Гомельский Государственный Университет

им. Ф. Скорины

Лабораторная работа №4.
Идентификация операционных систем

Проверил:

Грищенко В.В.

Студент МС – 42:

Черненок А.В.

г. Гомель

Цель работы: Целью лабораторной работы является обучение современным методам и средствам идентификации ОС анализируемой КС.

Постановка задачи

Выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

Последовательность действий

Шаг 1. Загрузить виртуальную машину. Войти в систему. Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.

```
breof@breof-80ru:~$ sudo apt install tcpdump
[sudo] пароль для breof:
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Уже установлен пакет tcpdump самой новой версии (4.9.3-4).
tcpdump помечен как установленный вручную.
Starting pkgProblemResolver with broken count: 0
Starting 2 pkgProblemResolver with broken count: 0
Done
Следующие пакеты устанавливались автоматически и больше не требуются:
  firebird3.0-common firebird3.0-common-doc firebird3.0-server-core firebird3.0-utils
  fonts-crosextra-caladea fonts-crosextra-carlito fonts-dejavu fonts-liberation2
  fonts-linuxlibertine fonts-noto-extra fonts-opensymbol fonts-sil-gentium
  fonts-sil-gentium-basic gstreamer1.0-gl gstreamer1.0-gtk3 libabw-0.1-1
  libboost-date-time1.71.0 libboost-filesystem1.71.0 libboost-iostreams1.71.0
  libboost-locale1.71.0 libboost-thread1.71.0 libbsh-java libcdr-0.1-1
  libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5 libcommons-logging-java
  libe-book-0.1-1 libeot0 libepubgen-0.1-1 libetonyek-0.1-1 libexttextcat-2.0-0
  libexttextcat-data libfbclient2 libfreehand-0.1-1 libgraphene-1.0-0
  libgstreamer-gl1.0-0 libharfbuzz-icu0 libhyphen0 libib-util libjuh-java libjurt-java
  liblangtag-common liblangtag1 libmhash2 libmspub-0.1-1 libmwaw-0.3-3 libmythes-1.2-0
  libneon27-gnutls libodfgen-0.1-1 liborcus-0.15-0 libpagemaker-0.0-0 libpq5
  libraptor2-0 librasqal3 librdf0 libreoffice-base libreoffice-base-core
  libreoffice-base-drivers libreoffice-calc libreoffice-common libreoffice-core
  libreoffice-draw libreoffice-gnome libreoffice-gtk3 libreoffice-impress
  libreoffice-java-common libreoffice-math libreoffice-nlpsolver
  libreoffice-report-builder libreoffice-report-builder-bin
  libreoffice-script-provider-bsh libreoffice-script-provider-js
  libreoffice-script-provider-python libreoffice-sdbc-firebird libreoffice-sdbc-mysql
  libreoffice-sdbc-postgresql libreoffice-style-colibre libreoffice-style-elementary
  libreoffice-style-tango libreoffice-wiki-publisher libreoffice-writer librevenge-0.0-0
  libridl-java libuno-cppu3 libuno-cppuhelpergcc3-3 libuno-purpenvhelpergcc3-3
  libuno-sal3 libuno-salhelpergcc3-3 libunoil-java libunoloader-java libvisio-0.1-1
  libwpd-0.10-10 libwpg-0.3-3 libwps-0.4-4 libxmlsec1 libxmlsec1-nss libyajl2 lp-solve
  python3-uno uno-libs-private ure
Для их удаления используйте «sudo apt autoremove».
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 455 п
акетов не обновлено.
breof@breof-80ru:~$ sudo tcpdump -D
1.wlp2s0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.enp3s0 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.bluetooth0 (Bluetooth adapter number 0) [none]
```

Шаг 2. С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

```
breof@breof-80ru:~$ nmap -O 127.0.0.1 -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-18 20:38 +03
Failed to resolve "-O".
Failed to resolve "-vv".
Failed to resolve "-vv".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp

Failed to resolve "-vv".
Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Шаг 3. С помощью сетевого сканера xprobe выполнить идентификацию ОС с использованием опроса модуля ICMP:
xprobe2 127.0.0.1

```
breof@breof-80ru:~$ sudo xprobe2 127.0.0.1

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 127.0.0.1
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping  -  ICMP echo discovery module
[x] [2] ping:tcp_ping  -  TCP-based ping discovery module
[x] [3] ping:udp_ping  -  UDP-based ping discovery module
[x] [4] infogather:ttl_calc  -  TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan  -  TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo  -  ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp  -  ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask  -  ICMP Address mask request fingerprinting module
[x] [9] fingerprint:icmp_port_unreach  -  ICMP port unreachable fingerprinting module
[x] [10] fingerprint:tcp_hshake  -  TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst  -  TCP RST fingerprinting module
[x] [12] fingerprint:smb  -  SMB fingerprinting module
[x] [13] fingerprint:snmp  -  SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 127.0.0.1. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 127.0.0.1. Module test failed
[-] No distance calculation. 127.0.0.1 appears to be dead or no ports known
[+] Host: 127.0.0.1 is up (Guess probability: 50%)
[+] Target: 127.0.0.1 is alive. Round-Trip Time: 0.47509 sec
[+] Selected safe Round-Trip Time value is: 0.95018 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Other guesses:
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Host 127.0.0.1 Running OS: @:\c@U (Guess probability: 95%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

Шаг 4. На узле TWS2 перейти в консоль XSpider. Обратить внимание на результаты определения ОС в ходе предыдущих сканирований. В используемом профиле сократить диапазон портов до 1–30 и выполнить повторное сканирование.

В профили сканирования включить опции «Искать уязвимости», «Искать скрытые каталоги». Выполнить сканирование. Убедиться в том, что ОС идентифицирована.