**Network Management Group Project – 2018**

**Mỗi báo cáo có độ dài không quá 10 trang và không sao chép nguyên xi từ tài liệu tham khảo, nội dung báo cáo chỉ trọng tâm vào công cụ tìm hiểu**

1. Tìm hiểu/ cài đặt về **Cacti** và ứng dụng trong quản trị SNMP (2 người)
   * Giới thiệu về Cacti cũng như các modun quản trị
   * Demo quản trị với 1 topology ảo trên gns3, có thể tham khảo trên
2. Tìm hiểu/ cài đặt về **Zabbix** và ứng dụng trong quản trị SNMP (2 người)

* Giới thiệu về Zabbix cũng như các modun quản trị
* Demo quản trị với 1 topology ảo trên gns3, có thể tham khảo trên

1. Tìm hiểu/ cài đặt về **Nagios** và ứng dụng trong quản trị SNMP (2 người)

* Giới thiệu về Zabbix cũng như các modun quản trị
* Demo quản trị với 1 topology ảo trên gns3

1. Tìm hiểu về một số kỹ thuật khai thác thông tin/ lỗ hổng trên hệ thống mạng và lựa chọn tìm hiểu các công cụ sau đây: **The Netstat Tool, Nmap, NetscanTool, Superscan, Hping**.
2. Tìm hiểu về IDS và IPS và lựa chọn tìm hiểu các công cụ sau đây: **Snort, Bro, OSSEC, Arpwatch (in Linux), Psad (in Linux), ippl (in Linux), BlackICE, M-ICE, Secure4Audit (auditGUARD), Emerald, Nides, SECUREHOST, GFI EventsManager, Sentivist, StoneGate IPS, McAfee.**
3. Tìm hiểu về các kỹ thuật tường lửa và lựa chọn tìm hiểu các công cụ sau đây: **Firewall Builder, Wflogs, T-REX Open Source Firewall, SQUID, WinGate, Symantec Enterprise Firewall**.
4. Tìm hiểu về Proxy Server và triển khai (tự chọn công cụ)
5. Tìm hiểu về HoneySpot và lựa chọn tìm hiểu các công cụ sau đây: **Backofficer Friendly, Specter, Honeyd, Homemade Mantrap, Honeynet.**
6. Tìm hiểu về các kỹ thuật log và auditing, lựa chọn tìm hiểu một trong những công cụ sau đây: **ASDIC, Tenshi, SpoofMAC, Gentle MAC PRO, Log Manager, LogSentry, SL2, Flog, Simple Log Clustering Tool(SLCT), xlogmaster, Dumpel.exe, Watchlog, LogDog**
7. Tìm hiểu về các lỗ hổng bảo mật với dịch vụ web
8. Tìm hiểu về các lỗ hổng bảo mật với dịch vụ email
9. Tìm hiểu về các lỗ hổng bảo mật trên mạng không dây và lựa chọn tìm hiểu các công cụ sau: **WEPCrack, AirSnort, Aircrack**.
10. Tìm hiểu về các kỹ thuật đánh giá hệ thống mạng và lựa chọn tìm hiểu các công cụ sau đây: **SAINT, Nessus, BindView, Nmap, Ethereal, Retina, Sandcat Scanner, Vforce.**
11. Tìm hiểu/ cài đặt về công cụ quản trị **Pchar**
12. Tìm hiểu/ cài đặt về công cụ quản trị **MGEN**
13. Tìm hiểu/ cài đặt công cụ **Netflow Monitor**
14. Tìm hiểu/ cài đặt công cụ **Netpy** (2 người)
15. Tìm hiểu về traffic monitor và chọn tìm hiểu các công cụ **Ntop, Ngrep, EtherApe, Argues**.