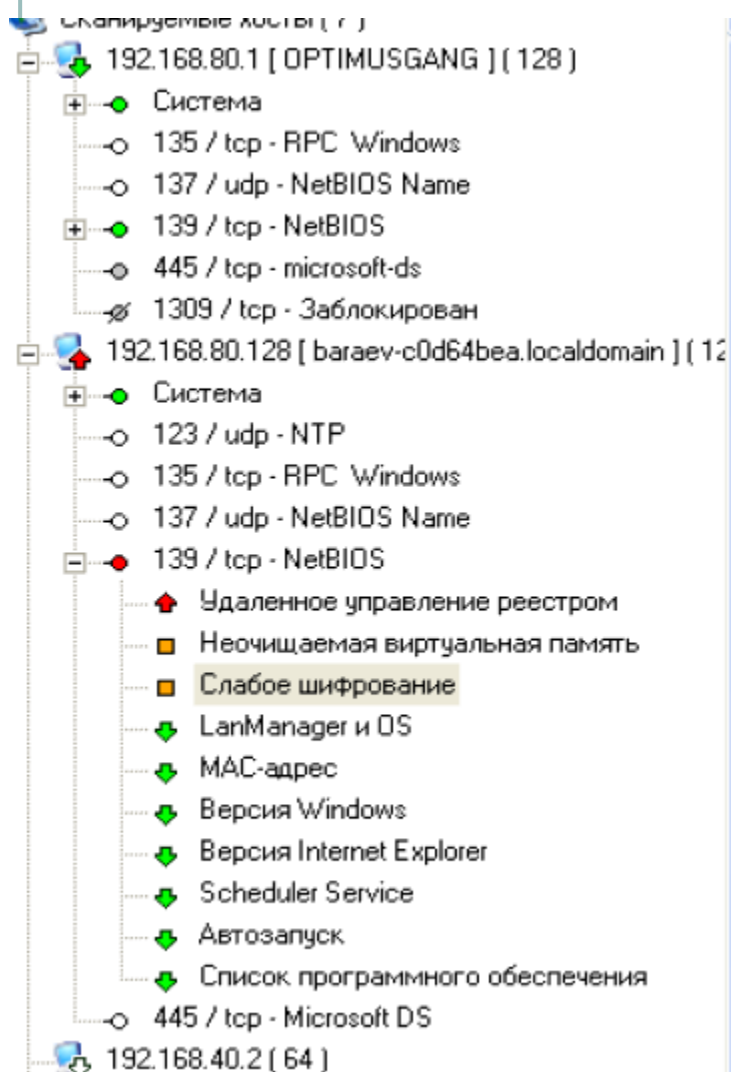
Политика	Параметр безопасности
DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Secu...	Не определен
DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Secu...	Не определен
Аудит: аудит доступа глобальных системных объектов	Отключен
Аудит: аудит прав на архивацию и восстановление	Отключен
Аудит: немедленное отключение системы, если невозможно внести ...	Отключен
Доступ к сети: Разрешить трансляцию анонимного SID в имя	Отключен
Завершение работы: очистка страничного файла виртуальной памяти	Отключен
Завершение работы: разрешить завершение работы системы без вы...	Включен
Интерактивный вход в систему: поведение при извлечении смарт-к...	Нет действия
Интерактивный вход в систему: требовать смарт-карту	Не определен
Интерактивный вход в систему: заголовок сообщения для пользова...	Не определен
Интерактивный вход в систему: количество предыдущих подключе...	10 Входы в с
Интерактивный вход в систему: напоминать пользователям об исте...	14 дн.
Интерактивный вход в систему: не отображать последнего имени п...	Отключен
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Не определен
Интерактивный вход в систему: отображать сведения о пользовате...	Не определен

Свойства: Завершение работы: очистка страничного файла виртуальной памяти

Параметр локальной безопасности: ☒ Включить ☐ Отключить

Объяснение параметра: Завершение работы: очистка страничного файла виртуальной памяти

ИЗМЕНЕНИЕ УЯЗВИМОСТИ ШИФРОВАНИЯ



НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА

```
root@:~ # cat /etc/rc.conf
hostname=""
#sshd_enable="YES"
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable
dhcpd_enable="YES"
dhcpd_flags="-q"
dhcpd_ifaces="em2"
dhcpd_conf="/etc/dhcpd.conf"
firewall_enable="YES"
firewall_type="usr/fw_rules/ruleFile"
dumpdev="AUTO"
gateway_enable="YES"
defaultrouter="192.168.40.57"
ifconfig_em0="192.168.40.2 netmask 255.255.255.0"
ifconfig_em1="192.168.80.2 netmask 255.255.255.0"
ifconfig_em2="192.168.120.2 netmask 255.255.255.0"
ipnat_enable="YES"
```


ВЫВОДЫ

В ходе данной лабораторной работы были устранены уязвимости системы Windows XP. Также была произведена настройка межсетевого экрана.