American Public University System
American Military University | American Public University

ISSC 474 Networking Surveillance Syllabus

Course Summary

Course: ISSC 474 **Title:** Network Surveillance
Length of Course: 8 weeks **Credit Hours :** 3
Prerequisites: None

Description

Course Description:

The ISSC 474 course will examine the methods needed to perform surveillance via a network. Learners will be taught and guided as to how network surveillance is implemented and why those in a security role need to be aware of why we need to practice network surveillance. Furthermore, the course will utilize tools downloadable tools for various forms of network scanning. Lastly, the notion of privacy will be reviewed and what we are able to and not able to observe in our networking surveillance practices.

Course Scope:

The scope of the course observes how an organization's network(s) have progressed and why surveillance is needed. As learners use tools such as Wireshark and complete various CompTIA labs, learners will obtain the knowledge needed as to how and why security professionals practice network surveillance. To obtain scholarly means regarding network surveillance, the scope of the course criterion will be observed via scholarly literature from the APUS Library database, the National Institute of Standards and Technology (NIST), along with supplemental materials that will provide an overview of the course content.

Objectives

After successful completion of this course, you will be able to:

1. Evaluate and review how the OSI Layers apply to means of network surveillance.
2. Evaluate previous, current, and future networking surveillance methods.
3. Evaluate the benefits of network surveillance.
4. Observe the risks of practicing network surveillance.
5. Analyze how networking surveillance is used to protect end users.
6. Observe the possible privacy violations while using networking surveillance.
7. Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
8. Analyze the cybersecurity frameworks regarding methods of networking surveillance.

Outline

Week 1: Introduction to Networking Surveillance

Learning Objectives:

- Evaluate and review how the OSI Layers apply to means of network surveillance.
- Evaluate previous, current, and future networking surveillance methods.
- Evaluate the benefits of network surveillance.

Required Readings:

- Surveillance or security? The risks posed by new wiretapping technologies – Chapters One and Two
- Wireless home automation networks for indoor surveillance: technologies and experiments

Supplemental Readings:

- Introduction to the Special Issue on Smart Communications and Networking for Future Video Surveillance
- Handbook of Surveillance Technologies: Third Edition – Chapter 18

Assignment:

Week One Discussion Forum – Due Sunday

Week 2: Monitoring of Computer Activity via Networks

Learning Objectives:

- Analyze how networking surveillance is used to protect end users.
- Observe the possible privacy violations while using networking surveillance.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.

Required Readings:

- Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses
- Protecting end-user privacy in federal cloud computing contracts

Supplemental Readings:

- On Social Networking and Communication Paradigms
- Young people's uses of wearable healthy lifestyle technologies; surveillance, self-surveillance, and resistance
- Packet Analysis with Wireshark – Chapter One

Assignment:

Lab – CompTIA (Network+) Assisted Lab 5: Analyze ARP Traffic – Due Sunday

---

Week 3: Monitoring and Pen Testing LAN Traffic and its Connected Devices

Learning Objectives:

- Evaluate and review how the OSI Layers apply to means of network surveillance.
- Evaluate previous, current, and future networking surveillance methods.
- Analyze how networking surveillance is used to protect end users.

Required Readings:

- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy – Chapter One
- The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-Ng, and Empire – Chapter Six
- Testing IoT security: The case study of an IP camera

Assignment:

Lab – CompTIA (Network+) Assisted Lab 11: Use Network Scanners – Due Sunday

---

Week 4: The Benefits of Wireshark

Learning Objectives:

- Evaluate and review how the OSI Layers apply to means of network surveillance.
- Evaluate previous, current, and future networking surveillance methods.
- Evaluate the benefits of network surveillance.

Required Readings:

Packet Analysis with Wireshark – Chapters Two and Three

Assignment:

Week Four Discussion Forum – Due Sunday

Week 5: Intrusion Detection System (IDS) Surveillance

Learning Objectives:

- Observe the risks of practicing network surveillance.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.

Required Readings:

- Intrusion detection networks: A key to collaborative security – Section II and Section III
- Designing a Machine Learning Intrusion Detection System: Defend Your Network from Cybersecurity Threats - How Machine Learning is Revolutionizing Intrusion Detection

Supplemental Reading:

Machine Learning for Cybersecurity Cookbook: Over 80 Recipes on How to Implement Machine Learning Algorithms for Building Security Systems Using Python

Assignments:

CompTIA Security+ Assisted Lab 17: Configuring an IDS – Due Sunday

Midterm Exam – Due Sunday

Week 6: Intrusion Prevention System (IPS) Surveillance

Learning Objectives:

- Observe the possible privacy violations while using networking surveillance.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
- Analyze the cybersecurity frameworks regarding methods of networking surveillance.

Required Readings:

Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers
Internal Threat Defense using Network Access Control and Intrusion Prevention System

Supplemental Reading:

Seven deadliest network attacks – Chapter 3 Penetration Testing

Assignment:

Week Six Discussion Forum – Due Sunday

Week 7: NIST and Cyber Frameworks regarding Networking Surveillance

Learning Objectives:

- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
- Analyze the cybersecurity frameworks regarding methods of networking surveillance.

Required Readings:

- Cyberspace Under Siege

Supplemental Readings:

- SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT
- 2020 Cybersecurity and privacy annual report
- Global export controls of cyber surveillance technology and the disrupted triangular dialogue

Assignment:

Week Seven Discussion Forum – Due Sunday

Week 8: Current, Present, and Future Tactics of Networking Surveillance

Learning Objectives:

- Evaluate previous, current, and future networking surveillance methods.
- Observe the potential self-surveillance methods users are providing when utilizing networking surveillance.
- Analyze the cybersecurity frameworks regarding methods of networking surveillance.

Required Reading:

- The death of the internet – Chapter Eight
- The Internet of Futures Past: Values Trajectories of Networking Protocol Projects
- Friendship and trust in the social surveillance network
- Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners – Chapters 10, 11, 12, and 15

Assignment:

Week Eight Discussion Forum – Due Sunday
Final Exam – Due Sunday

Grading:

Name	Grade %
Discussions	25 %
Assignments (Labs)	50%
Exams	25%

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to librarian@apus.edu.

Charles Town Library and Inter Library Loan: The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books

and articles from other libraries.
Electronic Books: You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
Electronic Journals: The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.
Tutor.com: AMU and APU Civilian & Coast Guard students are eligible for 10 free hours of tutoring provided by APUS. Tutor.com connects you with a professional tutor online 24/7 to provide help with assignments, studying, test prep, resume writing, and more. Tutor.com is tutoring the way it was meant to be. You get expert tutoring whenever you need help, and you work one-to-one with your tutor in your online classroom on your specific problem until it is done.
Legal Studies Program Guide: This should be your starting point as you explore the resources available to you: https://www.apus.edu/apus-library/online-research/research/research-guides/school-of-security-global-studies/legal-studies-paralegal-studies.

University Policies

Student Handbook
Drop/Withdrawal policy Extension Requests Academic Probation Appeals
Disability Accommodations

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.