Airgap - we don't connect it to the internet, so the only way we can get into it is to go directly into it and tap into it

We need to consider defensive and offensive mindset when we think about security

- Attackers are only going to go for the weakest points to attack, not the strongest links

ETHICS - make sure you agree to the don't be a dick policy cos you could be kicked out

Morris Worm - was not intended to be a malicious creation

- Student made this thing so it only went to computers that hadn't been infected and not the ones that had already been
- Was one of the first worms to go around the world
- Was self replicated - uses a vulnerability in RSH
- It was coded just to see if it could be done - no malice was intended here
- Did the kid deserve imprisonment for what he did?

What is scope - anything on the subdomain for *.quoccabank.com and infrastructure is free reign of to do things for

- Things not on scope - *unsw.edu.au, *moodle, *openlearning, *unsw, anything that touches the uni is out of scope

Bug bounties - these are a thing

- A way you can target things in the real world that you have permission to target
- E.g. hackerone, bugcrowd
- Note that they have scope - do not go outside of scope
- There are bonus points for bug bounty submissions

Kris - TrashPanda - Lecturer in charge

Hamish is usually the go to when it comes to the tech admin type stuff

Lecture structure

- 6-7 base course Tuesday
- 7-9 - looking at how to do the challenges Tuesday
- Wednesday - they look at things that are more advanced and attacking techniques
    - Most of these will not be recorded though

Note: all things will be on echo but shouldn't rely on them though

cs6443@unsw.edu.au

Don't share flags but you are encouraged to work with others to find flags

ASSESSMENT

- There is a final exam - worth 50% - is an online things where you have to hack particular resources
- There will be a self assessment quiz in Week 5 - if you want more time you can use the self assessment as your part a so you can work on part b and c
- Weekly activities (flags) - assess whether you submitted them on time
    - Reports are on how you did it and how you remediated it
    - These are due on Sundays - challenges released on Tuesday so you have 12 days to do the challenges
    - Points are static so no matter how many people are solving them you get that amount of points
- 40% on reports - 2 of them
    - Due the end of week 5 and end of week 10
    - They will look like a penetration test
    - If you're doing challenges write down what you did so that it helps with your report writing
    - You will be in groups - the groups are in tutorials, stick to a group in your tutorial
        - Learn to work together and ahead of deadlines

MEMES - we want to see memes, these won't deduct marks for memes but they are looked on fondly - want to see this (to an extent) - makes the tutor's life easier

WHAT HAPPENS WHEN WE MAKE A WEB REQUEST

- First thing that happens is where are you - way that this happens is through DNS (where is the website we want to access)
    - Sends a request to a DNS server
    - When you connect to a wifi network it will tell us which DNS server to use or the ones that we are able to use
        - 8.8.8.8 (google), 1.1.1.1 (Cloudflare)
- If it knows where this website is then it sends a response back in to where it is
- If it doesn't know then it's going to ask another DNS server
- www.uspto.gov (top domain is uspto.gov) (subdomain is www)
    - Authoritative server is the one that owns the top domain
    - If any servers in this chain knows the name of the site back early

DNS has 2 versions, recursive or iterative

- Recursive checks top domain first then go to subdomain servers until it finds the name
- Iterative - goes subdomain, then up to the next one and then the next authoritative server

Linux

- Dig sends DNS requests and prints them out to the screen
- Dig uspto.gov will show DNS requests
    - A record means that it is an IPv4 address
- After this you can move onto the next step
- Might have to find it yourself because it might not natively be there
- You can also look for this online

Burp Suite is a man in the middle tool - lets you edit packets before you send the response
- Tut 1 will get you set up to do this

The gap in the response text is important
- To render the page this is what comes after that gap

First set of lines in the request is metadata about the request - most of this is unnecessary for us to know, but learn everything as you go
- Accept encoding is important though

HTTP doesn't even verify who you are - just has a system of give and you shall receive

Requests come in many forms - most common request we will make is GET - gets some information
- Gets something, all it needs is the thing that you are getting
- Getting a slash '/' is the root domain

HTTP 1.1

Note, for all of our infrastructure we are working with you will need a host

What if you needed to get something

- There is a post method that allows you to upload information
- E.g. login page - you would need a username and password
- Why would you need a post that does nothing
    - All the data might be part of the URL query
    - Might be to see if you get a response - if you were trying to do recon might send a post request if your get requests are getting nothing
    - Data analytics could be another reason

When you make a post request there are 2 ways to do it
- Through the URL - anything beyond a ? is additional information we want to send to the location
- Through the body - the part after the space in the request
    - Could be in the form of a JSON

Response code - can show us if we are looking in the right place

- 200s - means something is good
- 300s - redirect
    - 302 is moved temporarily
- 400s - you screwed up something
    - 418 (means I am a teapot - is an April fools joke that got incorporated into standard)
- 500s - the server screwed up

Other terms

- TCP/IP (work together) - transfer protocol - allows us to capture if some information has been dropped
    - You can't have HTTP without this
- TLS - transport layer security - encryption - uses certificates
- HTTPS - HTTP over SSL
- HSTS - HTTP strict transport security - when you register a site here, we say load this site as HTTPS and if there is a bad certificate then drop the connection
- Cookies - are a way of implementing states in HTTP
    - HTTP doesn't know who you are
    - So instead of fixing HTTP - we have cookie
        - Looks up who previously looked at something and sends back that cookie
        - Are stored as text files
        - Important in terms of verifying who you are
        - Are a part of HTTP as a service
- Browsers - how you interact with HTTP
    - They will handle a lot of things like fetching the next request and handling cookies
    - Handles the overhead that you don't think of
    - The browser is a piece of software - so it can be hacked
    - Javascript can break out of the browser - is possible that you can get hacked just by clicking
        - But the irony is that lots of things use javascript to work though so hard to use the internet without it

1. Planning and reconnaissance
2. Scanning
3. Gaining access
4. Maintaining access
5. Analysis and WAF configuration

Recon - finding information, the more information you have on something the easier it is for you to hack it

GCP - google cloud program

- You can create a google cloud account, load a coupon and gives you a server so you can run a DNS script on

DNS is a good tool for reconnaissance
- www.quoccabank.com
- Dns.quoccabank.com

The best way to start to look at subdomains is to start with DNS records
- A record - pointing an address to a location
- AAAA record is an IPv6 record
- NS - name server record - this tells you who is hosting the DNS records for thai site
- You can describe what DNS record you are looking at by going dig -t NS [website]
- MX - to do with mailing
- TXT - you can put this into your site
    - These are verifications - instead of implementing a new record we just put what we need in here (this is what has happened in history)
- CNAME - domain you are looking for is over there - pointer to another domain name - is just a pointer
- Soa - state of authority
    - Tells you who is hosting the DNS and where it is
    - Last time it was updated
    - How long it stays in a DNS cache for

Dig -t txt [website] @1.1.1.1 - pings the DNS server - will force it into the cache if your DNS server doesn't already know

This is using Dig to query DNS records
- Bypass HTTP completely and ask the DNS server
- If the status is noerror status then it means that the subdomain exists
    - NXDOMAIN means that it is not a site - doesn't exist

Subbrute

- Asks multiple DNS servers about any list that you give it and it will ask for the subdomains
- How do you run it - is a python script using threads
- There are wordlist generators based on the input data
- Note that when you install this it has a limit on the word list - 1000 lines per wordlist
- Subrrute is python is not the fastest

Where else would you do some recon
- Could ask the person who made them
- Typing them into the url bar to see what works - guess and check - this is a slow method though

- Look at certs and hope that they are not using a wildcard
    - Can check the certificate on the browser - view the certificate
    - If it is not a wildcard might be easier for you to find something but wildcard could be anything
- There are online tools that will do it for you - these constantly scrape for this stuff
- Where else would you find things/resources to help you
    - Can use the source website too
    - If you are looking for analytics - if the analytics page is not protected then we have access to anyone who accesses the site
- Google dorking
    - Google hacking database - stores a list of cool google searches and get websites out
    - Typing things into google does not interact with the server (this is passive recon - if you click into those links then you are active reconning (out of scope)
    - Intext:"index of" "phpMyAdmin""inurl:[website]"
- You need to understand your tools
- There is a tone of places you can go to look for things

SHODAN - is an internet crawler - scans the internet and tells you what it found at that time of day

- Crawls internet via IP address
- These web crawlers are illegal
- Will tell you the ports that are open
- So if you find the IP you can get information from it

Websites - default port is 80
Port 443 is HTTPS site
Port 8080 is a development site

Sometimes you will get a certificate error when you are interacting with Quoccabank but most of the time these are intentional

Awesome shodan queries will show you some cool things

We want to find subdomains is a wider attack surface