

CURSO: Segurança da Informação

DISCIPLINA	Laboratório de Administração de Sistemas Operacionais de Redes (SEGMA3)				PROFESSOR (A)	Ms. Claudio Cura Jr	
ALUNO (A) Nome completo	Enzo Arrue Juan Fuso					RA	1680972411029
CICLO (SEMESTRE)	3	TURNO	Matutino	DATA	25/03/2025	NOTA	
Relatório: ATIVIDADE 3 - INSTRUMENTAÇÃO							

- 1) Obter através de linha de comando o último evento de ligar/startup do computador, e o último evento de desligar/shutdown

2)

R: de inicio de sistema: wevtutil qe System /f:text /q:"*[System[(EventID=6005)]]" /c:1

De desligamento: wevtutil qe System /f:text /q:"*[System[(EventID=6006)]]" /c:1

- 3) Obter através de linha de comando todos os processos em execução no sistema operacional, incluindo a quantidade de memória utilizada por cada processo, e o tempo de ocupação do processador.

R: wmic process get name, kernelmodetime, workingsetsize

- 4) Obter através de linha de comando lista contendo somente os serviços de rede em execução no sistema operacional, sem mais nenhuma informação adicional.

R: wmic service where "name like '%net%'" get name

- 5) Fabricante do computador, modelo do computador, nome do computador, nome do usuário logado, tipo da arquitetura (x86 ou x64), quantidade total de memória

R: wmic computersystem get manufacturer, model, name, username, systemtype, totalphysicalmemory

- 6) Modelo do processador, tipo do socket, número de núcleos físicos, número de núcleos lógicos

R: wmic cpu get name, socketdesignation, numberofcores, numberoflogicalprocessors

- 7) Quantidade de módulos de memória, a capacidade de cada módulo, fabricante, código do modelo, número de série, velocidade, ECC ou não ECC, single-channel ou dual-channel

R: wmic memorychip get banklabel, capacity, manufacturer, partnumber, serialnumber, speed, memorytype

- 8) Versão do sistema operacional, data de instalação, data do último boot, data atual (formatar corretamente data e horário no relatório)

R: wmic os get caption, installdate, lastbootuptime

- 9) Lista de todos os softwares instalados, versão, fabricante

R: wmic product get name,version,vendor

- 10) Obter a lista de todos os softwares que são carregados automaticamente ao iniciar

R: wmic startup get caption,command

- 11) Obter a lista de atualizações do sistema operacional (hotfix pacotes KB)

R wmic qfe list brief /format:table