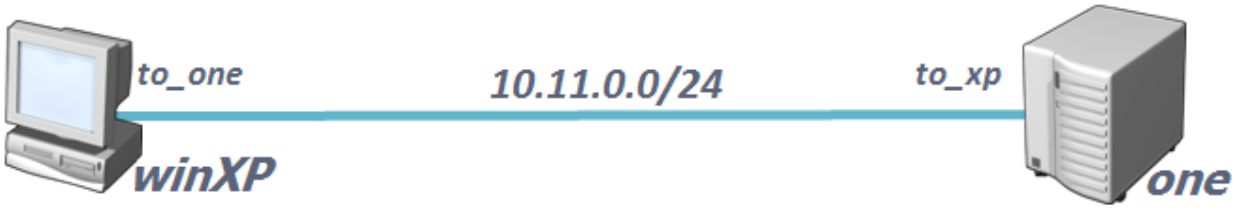
Laborator 6 – Monitorizare

➢ Topologie



Toate exerciţiile se vor realiza pe maşina virtuală “One”, ultimele patru exerciţii vor avea nevoie şi de calculatorul winXP.

➢ Event Viewer

1. [1 punct] Să se deschidă utilitarul Task Manager și editorul de fișiere Notepad. În Notepad scrieți un text aleatoriu (de exemplu „ana are mere”), după care închideți procesul notepad.exe folosind Task Manager.

2. [1 punct] Încercaţi să accesaţi site-ul mssr.cs.pub.ro. Folosind Event Viewer descoperiţi din fereastra Windows Logs -> System motivul pentru care accesarea acestui site nu este posibilă.

➢ Audit

3. [1 punct] Prin intermediul “Security Local Policy”, activaţi politica de *Audit object access* din *Local Policies / Audit Policy,* pentru auditarea oricărui tip de acces.

4. [1 punct] Creați un director numit *audit*. Pentru auditarea accesului la acest director, intrați în proprietățile lui, și din tab-ul *Security* deschideți proprietățile avansate. Din tab-ul *Auditing* adăugați utilizatorul cu care sunteți autentificat ce va fi auditat cu control deplin. După terminarea acestui pas, folosind Event Viewer, descoperiți evenimentul creat în urma accesării directorului. (HINT: Windows Logs/Security).

➢ Reliability and Performance Monitor

5. [1 punct] Folosind Performance Monitor, adăugați contoare referitoare la memorie : *Page Faults/sec, Pages/sec, Available Mbytes*. (HINT: Vezi curs, slide 15-17)

6. [1 punct] Creați un nou Data Collector Set definit de utilizator cu numele audit6. În interiorul acestuia creați un nou Data Collector care să includă contoare referitoare la procesor :

Processor time, Processor Queue Length, Queue Length, Interrupts/sec. (HINT: Vezi curs, slide 13-14) Creați și analizați raportul.

7. [1 punct] Folosind Reliability Monitor, analizați starea de stabilitate a serverului. Care este nota actuală a sistemului?

➢ Microsoft Network Monitor

8. [1 punct] Creați o nouă regulă custom de firewall, pe calculatorul "One", denumită *rule_imcp,* care să permită ping-ul venit de la calculatorul winXP. După aplicarea regulii de firewall, activaţi log-urile pentru profilul curent şi observaţi cum se realizează logarea datelor. (HINT: Properties pe Windows Firewall with Advanced Security).

9. [1 punct] Descărcați de pe site-ul oficial utilitarul Microsoft Network Monitor 3.3 și instalați-l pe serverul One. (http://www.microsoft.com/downloads/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f&displaylang=en)

10. [1 punct] De pe mașina XP dați ping în One și începeți monitorizarea pachetelor ICMP folosind utilitarul de mai sus. (HINT: Pentru un ping funcțional nu uitați să dezactivați firewall-ul de pe XP)

11. [1 punct] Creați o politică IPSec pentru criptarea traficului de tip ICMP dintre calculatoarele winXP şi serverul One.

12. [1 punct] Monitorizaţi pachetele ICMP folosind utilitarul de mai sus. Care este formatul în care sunt afişate datele?