

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: KỸ THUẬT THEO DÕI, GIÁM SÁT
AN TOÀN MẠNG
MÃ HỌC PHẦN: INT1429**

BÀI THỰC HÀNH 1

Sinh viên thực hiện: Trần Thị Thu Phương

Mã sinh viên: B21DCAT151

Giảng viên hướng dẫn: ThS. Vũ Minh Mạnh

HỌC KỲ 2 NĂM HỌC 2024-2025

1. Phân tích log giao thức DNS sử dụng ELK Stack

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork nsm-elk-dns
Results stored in directory: /home/student/labtainer_xfer/nsm-elk-dns
Labname nsm-elk-dns

Student | attacker1 | attacker2 | attacker3 | client1 | client2 | client3 | client4 |
===== | ===== | ===== | ===== | ===== | ===== | ===== | ===== |
B21DCAT151 | Y | Y | Y | Y | Y | Y | Y |
What is automatically assessed for this lab:

student@ubuntu:~/labtainer/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
```

2. Phân tích đăng nhập bất thường SSH sử dụng ELK Stack

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork nsm-elk-ssh
Results stored in directory: /home/student/labtainer_xfer/nsm-elk-ssh
Labname nsm-elk-ssh

Student | client1 | client2 | client3 | attacker | server1 | server2 |
===== | ===== | ===== | ===== | ===== | ===== | ===== |
B21DCAT151 | Y | Y | Y | Y | Y | Y |
What is automatically assessed for this lab:

student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"; date
Tran Thi Thu Phuong - B21DCAT151
Sun Apr 20 21:17:03 PDT 2025
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$
```

3. Phân tích gói tin TLS bằng Wireshark

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork nsm-wireshark-tls
Results stored in directory: /home/student/labtainer_xfer/nsm-wireshark-tls
Labname nsm-wireshark-tls

Student | cipher | cert | public-key | disconnect | client-hello | client-cert |
===== | ===== | ===== | ===== | ===== | ===== | ===== |
B21DCAT151 | Y | Y | Y | Y | Y | Y |
What is automatically assessed for this lab:

student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$
```

4. Phân tích gói tin ICMP bằng Wireshark

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork nsm-wireshark-icmp
Results stored in directory: /home/student/labtainer_xfer/nsm-wireshark-icmp
Labname nsm-wireshark-icmp

Student | ICMP-file | Answer | wireshark | ping |
===== | ===== | ===== | ===== | ===== |
B21DCAT151 | Y | Y | Y | Y |
What is automatically assessed for this lab:
    wireshark: Did the student run Wireshark?
    ping: Did the student run ping?

student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ echo "Tran Thi Thu Phuong - B21DCAT151"
Tran Thi Thu Phuong - B21DCAT151
```