Exercise 4
More Enumeration Techniques

Team 1

Initial Configuration

You are to set up at least three machines.

Machine #1
- Windows 2000 machine (SP2).
- SNMP should be enabled, with the default community string “public”.
- Add an interesting collection of shares and users.

Machine #2
- Red Hat 7.3 Machine
- rlogin, finger, and nfs should be enabled
- You should have a regular user account called user.
- The directory /home/user should be exported to 10.0.0.* with full read-write permission.

Machine #3
- Windows 2000 machine. (No SP)
- Null connections must be permitted, but may be restricted.
- IIS must be running.
- Add an interesting collection of shares and users.

General Instructions
- You may run as many other additional machines as you wish.
- Each of these additional machines may run any collection of services you wish.
- For all machines, all services that are running must be run on standard ports.

Offense (1/3 Credit)
- For each active machine, try to determine
  - The OS
  - The accounts
  - The open ports
  - The available shares

Defense
- Who scanned your machine?
- What did they discover?

Exercise 4
More Enumeration Techniques

Team 2

Initial Configuration
You are to set up at least three machines.

Machine #1
- Windows 2000 machine (SP2).
- SNMP should be enabled, with the default community string “public”.
- Add an interesting collection of shares and users.

Machine #2
- Red Hat 7.3 Machine
- rlogin, finger, and nfs should be enabled
- You should have a regular user account called user.
- The directory /home/user should be exported to 10.0.0.* with full read-write permission.

Machine #3
- Windows 2000 machine (No SP).
- Null connections must be permitted, but may be restricted.
- IIS must be running.
- Add an interesting collection of shares and users.

General Instructions
- You may run as many other additional machines as you wish.
- Each of these additional machines may run any collection of services you wish.
- For all machines, all services that are running must be run on standard ports.

Offense (1/3 Credit)
- For each active machine, try to determine
  - The OS
  - The accounts
  - The open ports
  - The available shares

Defense
- Who scanned your machine?
- What did they discover?

Exercise 4
More Enumeration Techniques

Team 3

Initial Configuration
You are to set up at least three machines.

Machine #1
- Windows 2000 machine (SP2)
- SNMP should be enabled, with the default community string “public”.
- Add an interesting collection of shares and users.
Machine #2
  • Red Hat 7.3 Machine
  • rlogin, finger, and nfs should be enabled
  • You should have a regular user account called user.
  • The directory /home/user should be exported to 10.0.0.* with full read-write permission.

Machine #3
  • Windows 2000 machine. (No SP)
  • Null connections must be permitted, but may be restricted.
  • IIS must be running.
  • Add an interesting collection of shares and users.

General Instructions
  • You may run as many other additional machines as you wish.
  • Each of these additional machines may run any collection of services you wish.
  • For all machines, all services that are running must be run on standard ports.

Offense (1/3 Credit)
  • For each active machine, try to determine
    • The OS
    • The accounts
    • The open ports
    • The available shares

Defense
  • Who scanned your machine?
  • What did they discover?

Exercise 4
  More Enumeration Techniques

Team 4

Initial Configuration

You are to set up at least three machines.

Machine #1
  • Windows 2000 machine. (SP2)
  • SNMP should be enabled, with the default community string “public”.
  • Add an interesting collection of shares and users.

Machine #2
  • Red Hat 7.3 Machine
  • rlogin, finger, and nfs should be enabled
  • You should have a regular user account called user.
  • The directory /home/user should be exported to 10.0.0.* with full read-write
permission.

Machine #3
- Windows 2000 machine. (No SP)
- Null connections must be permitted, but may be restricted.
- IIS must be running.
- Add an interesting collection of shares and users.

General Instructions
- You may run as many other additional machines as you wish.
- Each of these additional machines may run any collection of services you wish.
- For all machines, all services that are running must be run on standard ports.

Offense (1/3 Credit)
- For each active machine, try to determine
  - The OS
  - The accounts
  - The open ports
  - The available shares

Defense
- Who scanned your machine?
- What did they discover?