Program and Rules

Segurança em Redes de Comunicações

Mestrado em Cibersegurança
Mestrado em Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Professor

- Prof. Paulo Salvador (regente)
  - Email: salvador@ua.pt
  - Office: IEETA
- Flexible office hours
  - Email (to discuss any topic or schedule a meeting).
  - Discord: Invite https://discord.gg/bPPpKy5
    - Change your nick to your real name (First and Last names).
    - Ask SRC student role.
    - Only after you will have access the course contents.

Program (1)

- Introduction to Network Security
  - NOC vs SOC
  - Network vulnerabilities (known and unknown)
  - Attack vectors and attack phases.
  - Network management good practices and introduction to security architecture
- Corporate network architecture
  - Resilience and redundancy.
  - Layer1, 2 and 3 and 4+ architectures.
  - Network segmentation.
  - Networks and services isolation.
  - Virtual/overlay point-to-point and multi-point networks.
- Access Layer control
  - AAA architecture.
  - Ethernet com EAP/802.1X.
  - WiFi com WPA*/802.1X.
  - Authentication services (RADIUS / TACACS).
- Data flow control
  - Secure zones.
  - Firewalls, Load Balancers and Orchestrators.
  - Network deployment and integration.
  - DoS and DDoS (multi-stage defenses).
  - High availability scenarios.
  - Flow control rules (security policy deployment and good practices).

Program (2)

- Secure communications
  - Cryptography concepts fundamentals.
  - Local Certificate Authority (CA) characteristics and deployment.
  - Secure communication (SSL/TLS).
  - Secure communication (SSH and IPsec).
  - Site-to-site VPN (IPSec tunnel mesh and DMVPN).
  - Remote access VPN (types, deployment and integration)
- Security management
  - SOC and NOC deployment.
  - Device level monitoring and response (Agents, EDR)
  - Network monitoring (SNMP, Netflow, rsyslog,LMS,...).
  - Network level detection/prevention (IDS/IPS).
  - Centralized security operations and response (SIEM and XDR).
  - Cybersecurity KPIs.

Planning (tentative)

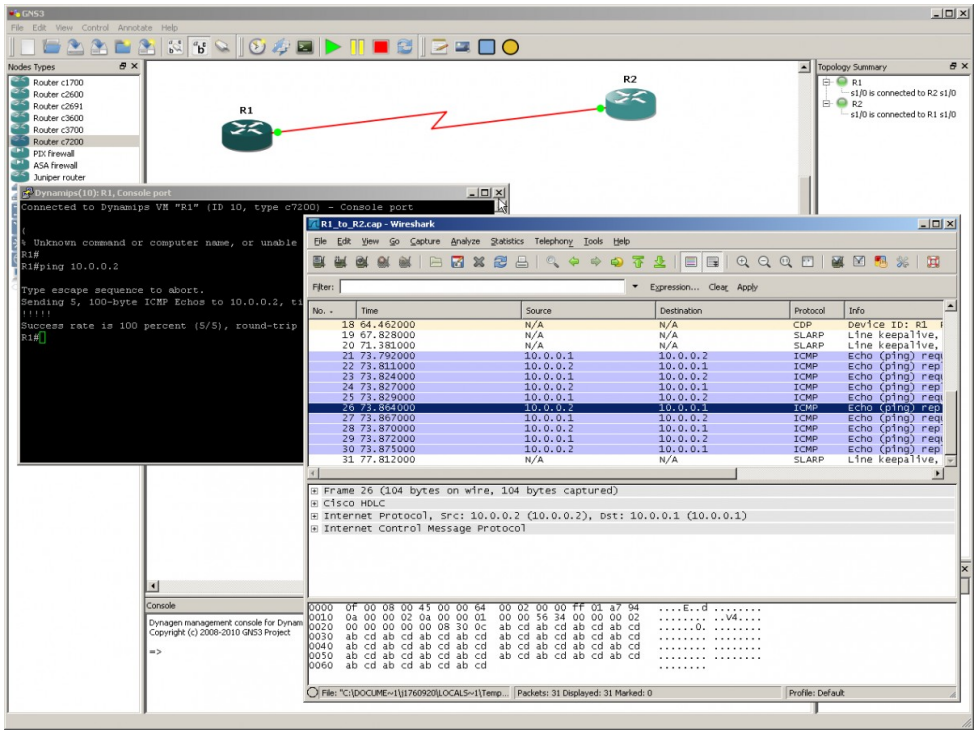
	Week	Theory	Practice	Tuesday	Friday	
1	Feb 11	T1: Program and Rules. Introduction to Network Security.	P0:Intro to GNS3	T1+P0	T1+P0	
2	Feb 18	T2: Corporate Network Topics.	P1: Corporate Network Fundamentals.	T2+P1	T2+P1	
3	Feb 25	T3:Access Layer control	P2: Layer2 Access Control (802.1X & RADIUS).	T3+P2	T3+P2	
4	Mar 04	T4:Data flow control	P3: Introduction to Firewall Deployment.	Carnaval	T4+P3	
5	Mar 11		P3: Introduction to Firewall Deployment.	T4+P3	P3	
6	Mar 18		P4:High-Availability Firewalls Scenarios.	P3	P4	
7	Mar 25	Project support	P4:High-Availability Firewalls Scenarios.	P4	P4	
8	Apr 01	Project support	P4:High-Availability Firewalls Scenarios.	P4	T5+P5	
9	Apr 08	T5: Secure communications (protocols and VPN site-to-site)	P5: Overlay IP and IPsec Networks.	T5+P5	P5	
10	Apr 15		P5: Overlay IP and IPsec Networks.	P5	Páscoa	
11	Apr 22	Páscoa	Páscoa	Páscoa	Páscoa	
12	Apr 29	Sem.Académica	Sem.Académica	Sem.Académica	Sem.Académica	Report 1
13	May 06	T6: Secure communications (remote access VPN)	P6: Network Remote Access (OpenVPN).	T6+P6	T6+P6	
14	May 13	T7: Security management (SOC,IDS/IPS, SIEM/XDR)	P7: Intrusion Detection (Suricata).	T7+P7	T7+P7	
15	May 20	T8: Security management (Network Monitoring. policies and rules)	P7: Intrusion Detection (Suricata).	T8+P8	T8+P8	
16	May 27	Project support	P8: Network Monitoring and analysis.	P8	P8	
17	Jun 03	T9: Security management (Cybersecurity KPIs). Project support	P8: Network Monitoring and analysis.	T9	T9	
18	Jun 10					Report 2

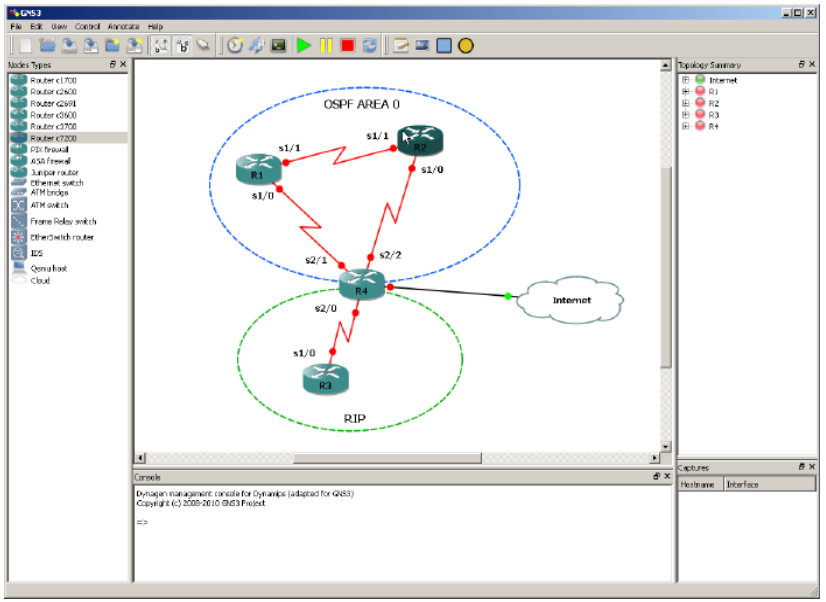
Evaluation

- Final Grade = 50% * Theory Grade + 50% * Practice Grade
  - There are no minimum grade for any component.
  - Theory grade
    - 1 Final Exam (50%) in the exam season;
    - and/or 1 Exam in “repeat exam” season;
    - The best grade is considered.
  - Practice Grade
    - 2 practice reports (25%+25%)
      - Tasks will be specified during the semester.
    - “Repeat exam” season
      - One single project with specific tasks.
      - The best grade is considered.

GNS3

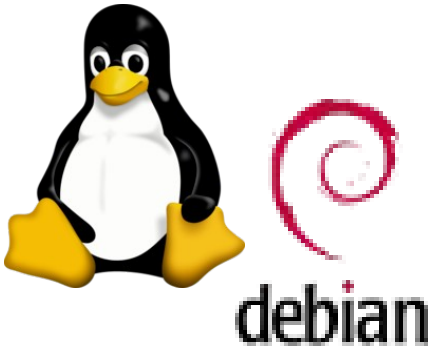
- Network Simulator + Device Emulator
  - Emulates Cisco devices(Routers)
    - Uses IOS/Firmware real with Dynamips
  - Emulates Servers and Firewalls with QEMU or VirtualBox.





Virtual Machines

- QEMU or VirtualBox
- Generic Linux image
  - For clientes, servers, optionally as firewall.
- VyOS (https://vyos.io/)
  - For firewalls and load-balancers.
  - Available image does not support ARM processors.
    - Firewall must be deployed with the Generic Linux image (iptables)
- Images available in elearning.ua.pt



Bibliography

- Ciampa, M. (2017). CompTIA Security+ Guide to Network Security Fundamentals - Standalone Book, 6th Edition. Cengage Learning, ISBN 1337288780
- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson. ISBN 978-0134444284
- Designing Cisco Network Service Architectures (ARCH), John Tiso, Cisco Press, ISBN-13: 978-1587142888, 3rd Edition, 2011.
- Yusuf Bhaiji, Network Security Technologies and Solutions (CCIE Professional Development), Cisco Press, 1st edition, 2008.
- Network Security Through Data Analysis: From Data to Action, Michael Collins, O'Reilly Media; 2nd edition, ISBN-13: 978-1491962848, 2017.
- Crafting the InfoSec Playbook: Security Monitoring and Incident Response Master Plan, Jeff Bollinger, Brandon Enright, Matthew Valites, O'Reilly Media; 1st edition, ISBN-13: 978-1491949405, 2015
- A Practical Approach to Corporate Networks Engineering, António Nogueira, Paulo Salvador, River Publishers, ISBN-13: 978-8792982094, 2013.
- Computer Networks: A Systems Approach, Larry Peterson, Bruce Davie, Morgan Kaufmann, ISBN-13: 978-0123850591, 5th Edition, 2011.
- Jeff Doyle, Jennifer Carroll, Routing TCP/IP, Volume 1 (CCIE Professional Development), Cisco Press, 2nd, edition, 2005.
- Jeff Doyle, Jennifer Carroll, Routing TCP/IP, Volume 2 (CCIE Professional Development), Cisco Press, 2001.