Faculty of Science, Engineering and Built Environment

SIT379 Ethical Hacking

Deakin University Unit Guide

Trimester 1, 2021

CONTENTS

WELCOME

Welcome to **SIT379 Ethical Hacking**. This unit is a core unit within the Bachelor of Cyber Security. It is also offered as an elective to students in other courses who wish to explore the world of ethical hacking. Cyber criminals are one of the biggest threats in today's digital world. Ethical hacking is a way of objectively analysing and penetrating organisations' systems to discover and fix security vulnerabilities. An ethical hacker is a security professional who knows how to find and exploit vulnerabilities and weaknesses in computer systems, like malicious hackers. Ethical hackers employ similar techniques and methods used by malicious hackers, however, an ethical hacker uses his skills in a legitimate, lawful manner to try to find vulnerabilities and fix them. An ethical hacker may be employed by governments, banks, or enterprises to prevent cybercrime.

Your first task should be to familiarise yourself with this unit guide and the other sections found on the unit's CloudDeakin website. Please read this unit guide carefully as it explains the structure, content, assessment and rules associated with this unit.

At any stage during the trimester if you have any concerns about the unit, that cannot be dealt with through the unit site discussion boards, please do not hesitate to get in contact with the Unit Chair. I wish you all good luck with your studies and I look forward to working with you this trimester.

Regards
Dr. Jesse Laeuchli

This Unit Guide provides you with the key information about this Unit. For the best chance of success, you should read it very carefully and refer to it frequently throughout the trimester. Your Unit site (accessed in **DeakinSync**) also provides information about your **rights and responsibilities.** We will assume you have read this before the Unit commences, and we expect you to refer to it throughout the trimester.

Due to the coronavirus (COVID-19) situation, you may be learning in a way that is new to you. We appreciate your flexibility and dedication to learning. For a range of helpful services and resources, please go to study support https://www.deakin.edu.au/students/studying/study-support.

WHO IS THE UNIT TEAM?

Unit chair: leads the teaching team and is responsible for overall delivery of this unit

Jesse Laeuchli

Unit chair details

Name	Dr. Jesse Laeuchli, Senior Lecturer in Cyber and Networking Security
Campus:	Melbourne Burwood Campus Building T, Level 2 221 Burwood Highway BURWOOD VIC 3125
Email:	j.laeuchli@deakin.edu.au
Phone:	+61 3 924 45629

Other members of the team and how to contact them

Geelong Campus Coordinator: contact the campus leader for assistance at your campus

Name: Leo Zhang
Role Lecturer in Cybersecurity
Email: leo.zhang@deakin.edu.au
Phone: +61 3 522 78720

Administrative queries

- Contact your Unit Chair or Campus Leader
- Drop in or contact Student Central to speak with a Student Adviser

For additional support information, please see the Rights and Responsibilities section under 'Content' in your unit site.

ABOUT THIS UNIT

This unit introduces ethical hacking and penetration testing techniques to students. Students will be able to solve problems in ethical hacking. That is, students will perform cyber attacks to machines and applications with certain security vulnerabilities. Students will also have opportunity to participate in security challenges and competitions at the national and international levels. Students will be assessed on the basis of their technical capabilities in ethical hacking, their communication skills in speaking and writing, their team-working skills and awareness of ethical and legal constraints.

Unit development in response to student feedback

Every trimester, we ask students to tell us, through eVALUate, what helped and hindered their learning in each Unit. You are strongly encouraged to provide constructive feedback for this Unit when eVALUate opens (you will be emailed a link).

In previous versions of this unit, students have told us that these aspects of the Unit have helped them to achieve the learning outcomes:

- The real-world pentest project was a useful exercise to teach real-world applied skills.
- The learning content was developed as hacking scenarios and this was a practical way of teaching hands-on hacking skills.
- Some students see this unit is a "unique learning experience and one that isn't offered everywhere"

They have also made suggestions for improvement, and so this is what we have done:

- Assessment tasks were redesigned for a better learning experience.
- Learning materials were enhanced with more low-level details to support low-achieving students and more challenging hacking scenarios to support high-achieving students.
- A help hub for the unit was created.

If you have any concerns about the Unit during the trimester, please contact the unit teaching team - preferably early in the trimester - so we can discuss your concerns, and make adjustments, if appropriate.

Your course and Deakin's Graduate Learning Outcomes

GLO1	Discipline-specific knowledge and capabilities:	appropriate to the level of study related to a discipline or profession
GLO2	Communication:	using oral, written and interpersonal communication to inform, motivate and effect change
GLO3	Digital literacy:	using technologies to find, use and disseminate information
GLO4	Critical thinking:	evaluating information using critical and analytical thinking and judgment
GLO5	Problem solving:	creating solutions to authentic (real world and ill-defined) problems
GLO6	Self-management:	working and learning independently, and taking responsibility for personal actions
GLO7	Teamwork:	working and learning with others from different disciplines and backgrounds
GLO8	Global citizenship:	engaging ethically and productively in the professional context and with diverse communities and cultures in a global context

Each Deakin course has **course learning outcomes** which explain what the Deakin Learning Outcomes mean in your discipline. Learning in each unit builds towards the course learning outcomes.

Your Unit Learning Outcomes

Each Unit in your course is a building block towards these Graduate Learning Outcomes - not all Units develop and assess every Graduate Learning Outcome (GLO).

	These are the Learning Outcomes (ULO) for this Unit **At the completion of this Unit successful students can:**	**Deakin Graduate Learning Outcomes**
ULO1	Apply ethical hacking techniques to exploit security vulnerabilities of systems, applications, and services.	GLO1: Discipline-specific knowledge and capabilities GLO3: Digital literacy GLO4: Critical thinking GLO5: Problem solving
ULO2	Communicate with peers effectively on ethical hacking practice	GLO1: Discipline-specific knowledge and capabilities GLO2: Communication GLO4: Critical thinking GLO8: Global citizenship
ULO3	Synthesize knowledge in effectively and efficiently defending real-world attacks performed by malicious attackers	GLO1: Discipline-specific knowledge and capabilities GLO4: Critical thinking GLO5: Problem solving
ULO4	Work effectively as a team member to perform penetration-testing tasks	GLO7: Teamwork GLO8: Global citizenship

These Unit Learning Outcomes are applicable for all teaching periods throughout the year

ASSESSING YOUR ACHIEVEMENT OF THE UNIT LEARNING OUTCOMES

Hurdle requirements

To be eligible to obtain a pass in this unit, students must meet certain milestones as part of the portfolio, and must achieve a mark of at least 50% in the examination.

Brief summary of the hurdle requirement/s	Rationale
1. Unit Tasks (Learning Portfolio) Students are required to complete tasks by submitting them, collaborating with their tutor to resolve any issues identified, and discussing their understanding of the associated concepts by each task's indicated due date. Task discussions must be conducted in practical class (for campus student) or via OnTrack discussions (for Cloud students only). Please ensure that you are enrolled in the correct mode of study. Tasks may be discussed with staff anytime within the submission period by the corresponding due dates. It is strongly recommended that Tasks are submitted well ahead of these due dates, as completion of the tasks involve submitting work for assessment, responding to feedback, discussing the task with teaching staff, and ensuring work submitted demonstrates the required outcomes. In many cases work will need to be corrected and resubmitted, potentially more than once, as part of this process. For a pass grade in this hurdle requirement the portfolio must include attempts on all Pass Tasks and demonstrate minimal acceptable standard for each learning outcome. For higher grades, all Pass Tasks must be complete, and additional Credit, Distinction, and High Distinction tasks are also required. Each of these tasks will have an indicated due date.	The pass tasks in this unit provide students the opportunity to develop and demonstrate achievement of the Unit Learning Outcomes at the minimum expected standards. These tasks are included as hurdle requirements so that students are able to provide evidence of achievement of these ULOs through their portfolio. The portfolio that they submit is used to measure their performance against the minimum standards as well as their ability to justify the outcomes that they have achieved through self-assessment and reflection. The hurdle requirement also provides a mechanism for student-staff interaction to check progress and address educational and motivational issues before it is too late in the trimester.
2. Examination The exam will consist of multiple sections, with Section A requiring students to demonstrate acceptable achievement of all unit learning outcomes. Students who are unable to demonstrate an acceptable level of achievement of all unit learning outcomes in Section A will not be awarded a passing grade for the examination. Other sections of the examination will provide challenge questions to demonstrate a higher standard of achievement of learning outcomes. Students do not need to attempt these sections, and answers provided in these sections will not be assessed if Section A does not demonstrate achievement of minimum standards for the unit.	This hurdle requirement is to authenticate student learning and support academic integrity in the unit.

Summative assessments

(tasks that will be graded or marked)

Deakin has a universal assessment submission time of 8 pm AEDT/AEST. A late penalty will apply to assessments submitted after 11.59 pm AEDT/AEST.

NOTE: It is <u>your responsibility</u> to keep a backup copy of every assignment where it is possible (eg written/digital reports, essays, videos, images). In the unusual event that one of your assignments is misplaced, you will need to submit the backup copy. Any work you submit may be checked by electronic or other means for the purposes of detecting collusion and/or plagiarism.

When you are required to submit an assignment through your unit site (accessed in DeakinSync), you should receive an email to your Deakin email address confirming that it has been submitted. You should check that you can see your assignment in the Submissions view of the Assignment folder after upload, and check for, and keep, the email receipt for the submission.

- Summative assessment task 1

	Learning Portfolio
Brief description of assessment task	Assessment in this unit is designed to encourage and reward students for demonstrating achievement of the unit learning outcomes; with higher grades representing better achievement of these outcomes. The unit will use a web application designed specifically to support the task-oriented assessment approach, with frequent formative feedback culminating in a portfolio for grading at the end of the teaching period.
	Tasks are designed to help students develop and demonstrate achievement of the unit learning outcomes. Tasks will consist of the following kinds of assessment activities: • Conducting penetration testing and security analytics on authorised systems • Writing reports for findings during the practice of ethical hacking • Demonstrating the use of different hacking tools and programs • Assessing the level of security of target systems • Evaluating the severity of security vulnerabilities and risks identified during the ethical hacking process. • Providing justified recommendations to mitigate cyber security threats and risks.
Detail of student output	In completing the unit tasks students will produce a range of artefacts that will be combined into their portfolio. This will include: • Screenshot Images • Documents including penetration testing reports • Links to videos of demos Each student will receive formative feedback on these tasks and will be encouraged to incorporate the feedback received to ensure the work is of the expected standard when it is finally assessed to determine the unit grade in the portfolio.
Grading and weighting (% total mark for unit)	80% - marked and graded Each task in the unit is associated with a grade: either Pass, Credit, Distinction, or High Distinction. Each grade will be awarded based on completion of the tasks associated with that grade, and the lower grades. For this unit the following will set the minimum standard for each grade: • Pass – Complete all Pass Tasks • Credit – Complete all Pass Tasks and all Credit Tasks • Distinction – Completed all Pass, Credit, and Distinction Tasks • High Distinction – Complete Pass, Credit, and Distinction Tasks and all High Distinction Task In general, the graded tasks will provide the following challenge levels: • Pass – scaffolded tasks to help achieve minimum acceptable standard. • Credit – students will apply what they have learnt in the pass tasks to new problems with less guidance. • Distinction – students will apply their advanced knowledge to build programs of their own design that demonstrate integrated understanding of unit topics. • High Distinction – students will extend their understanding to demonstrate greater technical ability, more complex solution structures, advanced algorithms, or in other ways exceed the expectations of the unit.

This task assesses your achievement of these Unit Learning Outcome(s)	The portfolio must demonstrate that you have achieved all unit learning outcomes by proving evidence and self-reflection against each outcome. ULO1 - through ethical applying hacking techniques to exploit security vulnerabilities of systems, applications, and services. ULO2 - by communicating with peer and reflecting on ethical hacking practice. ULO3 - by synthesizing knowledge related to effectively and efficiently defending real-world attacks performed by malicious attackers ULO4 - by working effectively as a team member to perform penetration-testing tasks.
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 – assessed through student ability to self-assess their application of ethical hacking knowledge GLO2 – assessed through student ability to succinctly communicate their personal and professional capabilities and competencies. GLO3 – assessed through student ability disseminate information and outcomes. GLO4 – assessed through evidence of professional judgement and evaluation of specific roles and responsibilities to effectively contribute to ethical hacking. GLO5 – assessed through student ability to evidence particular strategies that they have used in solving problems and making decisions in an ethical hacking scenario. GLO7 – assessed through student work ethic in learning with, from and about each other in a professional context. GLO8 – assessed through student ability to evidence application of high-level ethical and professional standards in completing work tasks as required.
How and when you will receive feedback on your work	Students will be required to work on and submit tasks for formative feedback each week. The teaching team will then review progress and provide individual feedback to each student to assist them in completing the tasks and achieving their target grade for the unit. To ensure that there is sufficient time to staff to provide feedback, and to help manage the learning process, tasks will have set target dates and deadlines. The target date is the date that the task is considered to be due, however, as this may require additional fixes in order to incorporate feedback provided, the work can be resubmitted up to the deadline. Work submitted after the deadline will be checked in the portfolio, and additional formative feedback will not be provided.
When and how to submit your work	At the end of the unit you will use the online task management tool to combine together the artefacts you have created and a learning summary report into a single portfolio for assessment by the end of **Week 12 (Sunday, 6 June 2021 8.00pm AEST)**.

- Summative assessment task 2

	Examination (online)
Brief description of assessment task	This examination requires students to demonstrate they have achieved the unit learning outcomes. Students will respond to questions covering all core aspects of the unit that are drawn out of the pass tasks in the unit.
Detail of student output	This is an individual assessment task. Students will be required to complete an online timed released exam of 2 hours duration. The exam will consist of multiple sections. All students are required to complete the Section A, which is associated with demonstrating a passing standard in the unit. Other sections can be attempted in order to demonstrate higher levels of achievement, but will not assist in demonstrating achievement of the passing standard if this is not achieved in Section A.
Grading and weighting (% total mark for unit)	20%

This task assesses your achievement of these Unit Learning Outcome(s)	ULO1 - through ethical applying hacking techniques to exploit security vulnerabilities of systems, applications, and services. ULO3 - by demonstrating how to effectively and efficiently defending real-world attacks performed by malicious attackers
This task assesses your achievement of these Graduate Learning Outcome(s)	GLO1 – assessed through student application of ethical hacking knowledge GLO3 – assessed through student ability disseminate information and outcomes. GLO4 – assessed through evidence of professional judgement and evaluation of specific roles and responsibilities to effectively contribute to ethical hacking. GLO5 – assessed through student ability to evidence particular strategies that they have used in solving problems and making decisions in an ethical hacking scenario. GLO8 – assessed through student ability to discuss ethical and professional standards
How and when you will receive feedback on your work	The examination assesses the core knowledge and skills developed through the Pass Tasks in the unit. Feedback received as part of successful completion of pass tasks in the unit will assist students in preparing for the examination. A practice examination will be provided to give students the opportunity to prepare for the examination. Student attempts can be submitted for feedback during the teaching period. Students can also make an appointment to get feedback on their exam.
When and how to submit your work	Students will be required to undertake a timed online assessment during the examination period. It is the responsibility of students to review their examination timetable when it is released via DeakinSync.

Your learning experiences in this Unit - and your expected commitment

To be successful in this unit, you must:

- Read all materials in preparation for your classes or seminars, and follow up each with further study and research on the topic;
- Start your assessment tasks well ahead of the due date;
- Read or listen to all feedback carefully, and use it in your future work;
- Attend and engage in all timetabled learning experiences as follows:

Scheduled learning activities - campus

1 x 1 hours class per week, 1 x 3 hour workshop per week.

Scheduled learning activities - cloud

1 x 1 hour scheduled online workshop per week.

Note (on-campus learning activities)

Teaching will be delivered in line with the COVIDSafe health guidelines. All classes will be delivered online but other activities may include a combination of online and on-campus activities. Please refer to the details provided below, and check your unit site for announcements and updates.

Students will on average spend 150 hours over the trimester undertaking learning and assessment activities for this unit. This also includes engaging in online learning activities, assessment activities, readings and study time. Students are expected to complete all allocated learning and assessment tasks for each week and actively engage in discussions with other students

and teaching staff. This unit requires students to complete milestones as they progress through the unit. This requirement is to ensure that students engage with teaching staff throughout the unit. This unit has been designed to provide all students with a high level of interaction and feedback from teaching staff as a strategy to support student success.
In the online task management system:

- Task sheets
- Task resources, as required
- Individual feedback
- Alignment of tasks to unit learning outcomes
- Visualisations of your progress to help keep you on track

Your work in this unit starts on Day 1 of the trimester. You are expected to complete the prescribed readings, reproduce the practical tasks shown in the classes, and complete unit tasks in the online task management system. As you complete the tasks, you will be able to collect evidence for justifying how you have met the unit learning outcomes through your portfolio. The process of developing your portfolio is simple and easy, so keep that in mind as you read the assessment instructions below.

In order to understand how assessment in this unit works, let's consider standard assessment practices. A typical unit has assignments and tests that you submit and get marks for. The problem is, you only get one chance to succeed, and any marks you lose are gone. This focuses your attention on marks, rather than on working to achieve good learning outcomes.

To focus your attention on learning in this unit, we avoid having marks for tasks during the unit and instead assess your final work to see how well you have achieved the outcomes at the end of the unit. This is the summative assessment at the end of the unit, where your grade is determined by the evidence you present in your portfolio.

We will work with you by providing formative feedback for these task as you submit them week by week. When you submit a task, we will review your work and provide you with feedback. Where your work does not correctly demonstrate the required outcomes, we will give you feedback to help enhance your learning and improve your work for your final portfolio submission. You then need to fix and resubmit the work, so we can check it again and sign it off as Complete when you have achieved the required standard.

We will keep track of all of this in the online task management system, which is where you submit work, receive feedback, resubmit it, and then finally see it signed off as Complete. The process for you is then just a matter of working through the required tasks week by week, and work with us to make sure they are ready for your final portfolio submission. At the end of the unit you can then combine together all of your work on the tasks and submit it for marking and grading.

So, learning in this unit is as simple as setting your target grade, and completing the unit tasks associated with that grade in the online task management system. The teaching team will work with you in providing weekly feedback so that you can achieve the goals you set, demonstrate your ability to complete the unit tasks and discuss your performance with confidence.

Note

At Deakin,

- *Lectures* are referred to as *classes* (definition: a general meeting for all students, for which students do not need to register and where students are engaged through presentations and learning activities)
- *Tutorials, workshops and seminars* are referred to as seminars (definition: more interactive meetings for smaller groups of students).
- For the complete list of agreed definitions for learning experiences, see the Course Design and Delivery Procedure.

UNIT LEARNING RESOURCES

Your unit learning resources are available in your unit site accessed in DeakinSync.

The texts and reading list for the unit can be found on the University Library via the link below: SIT379 Note: Select the relevant trimester reading list. Please note that a future teaching period's reading list may not be available until a month prior to the start of that teaching period so you may wish to use the relevant trimester's prior year reading list as a guide only.

Essential learning resources

There is no prescribed text for this unit.

Recommended learning resources

The following text is recommended:

- HACKER PLAYBOOK #3 : PRACTICAL GUIDE TO PENETRATION TESTING, 2014, Georgia Weidman

The textbook forms the basis of the learning material required for the unit. You should set aside some time during each week to complete the readings from the textbook. Please note that the textbook does contain more detailed information about the concepts discussed in classes. You will be asked to recall and use this more detailed information in the examination.

Textbooks, reference books, general books and software may be ordered from the bookshop:

- phone 1800 686 681 (freecall);
- Email to DUSA-Bookshop@deakin.edu.au; or
- order online from the University bookshop web site at http://www.dusabookshop.com.au

KEY DATES FOR THIS TRIMESTER

Trimester begins (classes begin)	Monday 8 March 2021
Intra-trimester break (a short break during trimester)	Friday 2 April - Sunday 11 April 2021
Trimester ends (classes cease)	Friday 28 May 2021
Study period (examination preparation period)	Monday 31 May - Friday 4 June 2021
Examinations begin	Monday 7 June 2021
Examinations end	Friday 18 June 2021
Inter-trimester break (the period between trimesters)	Monday 21 June - Friday 9 July 2021
Unit results released	Thursday 8 July 2021 (6pm)

UNIT WEEKLY ACTIVITIES

Week	Commencing	Topic	Learning activities	Assessment activity
1#	8 March 2021	Introduction to Ethical Hacking	Workshop 1	

2	15 March	Penetration Testing Reports	Workshop 2	
3	22 March	Kali Linux and Metasploit	Workshop 3	
4^	29 March	Social Engineering and Reconnaissance	Workshop 4	
5	12 April	External Network Penetration Testing	Workshop 5	
6	19 April	Internal Network Penetration Testing	Workshop 6	
7*	26 April	Advanced Ethical Hacking Skills	Workshop 7	
8	3 May	Advanced Ethical Hacking Skills	Workshop 8	
9	10 May	Advanced Ethical Hacking Skills	Workshop 9	
10	17 May	Revision	Workshop 10	
11	24 May	Portfolio submission and interviews.	Revision	
12	31 May	Study week		Learning portfolio due

#Victorian Labour Day public holiday: **Monday 8 March** - University open

^Easter vacation/intra-trimester break: **Friday 2 April - Sunday 11 April 2021** (between weeks 4 and 5)

*ANZAC Day observed, **Monday 26 April (in lieu of 25 April)** - University closed

Setup Virtual Environment.

Subtask 1

1. Setup your virtual machines. You should have the following, connected as in the figure below.
   (a) PFSense
   (b) Kali Linux
   (c) Windows XP
   (d) Metasploit

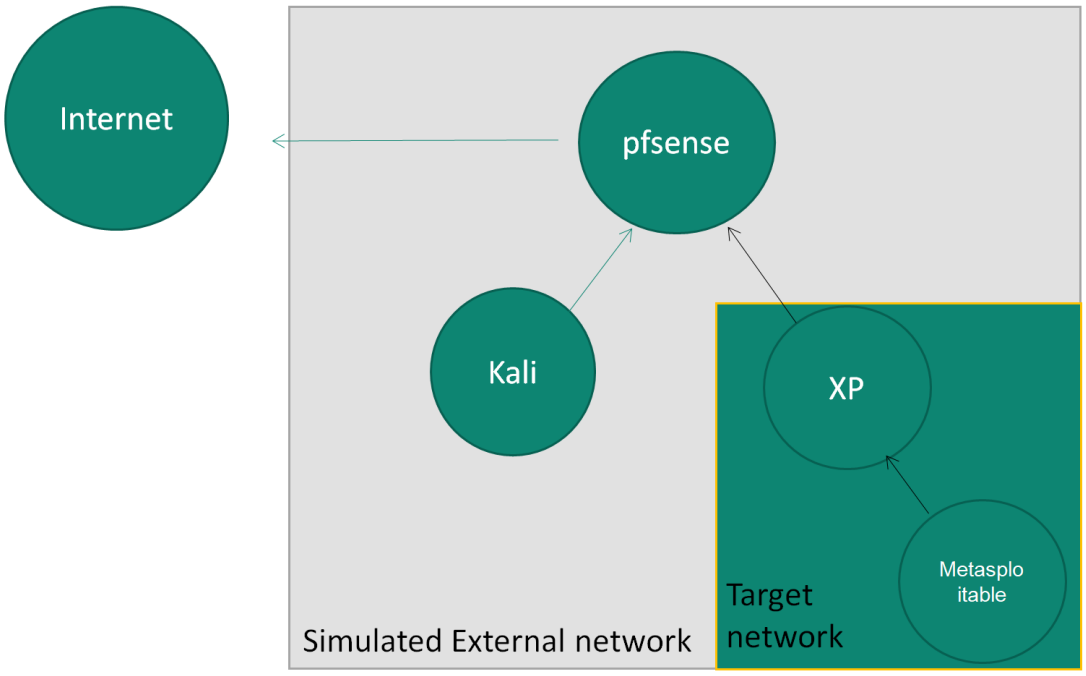

Figure 1: Virtual Network Design

When you submit include a document with a screenshot of your VMs running and a screenshot of the output of ipconfig on the XP machine.

Capture Packets

Subtask 1

1. Capture packets from your VMs. You should try two ways.
   (a) Using VirtualBox capture on the host
   (b) Using tcpdump on the pfsense command line

VirtualBox Capture

1. Open a command prompt
2. Navigate to the Virtual Box directory
3. Use VBoxManage with the flags 'modifyvm `VMNAME`', '–nictrace on', '–nictracefile1 `OUTPUTFILE`'
4. Import this file into your Kali VM
5. Open it in Wireshark

   line

Your submission here should be a screenshot of wireshark opening your captured pcap, as well as a screenshot of your command line enabling the capture

tcpdump

1. Open a shell on your pfsense virtual machine
2. use TCPdump to capture all traffic on port 80 (you may need to consult the tcpdump manual)

Submit a screenshot of you capturing some port 80 traffic on pfsense.

ARP/MAC attacks

Subtask 1

Use arpspoof to target your pfsense router. Use urlsnarf to determine when the attack has been successful. You should submit the following

1. A screenshot showing urlsnarf is picking up intercepted traffic
2. A screenshot showing the before and after ARP tables on your pfsense VM. Use the arp command to obtain this information.

Subtask 1

Use macof to launch a CAM table flooding attack. YOu should submit the following.

1. A screenshot showing macof in action.

ARP/MAC attacks

Subtask 1

Use arpspoof to target your pfsense router. Setup a packet capture of your attacking VM. Examine the packet capture. You should submit the following

1. A short write up referencing what the correct IP and MAC addresses are of the victim, the router, and the attacker.
2. A screenshot showing an ARP packet that you can tell to be incorrect based on the above.

ARP/MAC attacks

Subtask 1

Scapy is a popular python package that allows you to read and create packets. Use scapy to design a simple program to detect a possible arp attack. One design would be to run the program, detect and store MAC<->IP mappings, and alert the user if there are any changes. You are free to examine other implementations on the internet, but if you do, reference them. You should submit the following.

1. A short python script that detects any changes in the ARP mapping, with a brief explanation of the code.
2. A screenshot showing your program successfully detecting a change to the ARP tables while an ARP attack is in progress.

Below is some code to help you start.

Listing 1: Code Skeleton

```
from scapy.all import *
pkts = rdpcap('capture.pcap') %Can also do a live capture

ipadr=['192.168.1.1','192.168.1.2','192.168.1.3','192.168.1.4'] %populate this
macadr['00:03:ff:98:98:01','00:03:ff:98:98:02','00:03:ff:98:98:03','00:03:ff
    :98:98:30']%populate this

for p in pkts:
 if p.haslayer(ARP):
  %Do stuff
```

Setup Virtual Environment.

Subtask 1

Setup your virtual machines. You should have the following, connected as in the figure below. Add a network rule that blocks all traffic from internal network 1 to internal network 2 except for one port. Use traceroute to show this port is open and that there are no other hosts between your target and pfsense. You should submit the following.

1. A screen shot showing what happens when you use traceroute to the target when the port is open vs when it is closed.

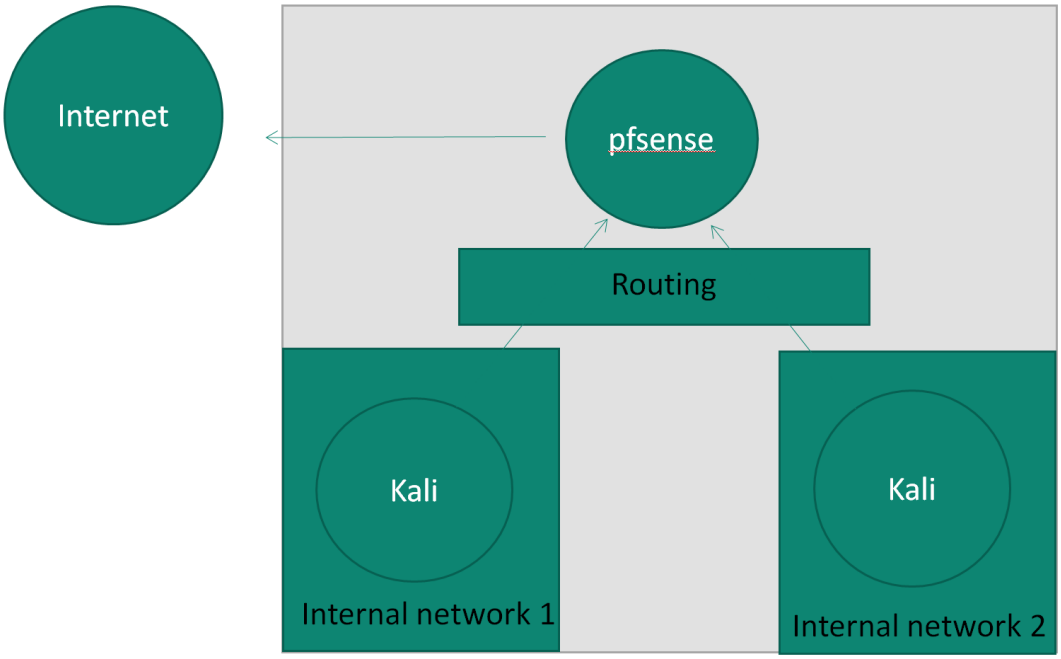

Figure 1: Virtual Network Design

Subtask 2

Place your two Kali Machines on the same virtual network. Perform the following scans with nmap, while performing a packet capture between the two. Submit the following.

1. A short explanation of each of the following scans, explaining the differences, when you would use them, and referencing the packet capture to illustrate your point.

(a) Full Connect

(b) Syn Scan

(c) Xmas Scan

Scanning

Subtask 1

Place your one Kali VM and one XP VM on the same virtual network. Perform an XMAS scan on the XP machine, while capturing the packets between them. You should submit the following.

1. A short explanation of the differences you see in the XMAS scan against the Windows machine versus against what happened when scanning the Kali machine. Reference your packet capture in the explanation.

Scanning

Subtask 1

Scapy is a popular python package that allows you to read and create packets. Use scapy to design a simple program to syn scan a range of ports. You are free to examine other implementations on the internet, but if you do, reference them. You should submit the following

1. A short python script that syn scans a target, with a brief explanation of the code.
2. A screenshot showing your program successfully scanning a target.

Below is some code to help you start.

Listing 1: Code Skeleton

```
import time
import logging
from scapy.all import *

closed_ports = 0
open_ports = []
ip = IP

def is_up(ip):
    % Tests if host is up
    icmp = IP(dst=ip)/ICMP()
    resp = sr1(icmp, timeout=10)
    if resp == None:
        return False
    else:
        return True

if __name__ == '__main__':
    start_time = time.time()
    ports = range(1, 1024)
    if is_up(ip):

        for port in ports:
    else:
```

Hijack DNS

Subtask 1

Hijack a DNS query from your XP VM to pfsense. Capture the packets between your Kali attacker and your victim. You should submit the following.

1. A screenshot showing your victim receiving the wrong website when they attempt to navigate to bing.com.
2. A screenshot of where in the packet capture the DNS hijacking is taking place.

Session Hijacking

Subtask 1

Instead of using ettercap to hijack the DNS session use dnsspoof. Capture the packets between your victim. Does this program work as well as ettercap? You should submit the following.

1. Submit a short explanation of why or why not the program works as well as ettercap, referencing the packet capture to describe any problems.

Session Hijacking

Subtask 1

Scapy is a popular python package that allows you to read and create packets. Use scapy to hijack a telnet session and insert your own commands. If you find it easier you may provide your program with the packet sequence number. Your metasploit VM has a Telnet server you can attack. You should submit the following.

1. A short python script that allows you to hijack a telnet TCP session, with a brief explanation of the code.
2. A screenshot showing your program successfully running a command on the target

Below is some code to help you start.

Listing 1: Code Skeleton

```
import sys
from scapy.all import *

IPLayer = IP() %what should I put here?
TCPLayer = TCP()  %what should I put here?
Data =  %what should I put here?
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
```

Metasploit

Subtask 1

Create a reverse shell using netcat using two Kali Linux machines. You should submit the following.

1. A screenshot showing your victim receiving commands from the attacker via a netcat reverse shell.

Subtask 2

Use msfvenom to create a meterpreter exploit targeting XP. Create a listening post on Kali and then run the exploit on the XP machine.You should submit the following.

1. A screenshot showing your victim receiving commands from the attacker via a metasploit reverse shell.

Subtask 3

Use metasploit to attack windows XP using exploit ms08_067_netapi . Create a listening post on Kali and then run the exploit on the XP machine. You should submit the following.

1. A screenshot showing your victim receiving commands from the attacker via a metasploit reverse shell, as well as a screenshot configuring ms08_067_netapi.

Metasploit

Subtask 1

Use msfvenom to create a meterpreter exploit targeting Android. Create a listening post on Kali and then run the exploit on Android. You will need to enable the ability to run unsigned code on the Android VM, as well as enable the super user account.

1. A screenshot showing your victim receiving commands from the attacker via a metasploit reverse shell.

Acquiring New Targets

Subtask 1

1. Use DNS Spoofing to redirect victim XP machine to your webserver. On your webserver have a malicious iframe which targets internet explorer 6, as described in class. You should submit screenshots showing the following

   (a) Successfully exploitation of IE 6

   (b) Migrating out of the IE process

Subtask 2

1. Once you have exploited the XP machine, setup a route and use it to gain access to the metasploitable machine by exploiting VSFTP. This VM should be on a private network shared by the XP and Metasploitable machine. You should submit screenshots showing the following

   (a) Successfully exploitation of the Metasploitable Machine

Acquiring New Targets

Subtask 1

1. Once you have setup a route from your Kali machine to the Metasploitable VM via XP, use this route to scan the Metasploitable machine for open ports. You should submit screenshots showing the following

   (a) Successful port scanning from Kali

Acquiring New Targets

Subtask 1

1. Once you have setup a route from your Kali machine to the Metasploitable VM via XP, instead of exploiting VSFTPD, use Unreal IRC. Routing this attack through XP will fail. Setup a package capture of the traffic to the Metasploitable VM and determine why. You should submit

   (a) A short write-up explaining why the attack failed, referencing what you see in the packet capture.

Subtask 2

1. Once you have determined why the attack failed,you should fix it. You will want to start by using your XP session from the start of the exploit to modify certain settings with the tool netsh. Following this you will want to set a generic payload in Kali prior to attacking metasploitable.

   (a) A screenshot of the commands you used on windows XP

   (b) A screenshot of your payload configuration

   (c) A screenshot demonstrating that you successfully gained access to the metasploitable box via the unreal ircd exploit.

Complete this task if you are interested in receiving a free study package and exam voucher for the Certified Ethical Hacker certification. To be eligible for this task you must have completed all the tasks up to and including 2.3D. If you have done so, then fill out the form here, and on On-track submit a screenshot showing the ontrack tasks you have completed, as well as a CSV file containing in this order your name, email address, and student ID.

On Access

Subtask 1

Create a new user. Give him a short 3-4 letter password. Use crunch to create a dictionary, and then use hashcat to recover the password. You should submit the following.

1. A screenshot of your shadow file showing your new user and his hashed password.
2. A screenshot showing hashcat recovering your password.
3. Assume your password is three letters long, and the symbols are only alphanumeric(A-z0-9). How many bits of entropy is the password?

On Access

Subtask 1

Gain access to the windows XP box using the exploit of your choice. Use mimikatz to aquire the hash of the password on the machine. You should submit the following.

1. A screenshot of the hashes of the XP VM recovered through mimikatz.
2. A screenshot of a minesweeper layout recovered by mimikatz.

On Access

Subtask 1

As we saw in the class and in the pass task, if the salt and hash is known, one can attempt to recover the original string that produced the hash. Linux comes with a default crypt library. Use this to create a short C program that will attempt to reverse the hash `dNpxBzJg/Cg`, given that the salt was 23. You may use brute force or a dictionary you create. You should submit the following

1. A short program that recovers the original string.
2. The original string.

Below is some code to help you start.

Listing 1: Code Skeleton

```c
#include <stdio.h>
#include <crypt.h>
int main(int argc, char *argv[])
{
    printf ('%s', crypt(argv[2],argv[1]) );
    return 0;
}
```

On Access

Subtask 1

As we have seen, one way to detect an attacker is to notice unwanted connected on the victim machine via netstat. Netstat is an open source project. Download netstat and edit the code so that it does not display connections on your chosen port. Create a reverse shell using netcat and demonstrate how the connection does not appear in the logs.

1. An edited copy of netstat, along with an explanation of what you changed.
2. A screenshot showing your version of netstat successfully hiding your connection.
3. A comparison of the hash of the original netstat vs your own. Is it possible to detect your corrupted version of netstat through comparing the hash?

Finding Exploits

Subtask 1

Fuzz SLmail by finding out how long a password string will crash the program. You should submit the following.

1. A screenshot of the SLMail crashing
2. How long the string had to be before the program crashed.

Below is some code to help you start.

Listing 1: Code Skeleton

```
import socket

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

buffer = A * X %change X to fuzz

try:
    s.connect(('192.168.97.130', 110))
    data = s.recv(1024)
    s.send('USER legit' + '\r\n')
    data = s.recv(1024)
    s.send('PASS ' + buffer + '\r\n')
    data = s.recv(1024)
    s.close()
    print 'Done!'
```

Finding Exploits

Subtask 1

Create a full exploit for SL mail, meaning once you run it you will start a reverse shell. You are welcome to examine other implementations online, but if you do, you should cite them. You should submit the following.

1. Your code, along with a brief explanation of how it functions.
2. A screenshot showing the reverse shell resulting from running the program.

Below is some code to help you start.

Listing 1: Code Skeleton

```
import socket

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

buffer = A * X %change X to fuzz

try:
    s.connect(('192.168.97.130', 110))
    data = s.recv(1024)
    s.send('USER legit' + '\r\n')
    data = s.recv(1024)
    s.send('PASS ' + buffer + '\r\n')
    data = s.recv(1024)
    s.close()
    print 'Done!'
```

Web Exploits

Subtask 1

Scan Bodgeit in OWASP. You should find an XSS vulnerability in the app.

1. A screenshot showing the scan OWASP finding a XSS bug
2. A screenshot showing you exploiting the bug.

Web Exploits

Subtask 1

Complete the Bodgeit challenge in OWASP.

1. A screenshot showing that you have completed the challenge
2. A short write-up describing how one can replicate the attacks

Web Server Exploits

Subtask 1

Create a reverse shell to the DVWA web app server as we discussed in class. You should submit the following.

1. A screenshot showing that you have access to the DVWA server via a reverse shell.
2. A screenshot showing your level of privilege.

Web Server Exploits

Subtask 1

Create a reverse shell to the DVWA web app server as we discussed in class. Use it to gain root access. You should submit the following.

1. A screenshot showing that you have access to the DVWA server.
2. A screenshot proving that you have root level access.

Web Server Exploits

Subtask 1

Take a Ethical Hacking practice test from the EC website. You should submit the following.

1. A screenshot showing that you took the practice exam and what the outcome was.

Ethical Hacking Certificate

Subtask 1

Pass the exam for the Ethical Hacking Certificate. You should submit the following.

1. A screenshot of your certificate.

Good luck!