CYB 595 – Practical Cyber Security
Fall 2022

Instructor	Bhrigu Celly	**E-Mail**	bcelly@csudh.edu
Classroom	Alternative Instruction	**Class Time**	Sat – 1:00 pm – 4:00 pm
Office		**Office Hours**	
Phone	(310) 243-3398	**URL**	*http://csc.csudh.edu*

COURSE DESCRIPTION:

This course provides theory and hands-on experience in playing with security software and network systems in a laboratory environment, with the purpose of dealing with and understating real-world threats. The course will explore latest development with tools and research in the area of security with exploring current trends. The course will also take both offensive and defense methods to help student explore security tools and attacks in practice. It will focus on attacks (e.g., buffer overflow, heap spray, kernel rootkits, and denial of service), hacking fundamentals (e.g., scanning and reconnaissance), defenses (e.g., intrusion detection systems, port vulnerability scanning and firewalls). Students are expected to finish intensive lab assignments that use real-world malware, exploits, and defenses.

PRE-REQUISITE: Graduate Standing, Consent of Instructor.

TEXTBOOKS [Required]:

Wenliang Du, Computer Security: A Hands-on Approach, ISBN-13: 978-1548367947, ISBN-10: 154836794X

COURSE GOALS:

- To understand a conceptual overview of network security.
- To introduce students to a broad range of research topics in network security, including topics that involve the triad of people, policies and procedures, and technology.
- Gives the students a solid yet concise overview of the fundamental algorithms and techniques underlying network security.
- To enable students to understand the need for information assurance, identify security vulnerabilities, and devise security solutions that meaningfully raise the level of confidence in network security.
- To help students learn how to read and present research paper and to carry out new and significant research projects related to network security.

COURSE OUTCOMES:
Upon completing this course students will be able to:

- Develop a basic knowledge of the context for network security within the enterprise
- Identify and prioritize threats to network security.
- Identify real-world threats and defenses.
- Understanding on real-world security vulnerabilities, exploits and defenses
- Having hands-on labs in network and system security experiments
- Learning knowledge of practical security problems and their solutions

STUDENT ACADEMIC APPEALS PROCESS
Authority and responsibility for assigning grades to students rests with the faculty. However, in those instances where students believe that miscommunication, error, or unfairness of any kind may have adversely affected the instructor's assessment of their academic performance, the student has a right to appeal by the procedure listed in the Undergraduate Catalog and by doing so within thirty days of receiving the grade or experiencing any other problematic academic event that prompted the complaint.

AMERICANS WITH DISABILITIES ACT
CSUDH adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with temporary and permanent disabilities. If you have a disability that may adversely affect your work in this class, I encourage you to register with Disabled Student Services (DSS) and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: no accommodation can be made until you register with the DSS. For information call (310) 243-3660 or to use the Telecommunications Device for the Deaf, call (310) 243-2028, or go to: http://www4.csudh.edu/dss/

COMPUTER INFORMATION LITERACY EXPECTATIONS
It is expected that students will:

1. *Use Microsoft Word for word processing unless otherwise approved by the instructor,*
2. *Be familiar with using email as a communication tool and check your official campus email account at least every other day;*
3. *Be able to access websites and online course materials which may require Flash and other plug-ins;*
4. *Use the library databases to find articles, journals, books, databases and other materials;*
5. *Be able to create an effective PowerPoint presentation;*
6. *Be able to record audio (ideally video) to share with the instructor via the web; and*
7. *Have regular access to a computer and internet access for the term of this course.*

ACADEMIC INTEGRITY

Academic integrity is of central importance in this and every other course at CSUDH. You are obliged to consult the appropriate sections of the University Catalog and obey all rules and regulations imposed by the University relevant to its lawful missions, processes, and functions. ***All work turned in by a student for a grade must be the students' own work.*** Plagiarism and cheating (e.g. stealing or copying the work of others and turning it in as your own) will not be tolerated, and will be dealt with according to University policy. The consequences for being caught plagiarizing or cheating range from a minimum of a zero grade for the work you plagiarized or cheated on, to being dropped from the course.

COURSE POLICIES:

- Deliverables (Class Assignments, Projects) submitted late are not accepted.
- Deliverables (Class Assignment, Projects) not submitted before the end of the final class will earn 0%.
- Any exceptional, non-academic circumstances need to be discussed with the instructor as soon as they arise, prior to the due date of the deliverable. At the time of the discussion, NO make-up work will be assigned.

The instructor reserves the right not to award credit for deliverables that are incomplete. Partial credit is awarded at the instructor's discretion, and only for work that merits such an award. Assignments that are incomplete or incongruous with the specifications may be returned to the student.

MIDTERM & FINAL EXAM:
Midterm exam is during the 8th week of the class and the date for the final exam is based on the final examination schedule printed in the campus Class Schedule. All projects are due no later than the last week of the semester.

No makeup or early exams will be administered.

GRADES:
The following grading scale will be used:

Score	Grade	Score	Grade
94-100	A	91-93	A-
88-90	B+	84-87	B
81-83	B-	78-80	C+
74-77	C	71-73	C-
68-70	D+	64-67	D
0-63	F		

GRADING:
The weighting of the coursework is listed below:

Final Exam	**100**
Hands-On Mini Projects	**500**
Final Exam Presentation	**150**
Mideterm Exam Presentation	**150**
Midterm	**100**
Class Participation	**200**
Total:	**1200**

TOPIC OUTLINE (Will be conducted according the following. However, the schedule of the topics schedule or timetable may be varying slightly)

Tentative Course Schedule

WEEK #	DATE	TOPIC	*Reading Assignment/ Computer Lab Topic/In Class Assignments*
Week 1	TBD	Course Introduction & Requirements/ Overview of References, Virtual Box and Intro to Security Tools. Kali Linux Introduction Features and Tools	Lab 1 – Kali Linux and Setting Up VirtualBox Kali Linux Environment. Setting up Snapshots
Week 2	TBD	Packet Sniffing and Wireshark	Lab 2 - Wireshark: Network protocol analyzer. TCPDump and LibPCAP. Packet Sniffing Basics. In Linux Journal.
Week 3	TBD	Buffer Overflow	Lab 3 Smashing the Stack for Fun and Profit. Aleph One. Local Stack Overflow Debugging Under Unix: gdb Understanding DEP/NX DynaGuard: Armoring Canary-based Protections against Brute-force Attacks.
Week 4	TBD	Scanning and Reconnaissance	Lab 4 - Nmap: The Network Mapper OpenVAS: Open Vulnerability Assessment System. Setting up OpenVAS on Kali Linux. NESSUS: Vulnerability Scanner. ZMap: Fast Internet-Wide Scanning and its Security
Week 5	TBD	Metasploit Framework	Lab 5 Metasploitable2 Armitage: Cyber Attack Management for Metasploit.
Week 6	TBD	Reverse Engineering and Obfuscation	Lab 6 AppSpear: Bytecode Decrypting and DEX DexHunter: Toward Extracting Hidden Code from Packed Android Applications. Reassembling for Packed Android Malware. Wenbo smali/baksmali: an assembler/disassembler for the Dex.
Week 7	TBD	OS Security for the Internet of Things	Lab 7 Zephyr: Real Time OS for IoT
Week 8	TBD	OS Security for the Internet of Things	Lab 8 Brillo: Google's Operating System for the Internet of Things. Contiki: The Open Source OS for the Internet of Things.
Week 9	TBD	Wireless Exploitation & Defenses	Lab 9 Wireless Pre Connection Attacks - Packet Sniffing - aerodump-ng - MAC Address / Channel description . 2.4 Ghz and 5GHz Wireless Pre Connection Attacks - Deauthentication attack - aerodump-ng - MAC Address / Channel description/connection devices. Capturing packets. aireplay-ng, Capturing handshake Security of the WEP and WPA/WPA2 Algorithm

Week 10	TBD	Wireless Exploitation & Defenses	Lab 10 WPA/WPA2 Cracking - Handshake packets and unique keys. (WPS disabled or configured to push botton PBC) or Deauthentication attack WPA/WPA2 Cracking - create wordlist/ dictionary. crunch. WPA/WPA2 Cracking - PMK List. aerolib-ng, aircrack-ng, rainbow tables WPA/WPA2 cracking using GPU, aircrack-ng. keycracking. checking passwords and do the cracking process. hashcat. On GPU. AMD and NVIDIA
Week 11	TBD	Firewalls & Intrusion Detection Systems (IDS)	Lab 11 The Snort Project. The Splunk Project The Linux Firewall iptables
Week 12	TBD	Python and creating attacks	Lab 12 Python introduction. Loops and basic programming Mac Address Changing Network Scanning Dictionaries and Lists ARP Spoofing Attack
Week 13	TBD	Python and creating attacks 2	Lab 13 DNS Spoofer Code Injection File Interceptor
Week 14	TBD	Python Malware Creation 1	Lab 14 Malware Creation – Download / Upload Files Backdoor creation. download and upload files from target system, All OS functionality and testing. Transferring data over TCP and Sockets, Serialization.
Week 15	TBD	Python Malware Creation 2	Lab 15 Webserver, Chat Program. Reverse Backdoor, Access file systems, execute system commands, Download files, Upload files and persistence. Keylogger email report. Python packaging. Program execution.
Week 16	TBD	Trojan Creation	Lab 16 website data communication and hacking, Information gathering, Files, Directories and sub domains

GO TOROS!