COMP 012 - Network Administration

Windows + Linux + Packet Tracer + Python Automation

SESSION 11: PYTHON FOR CYBERSECURITY

ACTIVITY 11.1: NETWORK SCANNING WITH PYTHON

Topic: Building network reconnaissance tools

Description: Create Python tools for network discovery and scanning

INSTRUCTIONS:

Install required libraries:
- pip install scapy python-nmap

Build network scanner:
- ARP scan for local network discovery
- Identify live hosts
- Detect MAC addresses and vendors

Port scanning techniques:
- TCP Connect scan
- SYN scan (requires root/admin)
- Service version detection

Using python-nmap:
- Wrapper for nmap functionality
- Scan target for open ports
- Detect services and versions
- Parse and display results

Create comprehensive scanner:
- Input: Target IP or range
- Output: Live hosts, open ports, services
- Export results to JSON/CSV
- Add command-line arguments

Note: Only scan networks you own/have permission

Deliverables: Submit network scanner script with sample output	**35 Points**

ACTIVITY 11.2: PACKET CAPTURE AND ANALYSIS

Topic: Capturing and analyzing network traffic with Python

Description: Build packet capture tools for network analysis

INSTRUCTIONS:

Using Scapy for packet capture:
- from scapy.all import *
- sniff() function basics

• Filtering packets (BPF filters)

Build packet analyzer:

• Capture packets on interface

• Filter by protocol (TCP, UDP, ICMP)

• Extract: src IP, dst IP, ports

• Display packet summary

Create specific analyzers:

Tool 1 - HTTP Traffic Logger:

• Capture HTTP packets

• Extract URLs, methods

• Log to file

Tool 2 - DNS Query Monitor:

• Capture DNS packets

• Extract queried domains

• Detect suspicious queries

Tool 3 - ARP Spoof Detector:

• Monitor ARP packets

• Detect multiple MACs for same IP

• Alert on potential spoofing

Handle packets safely (don't capture sensitive data)

Deliverables: Submit packet analysis scripts with sample captures	**30 Points**

ACTIVITY 11.3: VULNERABILITY ASSESSMENT SCRIPTS

Topic: Building security assessment tools

Description: Create Python tools for basic vulnerability assessment

INSTRUCTIONS:

Password strength checker:

• Check length, complexity

• Check against common passwords list

• Calculate entropy score

• Provide improvement suggestions

SSL/TLS checker:

• Connect to HTTPS server

• Retrieve certificate info

• Check expiration date

• Verify certificate chain

• Check for weak protocols

Web vulnerability scanner (basic):

• Check for common security headers

• X-Frame-Options

• X-XSS-Protection
• Content-Security-Policy
• HSTS
• Report missing headers

Combine into security audit tool:

• Input: Target URL or IP
• Run all checks
• Generate security report
• Provide recommendations

Use responsibly - only scan authorized targets

Deliverables: Submit vulnerability assessment scripts with sample report	**40 Points**

TOTAL POINTS: 105