IFS4103:
Penetration Testing Practice

Lecture 1:
Overview, Administration
& Introduction to Pen-Testing

Outline

- Course overview
- Course admin: Schedule, projects, grading
- *Ice breaking*

- Brief introduction to Penetration Testing
- Seven important tips
- Your pen-testing system set-up (Lab 1)
- Discussions

What is IFS4103?

Course Description

- **Title**: Penetration Testing Practice
- **Description**:

  This is a practice-oriented and project-based course that provides a hands-on experience of performing penetration testing on a collaborating organisation's system. It aims to provide students with a realistic platform for applying offensive-based vulnerability assessment and analysis techniques on designated target systems. Students will be part of a penetration testing team, and be guided to apply the methodology, techniques, and tools of assessing the security of the target systems. This course contains a mix of technical-review seminars, testing-scoping meetings, and penetration testing exercises, analysis, as well as reporting.

Course Description

- **Examinable**: -
- **Units**: 4
- **Pre-requisite**: CS3235 Computer Security
- **Course Workload** (A-B-C-D-E)* : 2-0-1-6-1
  * A: no. of lecture hours per week
    B: no. of tutorial hours per week
    C: no. of laboratory hours per week
    D: no. of hours for projects, assignments, fieldwork etc per week
    E: no. of hours for preparatory work by a student per week

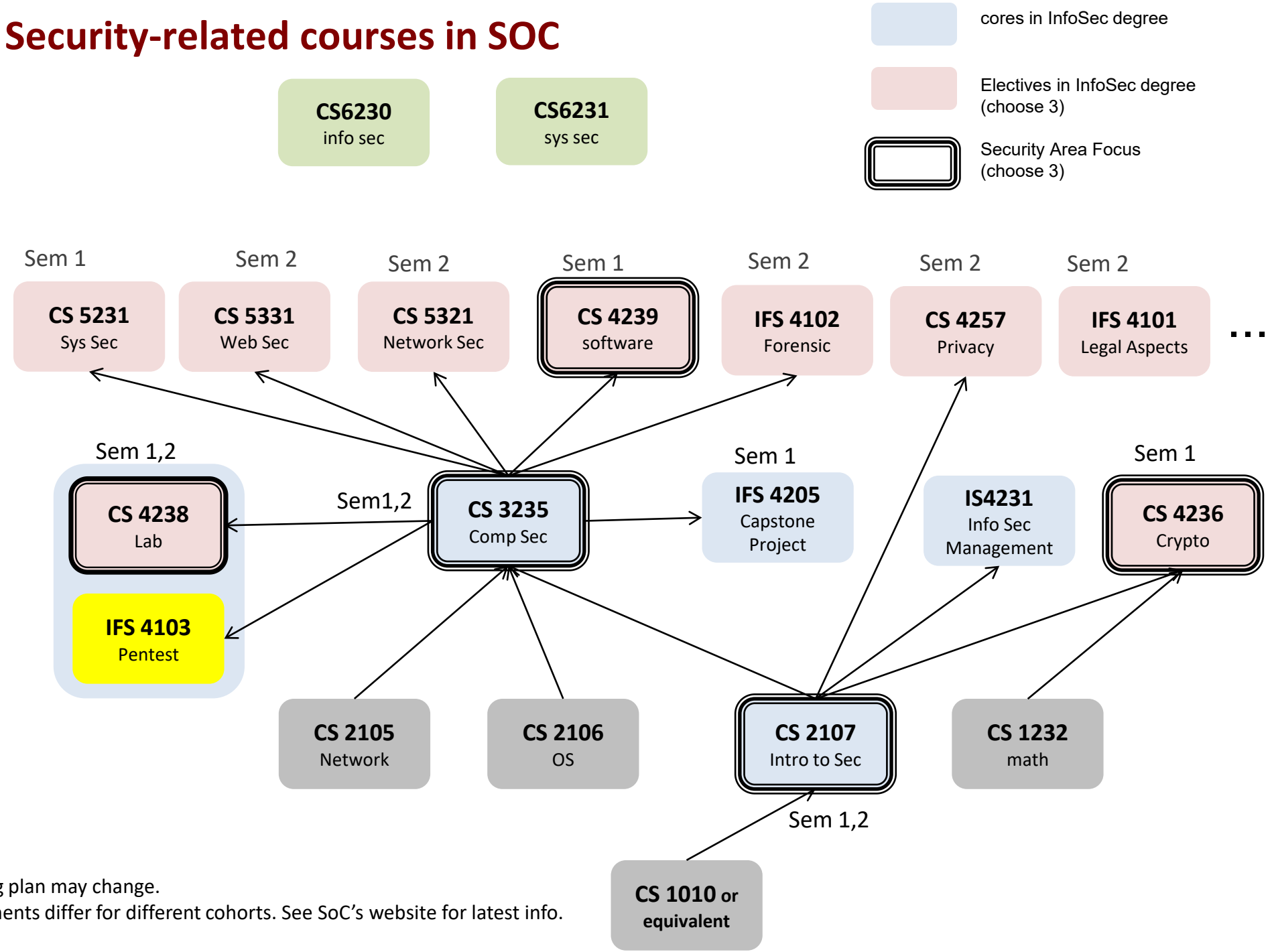
Intended Course Learning Outcomes (CLOs)

After completing the course, you will gain *practical real-word hands-on experience* on:

- **Scoping** a pen-testing exercise with a target organization
- **Planning** pen-testing phases using a *known methodology*
- **Performing** pen-testing using various offensive-security tools
- **Reporting** the results of the conducted pen-testing, and **suggesting** security counter measures (remediations)
- **Communicating** the findings

Important Note:
This course is *not* only about utilizing pen-testing tools, but also about learning *other activities & aspects* of a pen-testing project *by doing*

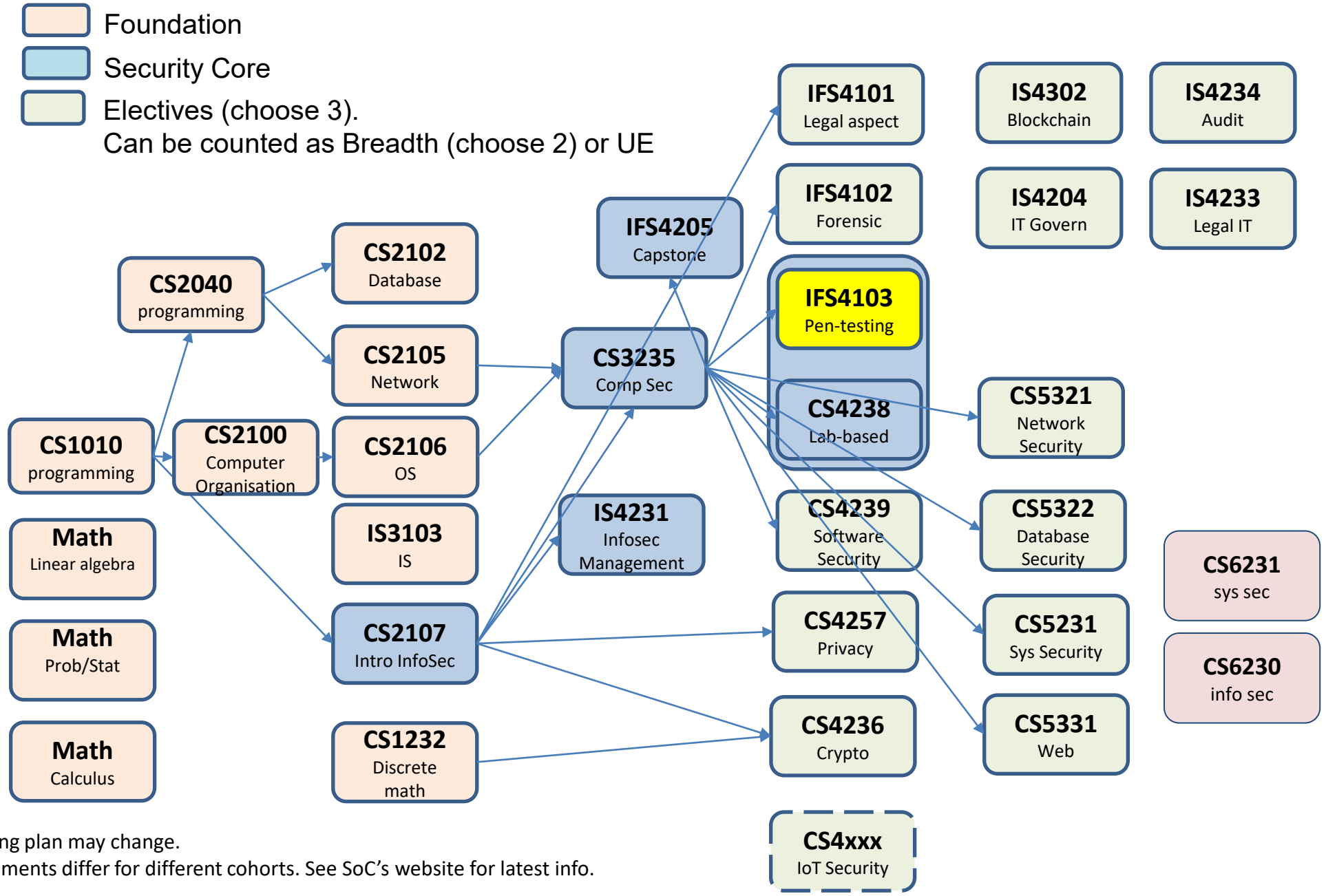
Security-related courses in SOC



Note:

1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

Security-related courses & BCOMP InfoSec requirements



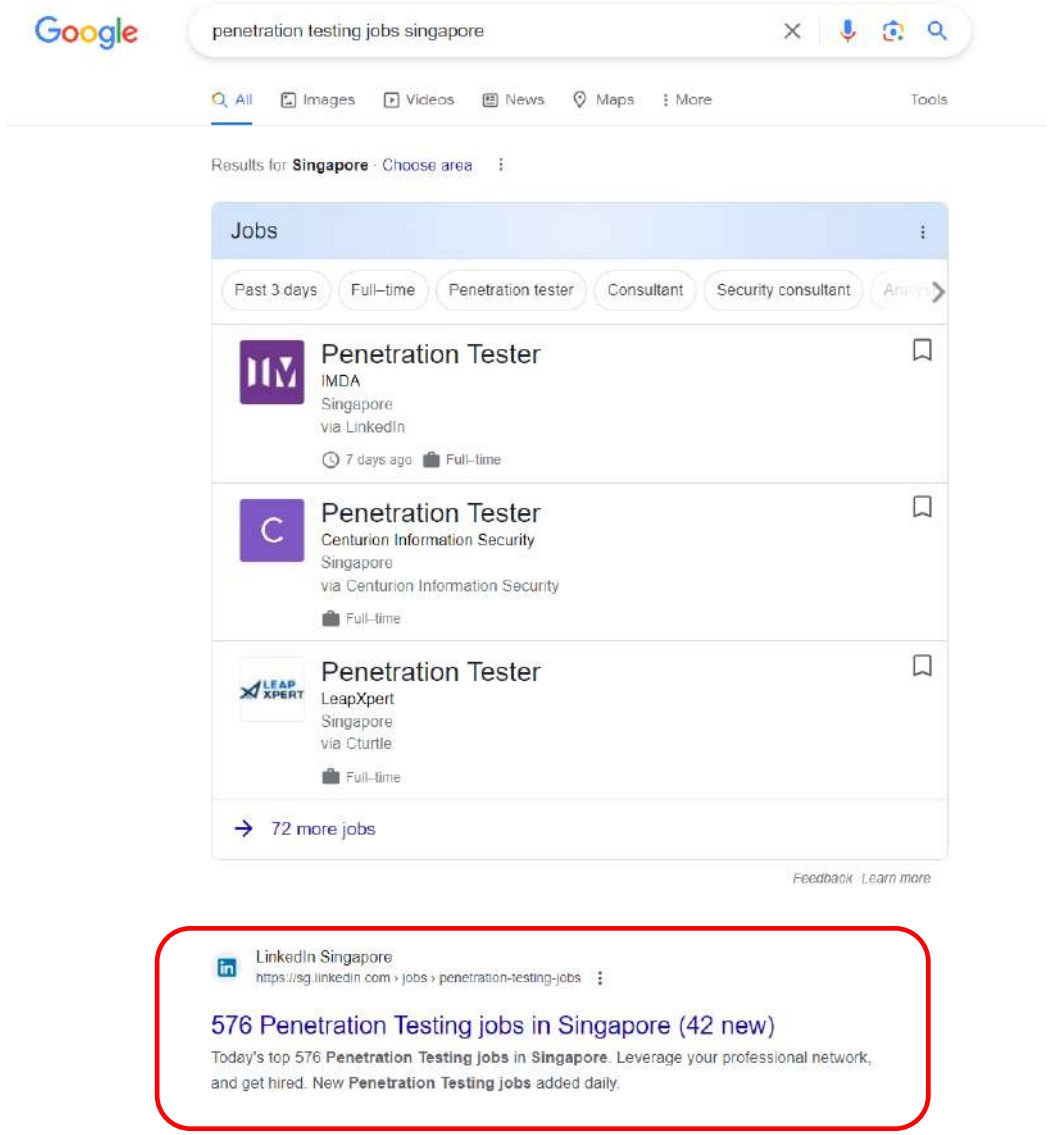
Note:

1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

What is Penetration Testing?

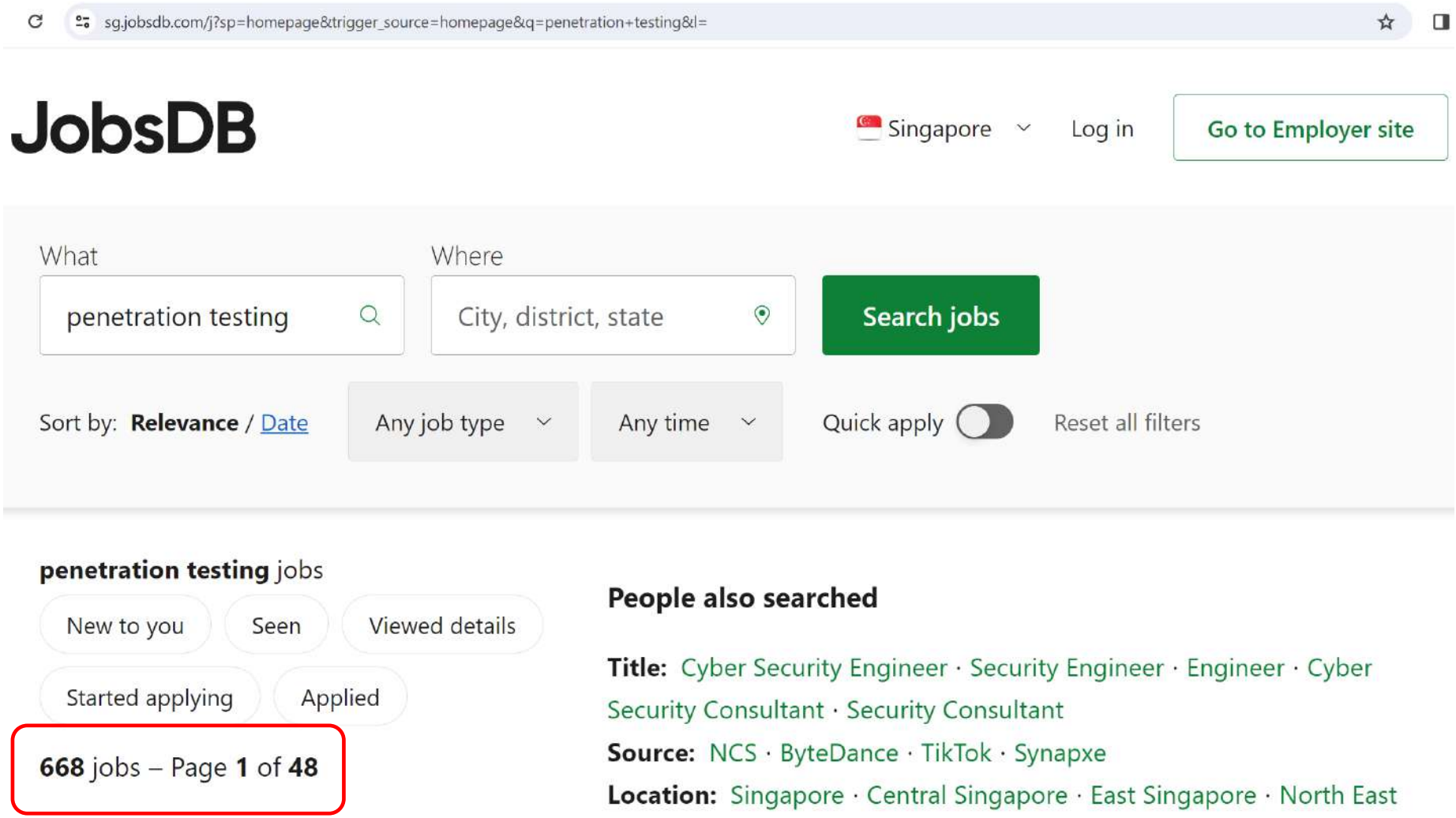
- Wikipedia:
  - "A penetration test, colloquially known as a *pentest* or *ethical hacking*, is an **authorized simulated cyberattack** on a computer system, performed to **evaluate the security** of the system; …"
  - "The test is performed to identify **weaknesses (or vulnerabilities)**, including the potential for unauthorized parties to gain access to the system's features and data, as well as **strengths**, enabling a **full risk assessment** to be completed."

Pen-Testing Jobs in Singapore



As of 17 Jan 2024

Pen-Testing Jobs in Singapore



As of 17 Jan 2024

Why Penetration Testing Practice Course?

- There is a strong need & demand for pen-testing service
  - https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/five-reasons-career-penetration-testing/
  - https://techcareers.smartnation.gov.sg/job-profiles/simulated-attack-specialist/overview/
- As a **follow-up** of some relevant cybersecurity courses in SoC:
  - **CS4238**: Computer Security Practice
  - CS4239: Software Security
  - **CS5331**: Web Security (*I'll share my past semester's lecture notes*)
- To provide a platform for experiencing a **complete pen-testing project**: from the scoping meeting to findings presentation

Difference with CS4238?

- CS4238:
  - Hacking **techniques**
  - Goal: understand how attacks work & possible countermeasures
- **IFS4103**:
  - ***Authorized*** simulated cyberattack (***ethical*** hacking)
  - Goal: **evaluate** the security of a **real** system (e.g. University's apps)
  - ***Beyond*** just hacking:
    - Scoping & staying in scope: the evaluation needs to be planned & done carefully
    - Description & PoC of found vulnerabilities, suggested remediation
    - Pen-testing project management with clients
    - Deliverables: pen-testing report & findings presentation

Course Relevance to Cybersecurity Education

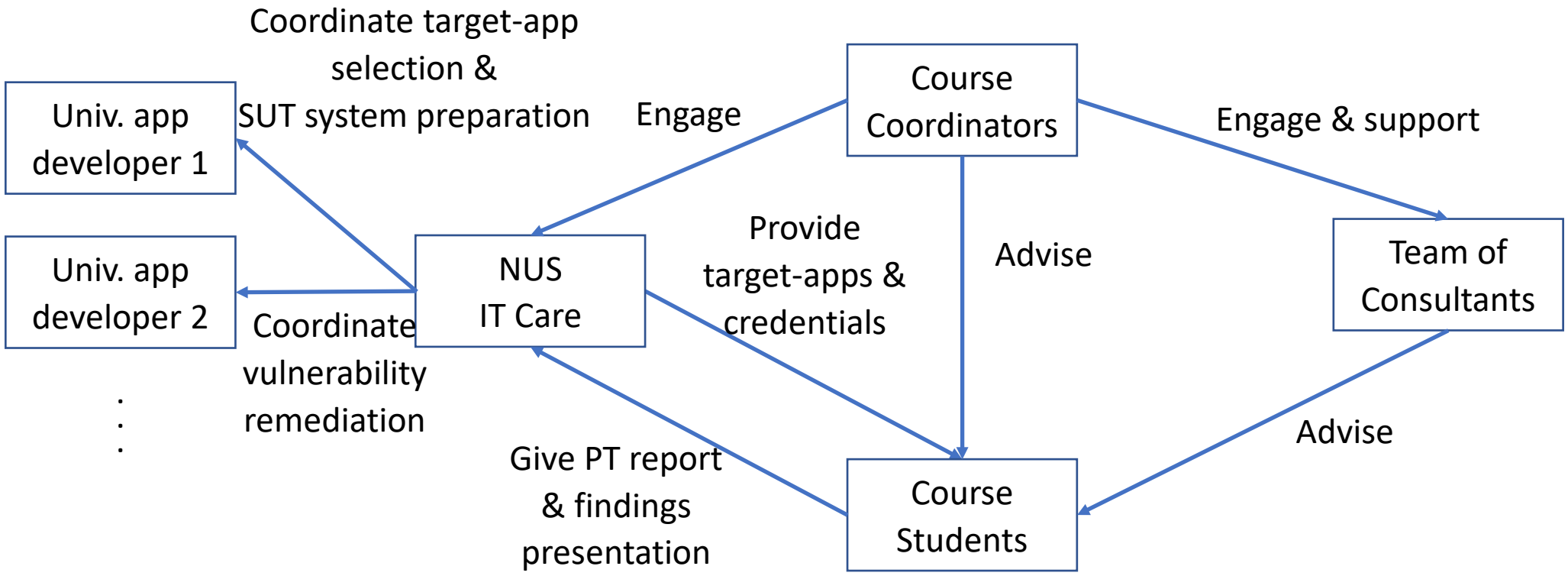
- **ACM/IEEE** Joint Task Force on Cybersecurity Education's "***Cybersecurity Curricular Guideline***":
  - **Penetration testing**: under system security knowledge area
  - **Ethical hacking**: under societal security knowledge area
- **NIST** National Initiative for Cybersecurity Education (NICE)'s "***Cybersecurity Workforce Framework***":
  - Defines **Vulnerability Assessment Analyst** (PR-VAM-001) **work role**: task includes conducting and/or supporting authorized pen-testing

Course Relevance to Cybersecurity Profession

- **Jones et al.** [ACM Trans. on Computing Education, 2018]:
  - Surveyed cyber professionals at the premier hacker conferences about **knowledge, skills & abilities** most important to their jobs
  - They considered **soft skills involved in pen-testing** (e.g. client communication, written communication, giving presentations) as **important**
  - In particular, ***communicating one's technical knowledge in a non-technical way***
  - Soft skills were mentioned most frequently to the question "Was there anything you've had to learn on the job that you wish you had learned in school?"
- **Kapoor et al.** [ACM TS on Computer Science Education, 2020]:
  - It explored participation of UG students in **industry internships**
  - About **45%** of the 486 students described that **they were building technical & professional skills, including ethical hacking**, by getting involved ***outside of coursework*** to prepare for securing an internship position

Our Pen-Testing Course Arrangement

- **Four parties** working **collaboratively** using **operational NUS apps**:
  - Students, pen-testing consultant (Ensign), NUS IT Care, CIT/SoC/…



Pedagogical Approach

- ***Authentic learning***:
  "educational & instructional techniques that focus on connecting what students are taught in school to **real-world issues, problems & applications**"
- ***Authentic assessments***:
  Mirror the tasks & problem solving that are required in the reality
- *"Authentic" → experiential*
- SoC & facilitator **role**:
  To provide **platform & support** for the students to engage in real-world connected **problem-solving**, **critical thinking**, **experience** & **reflection**

Your Benefits

- **Benefits** of the course:
  - **Hands-on experience** of pen-testing a realistic/real-world target systems
  - You can **help NUS systems** become more secure too
  - Guidance by **practising professional pen-testing team**
  - Also possible **follow-up recruitment**? *Why not!*
  - **Team work experience** in a project-based setting
  - Other **non-technical skills**: project management & client-facing skills
  - *Something very good for **your CV**!*

Teaching Mode

- Weekly contact hours:
  - Lecture : **Thursday, 1400-1600**
  - Lab : **Thursday, 1600-1700** (from Week 2)
- **Activity types** during contact hours:
  - Lecture
  - Hands-on lab
  - Scoping meeting: with *the clients*
  - Pen-testing sharing: with *your classmates*
  - Group discussion & consultation: with *the consultant team*
  - Presentation: to *the clients*
  - *Pizza party!*

Attendance & Recordings

- Course activities are conducted **F2F**
- It's important to **attend the classes**:
  - **Lectures**: on pen-testing methodology & management, web app pen-testing review + techniques, Burp Suite, ….
  - **Labs**: Burp Suite, web hacking practice
  - With **the consultant team**: mentoring, discussions, live pen-testing
  - Project 1: class pen-testing sharing + Q&A
  - Project 2: scoping, internal findings presentation, client presentation
- Attendance marks: **5 marks** (from **10** attended sessions)
- In general, we ***don't*** **do** any recordings:
  - For selected sessions (e.g. demos, presentations), we may have a Zoom recording as a kind of backup/reference

Teaching/Facilitating Staff & Online Resources

- SoC course coordinator:
  - Sufatrio (Rio): dcssu@nus.edu.sg
- Professional pen-testing consultant team:
  - **Ensign InfoSecurity** (https://www.ensigninfosecurity.com/)
  - 2 consultants involved
- IFS4103 **Canvas**: as communication & coordination media
  - **File**: for lecture notes, other materials (readings, relevant other SoC course materials)
  - **Announcement**
  - **Discussion** (forum): for discussion
  - *Please check it regularly!*

Other Involved Parties

- **NUS IT Care** (Computer Centre):
  - Website: https://nusit.nus.edu.sg/itcare/
- **Two** operational **NUS target systems**:
  - Developed by **NUS app developers**, maintained/monitored by NUS IT Care
  - Fully deployed or customized in NUS
  - **SUT systems**: real systems *but* not the production systems
  - Access to SUT systems will be **regulated** during the pen-testing:
    - E.g. based on SoC IP address range (accessible from outside via NUS VPN)
    - Limited pen-testing window period
    - *TBD during the scoping meeting!*

Learning Mode

- **Lectures & labs**: review web pen-testing techniques & tools
- **Projects**:
  - Primarily **self + team learning**, culminating in real-world pen-testing (Project 2)
  - You are expected to consider the course as **platform + mentoring + support + resources** that facilitate & support your self learning
- **The consultant team (Ensign)** provides advice & guidance as senior/experienced pen-testers
  - **Industrial perspective & sharing** on how they do their pen-tests
  - *Note*: different pen-testing companies can operate differently
  - Please **leverage** on their knowledge & experience (Q&A)

Tentative Schedule

IFS4103 Tentative Schedule: Semester 2 AY2023/24 (January-April 2024)								
Week No	Date (Thur)	Agenda	Activity Type					
			Lecture	Consultation	Presentation	Lab	Client Meeting	
1	18-Jan	Introduction to pen-testing, course administration						
2	25-Jan	Pen-testing methodology & management, CVSS + lab tasks						
3	01-Feb	Web app pen-testing review, release of group assignment + lab tasks						
4	08-Feb	Burp & web pen-testing sharing + lab tasks						
5	15-Feb	Burp & web pen-testing sharing + lab tasks						
6	22-Feb	Scoping meeting of NUS apps (teams to possibly pen-test both apps)						
		Recess Week (29-Feb, Follow-up meeting of NUS apps for credential issuance matters if still needed)						
7	07-Mar	Group-based web vulnerability & exploitation sharing						
8	14-Mar	Group-based web vulnerability & exploitation sharing						
9	21-Mar	Pen-testing of NUS apps & consultation						
10	28-Mar	*NUS Well-Being Day (no class)*						
11	04-Apr	Pen-testing of NUS apps & consultation						
12	11-Apr	Internal-group presentation & discussion						
13	18-Apr	Final pen-testing presentation with clients, module wrap-up						
		Sessions conducted by SoC						
		Sessions conducted by Ensign						
		Session conducted together by SoC & Ensign						

Course Grading

- 100% **Continual Assessment** (CA):
  - Class attendance (attend at least **10** out of 13 sessions): **5%**
  - Individual lab tasks: **20%**
  - Project 1: **25%**
  - Project 2: 40% + 10% = **50%**
  - ***No*** final exam
- **Two group-based projects**:
  - **New arrangements** for this semester: 2 different grouping
  - Project 1: Group-based web vulnerability & exploitation **sharing**
  - Project 2: Group-based **pen-testing** of NUS apps
- Course is **letter graded**

Project 1: Group-based Sharing

- Work in **a team of 4**: you can *self-form* your team
- Weightage: **25%**
- Presentations in **Weeks 7 & 8** (3+3 teams):
  - Each team's presentation (up to 1 hour): background of vulnerability + set-up & demo + Q&A
- Sharing on **web vulnerabilities & exploitations**:
  - A list of topics will be given in Week 3
  - Vulnerable code analysis & exploitation walkthrough
  - You can develop **your own** (simple) vulnerable web app
- Marks from other students, Ensign & course coordinator

Project 2: Pen-Testing Scenarios

- Possible **types** of system under test (SUT):
  - Web app – ***typical IFS4103 scenario***
  - Windows software/app
  - Mobile (Android) app
  - Network infrastructure
- **Access** type?
  - Black box: with near zero knowledge about the target system
  - Grey box: more knowledge about the system – ***typical IFS4103 scenario*** (with user credentials given)
  - White box: even more knowledge, e.g. source code

Project 2: Weightage & Team Formation

- **Total weightage: 50%**
  - Findings & report: **30%**
  - Presentation (Week 12): **10%**
  - Combined/delivered final report & client presentation (Week 13): **5%+5%**
- **Team formation:**
  - **Four teams** of 5-6
  - **Teams 1 & 2**: each works on **NUS target system #1**, to form **Team A** for the final presentation
  - **Teams 3 & 4**: each works on **NUS target system #2**, to form **Team B** for the final presentation
  - ***Note***: depending on the 2 NUS apps, each team may pen-test both apps

Team Formation

- Team member **allocation**:
  - "Semi-randomly" assigned!
  - Takes into account past InfoSec background & courses taken
  - To be finalised in Week 2 after your **questionnaire** submission
- **Background questionnaire**:
  - **Get** the form from Canvas File (under "`Lecture Notes`")
  - **Upload** your filled-out form to Canvas via "`Background questionnaire`" assignment before next week's class (25 Jan, 2pm)!

Project 2 Report: Assessment Rubrics

- The **total marks** possible for Project 2 report: **100**
- **Components/criteria**:
  - Vulnerability findings & validations reported: **50***
  - Report writing: **50***
    - Section completeness: **15**
    - Finding-details (including impact, mitigation) explanation writing & style: **20**
    - Report clarity/readability: **15**

Note: * The ratio can be adjusted *if needed*

Project 2 Presentation: Assessment Rubrics

- The **total marks** possible for each project presentation: **100**
- **Components/criteria** & respective weightages:
  - Slide content, lay-out & design, clarity/readability: **50**
  - Presentation: **35**
  - Q&A: **15**

Projects 1 & 2: Team Diary

- Each team keeps a **diary** (with shared editing)
- Could use Google Doc (requires Gmail IDs)
  or maybe Microsoft Teams (?)
- Record what each team member is doing:
  - Each team member should edit ***his/her own text*** only
  - Include **date** for each added entry
  - Use it as ***append-only*** **document**: even if you could re-edit past entries, just do it as a change-log while keeping the original past entries
- Free-format except for above rules

Notes on Group Marks

- Group marks of each project are **to be shared**
- ***But***, with a **possible moderation/deduction** based on **your team's** peer-review feedback:
  - Group marks of those with **no** contribution at all or **minimal** contribution will be moderated
  - The moderation will be determined based on teammate's comments & the **team diary**
  - *How about negative feedback from **only 1 teammate**?*
- **The message is**: please work together, contribute what you can, help & support each other, perform together as a team

Ice Breaking!

- **What** to share:
  - Your background
  - Your past information-security experience
  - What you would like to get out of the course
- **How** to help you share:
  - You can refer to the **prepared questionnaire**: uploaded to Canvas File (under "`Lecture Notes`")
  - Share your answers with your fellow friends

Break

(Please fill out your questionnaire)

Ice Breaking!

Source:
PowerPoint

- **What** to share:
  - Your background
  - Your past information-security experience
  - What you would like to get out of the course

What is Penetration Testing?

(Note: As general background information & field introduction)

Penetration Testing

- **Defined** as:

  "***authorized*** *simulated attack on a computer system, performed to* ***evaluate*** *the security of the system*" [Wiki]

- **Goal**:

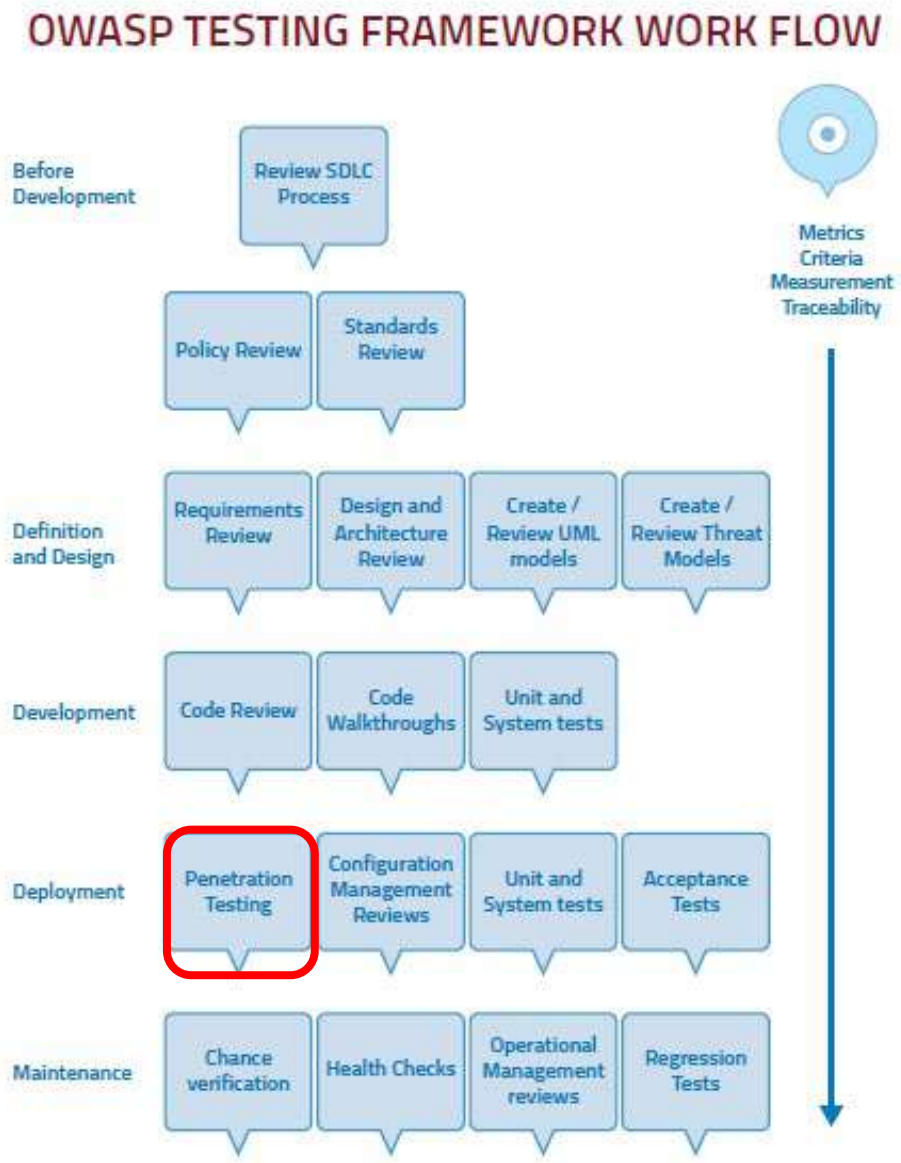
  To identify ***both*** weaknesses (vulnerabilities) as well as strengths, enabling a full risk assessment to be completed [Wiki]

- Security issues that the pen-test uncovers: should be reported to **the system owner *only***, and ***must be kept confidential***

- Possible **remediation** actions are usually suggested too

Where & Why is Penetration Testing?

- OWASP Testing Guide 4.0
- Software testing: developer testing, user testing, operation testing **+ *independent pen testing!***



Who Needs Penetration Testing?

- MAS, "*Technology Risk Management Guidelines*", 2013:
- **Section 9.4. Vulnerability Assessment and Penetration Testing**
  - 9.4.1 **Vulnerability assessment (VA)** is the process of identifying, assessing and discovering security vulnerabilities in a system. The **FI should conduct VAs regularly** to detect security vulnerabilities in the IT environment.
  - 9.4.4 The FI should carry out **penetration tests** in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. The FI **should conduct penetration tests** on internet-facing systems **at least annually**.

Types of Pen-Testing

- Based on the **given *information availability***:
  - **Black box** pen-testing:
    - No information except the company name or target asset URL is provided
  - **White box** pen-testing:
    - Comprehensive background & system information (including relevant credentials) are provided
  - **Grey box** pen-testing:
    - Somewhere in between
    - E.g. **user credentials** are provided (ABS, "*Penetration Testing Guidelines For the Financial Industry in Singapore*", 2015)

Types of Pen-Testing

- Based on **pen-testing *targets*** [see Rapid7's report]:
  - **External** pen-testing:
    - Focus on web-based attacks against the target organization's **web site** or **customer-facing web apps**, email-based phishing campaigns, and credential collection efforts via externally-facing **endpoints**
  - **Internal** pen-testing:
    - Focus on the **internal** LAN & WLAN, and the **systems** that are **not (intentionally) exposed** to the internet: payroll systems, factory floor equipment, internal source code repositories, etc.

Types of Pen-Testing

- The Association of Banks in Singapore (ABS), "*Penetration Testing Guidelines For the Financial Industry in Singapore*", 2015:
  - **Network** pen-testing:
    - Identification & assessment of weaknesses that may lead to vulnerabilities on **host systems & network devices** exploitable remotely from an external attacker's perspective
    - Network devices should include **wireless network** (e.g. AP) testing & **network infrastructure** testing
  - **Application** pen-testing:
    - Identification & assessment of weaknesses & vulnerabilities on **online systems** exploitable remotely from an external attacker's perspective
    - ***Web (IFS4103 scenario)*** *& non-web applications?*

(Yet Another) Penetration Testing Type

- Another classification of **pen-testing type (CompTIA)**: based on **testing *requirements* or *objectives***
  - ***Goal-based/objective-based***: assessment via a simulated cyber attacks
  - **Compliance-based**: PCI, HIPPA, …
  - **Read-team**:
    - Evaluates how well an organization would fare on a cyber-attack scenario, including APT
    - Tests: time to detect, time to response, time to recover
    - Can involve a lengthy process!

Vulnerability Assessment vs Pen-Testing

- For their **differences**, read:
  - "*The Difference Between a Vulnerability Assessment and a Penetration Test*", Daniel Miessler, 2018
- Depending on the **client's intent**:
  - To find out the security vulnerabilities; or
  - To determine the security resiliency of the application
- **Vulnerability Assessment** (VA):
  - A ***non/less-intrusive*** approach that serves to produce a prioritised list of security vulnerabilities

Vulnerability Assessment vs Pen-Testing

- **Pen-Testing** (PT):
  - Uses an **intrusive approach** to discover security weaknesses in the client's scoped target IT system (i.e. infrastructure & applications)
  - Pen testers would attempt to **exploit** identified security weaknesses to **gain privileged access** into the IT target system
  - Emulates **a real attack**, and would determine the robustness of the client's IT system in protecting sensitive information

Vulnerability Assessment vs Pen-Testing

- Main **difference**:
  - VA: helps **discover** the security loopholes but ***does not*** exploit the vulnerabilities
  - PT: demonstrates **how damaging** security vulnerabilities could be in a real cyber-attack
- Important note: your clients **may not be aware** of the difference, and what they really want
- Determine what they want during the **scoping meeting**
- *Can an organization do both VA and PT??*

Vulnerability Assessment Steps

- **General steps**:
  1. Assessment
  2. Identify exposures
  3. Address exposures
- Reference:
  - "*Vulnerability Assessments: The Pro-active Steps to Secure Your Organization*", SANS White Paper

Penetration Testing Steps

- **General steps**:
  1. ***Planning & preparation*** (pre-engagement):
     - Scope
     - Testing window
     - Contact information**:** *PIC as your PoC*
     - **Nondisclosure agreement (NDA)**
     - **Master Service Agreement (MSA)**:
       a "get out of jail free" card, payment terms
     - **Statement of Work (SOW)**
     - **Rules of Engagement (RoE)**

Steps of Penetration Testing

2. **Information gathering** & analysis
3. **Vulnerability detection**
4. **Penetration** attempt and possible post-exploitation
5. ***Clean up***
6. ***Reporting*:**
   - Executive summary
   - Technical report
   - Findings presentation

- Reference:
  - "*Conducting a Penetration Test on an Organization*", SANS White Paper

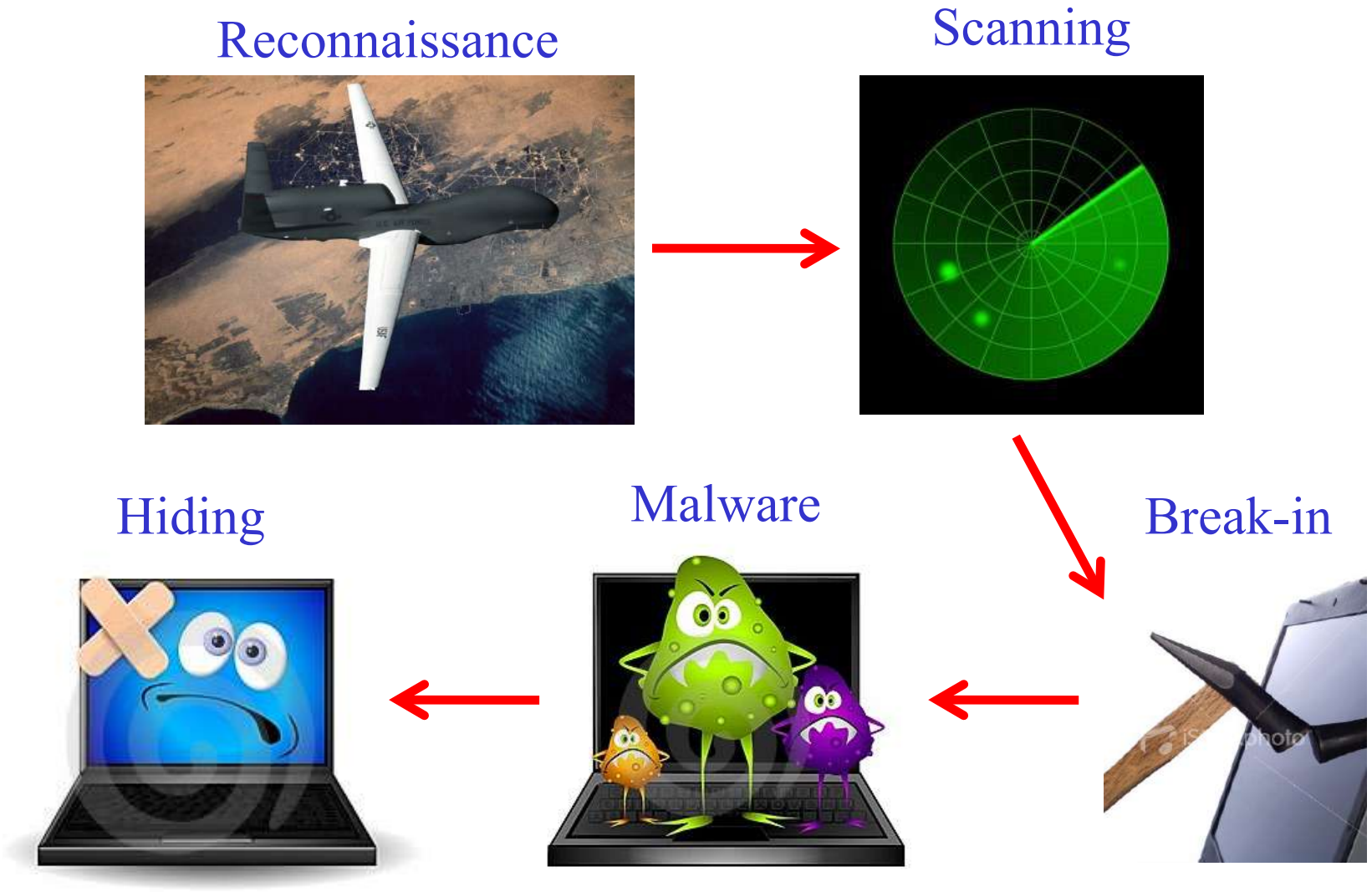
Contractual Agreements

- **Nondisclosure agreement (NDA)**:
  - For **your client** to protect its private information & intellectual property
- **Master Service Agreement (MSA)**: contains **contractual matters** between 2 or more parties, including:
  - A "get out of jail free" card/term!
  - Payment terms
  - Allocation of risks
  - Dispute resolutions
- **Statement of Work (SOW)**:
  - Outlines an organization's **project-specific work** to be executed by a service provider
  - Can be part of MSA

Contractual Agreements (Cont)

- **Rules of Engagement (RoE):**
  - Specifies **guidelines & constraints** of a pen-testing execution
  - Can be part of SoW or as a separate document
  - Example: "Appendix B—Rules of Engagement Template" of *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115 (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf):
    - **Introduction**: Purpose, scope, assumptions & limitations, risks
    - **Logistics**: Personnel, test schedule, test site, test equipment
    - **Communication Strategy**: General communication, incident handling &response
    - **Target System/Network**: including the "exclude list"
    - **Testing Execution**: Nontechnical & technical test components, data handling
    - **Reporting**
    - **Signature Page**

Differences with the Usual Attack Steps



Differences with the Usual Attack Steps

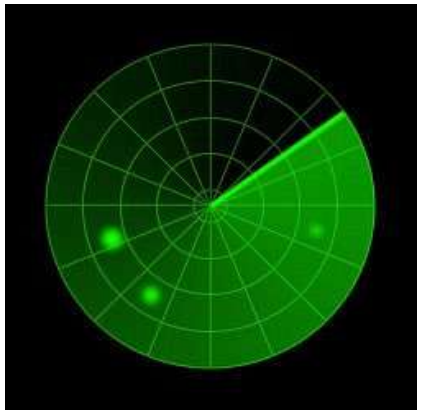
- **Pen-testing** stages:
  - ***Pre-engagement***: planning & scoping
  - Information gathering: reconnaissance & scanning
  - Attack: vulnerability analysis & exploitation (vulnerability verification!)
  - Post-exploitation: testing ***cleaning up***
  - ***Reporting***
- Omitted CS4238's attack stages:
  - Post-exploitation to *maintain access*
  - Post-exploitation to *hide attacks*
- Two new important stages:
  - **Pre-engagement**: planning & scoping
  - **Reporting**

Pen-Testing Stages

Pre-engagement

Reconnaissance

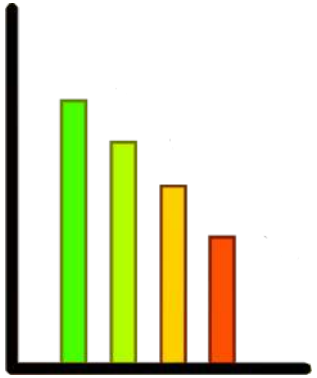
Scanning



Break-in

Clean-up

Reporting



Scoping: Main Matters & Inputs

To be Revisited Later!

- Main **matters** to address:
  - Target selection
  - Testing requirements
  - Testing strategy & methodology
  - Scheduling & timelines
  - User credentials required: depending on type of testing (no/limited access, user-level access, admin/privileged-level access)
- How to seek your **client's inputs** on these matters:
  - Scoping or **pre-engagement survey/questionnaire**: e.g. http://www.pentest-standard.org/index.php/Pre-engagement → Questionnaires
  - Discussion during scoping or kick-off meeting(s)

Scoping: Other Additional Considerations

To be Revisited Later!

- Other important **questions/issues** to discuss are below
- **Third-party** involvement
  - Cloud services: Any specific procedures for pen-testers to follow, permission request forms, scheduling, …
  - ISP: Specific ISP provisions for pen-testing
  - Countries where servers are hosted
- **Stress** or **DoS** testing
- **Coordination/communication arrangements**:
  - Lines of communication
  - Emergency contact information
  - Incident reporting process that is in place

Seven Important Tips on Conducting Pen-Testing

Seven Important General Tips

- The following are **7 important tips** that are useful when conducting a pen-testing project, especially a real project
- You need to be aware of potential issues **from the very beginning**!
- **More tips** & best practice from our professional consultant team later as we go along

#1: Stay within Pen-Testing Scope

- Know the pen-testing scope and **stay** within that scope
- Going out of the scope is considered a **serious offence**
- E.g. banking clients:
  - Usually have an independent **Incident Response (IR) team**, that will monitor any conducted pen-testing
  - Should a scope violation occur, the IR team will come in & seize the notebooks/PCs used in conducting **any out-of-scope activities**
  - Subsequently, a **digital forensic (DF)** analysis will be performed to recover the proof of any misconducts done

#2: Don't Breach Non-Disclosure Agreement (NDA)

- NDA: a **legal contract** among the involved parties that outlines confidential material, knowledge, or information that the parties wish to share with one another, but wish to restrict access to or by third parties
- Understand the signed NDA & the **consequences** of any misconducts
- Understand your **responsibilities** too
- For our course:
  - Specially set-up SUT/pre-production systems
  - Yet, keep all the findings confidential!

#3: Be aware of Potential Risks on Data

- Risks of pen-testing activities on target systems:
  - **Data disclosure**: information leakage
  - **Data erasure**: system unavailability, especially on production systems
- Web pen-testing can **easily delete** important data stored on the web/database server
- An experienced web pen-tester will be very careful in spidering target web links & invoking **operations that could delete data**
- In many cases, a **simpler PoC** without data erasure is sufficient

#3: Be aware of Potential Risks on Data

- If the links & operations that could delete data (e.g. dangerous SQLi operations) are in scope & allowed, then **their invocations should be done last**
- Sometimes **extra permissions** are also needed, which can be obtained during the scope meeting and/or pen-testing stages
- Always ask your client to **snapshot/backup** their data before your pen-testing!

#4: Plan Your Pen-Testing & Time It Well

- Usually there is a **limited time period** where a particular target system is open for pen-testing
- This is particularly true for **production-related** systems: e.g. during off hours only
- It may apply to **SUT systems** too: e.g. daily back-up period
- The client needs to specifically assign/limit the testing period, and usually also **monitor** the systems during this period
- **Plan** your testing well w.r.t. the given time period
- **Manage** your time well, and make the most of it too!

#5: Document Your Steps & Findings

- Any found vulnerabilities must be supported by **well-documented facts**
- Don’t forget to document your key **pen-testing steps** as well
- A pen-testing report can be used for regulatory **compliance purposes** & potential follow-up **risk assessment**
- Given a good documentation of vulnerability existence, the client cannot **possibly deny** any vulnerabilities found during the pen-testing

#6: Hack Well & Report Well Too

- For your pen-testing, you can adopt well-known methodologies:
  - **OWASP Web Security Testing Guide (WSTG)** for web app pen-testing
  - **Common Vulnerability Scoring System (CVSS)** for severity rating
- Report writing is ***not*** a **supplementary** activity
- It is ***not*** enough to only discover & exploit vulnerabilities,
- **Document** the findings & communicate them properly
- Pen-testing report as a **deliverable**, and also basis for further remediation/assessment actions by the client
- Your report must be easily understandable & **non-judgmental**: you want to help your clients!

#6: Hack Well & Report Well Too

- Hacking skill is ***not*** everything:
  many big pen-testing companies recruited their staff/interns
  by asking them to hack a system and **then**
  write a mini report documenting the findings
- Importance of a **limitation/caveat section**,
  which mentions: any untested system components,
  omitted in-scope pen-testing activities,
  encountered performance or technical issues
- **Good news**:
  - Some **standard report templates** are available
  - More on these templates later!

#7: Present Your Finding Professionally

- You need to deal with your client's technical staff members as well as **management**
- Different **levels of detail** in your report & presentation
- Be **professional** in your presentation & dealings with your client
- Pen-tester's motto:
  "hack as a hacker, present/deal as a professional"

Get Ready for Next Week

- Set up your **pen-testing work environment**:
  - Install **VirtualBox/VMware**
  - Set up a **Kali Linux machine** as your hacking system
  - Install **Burp Suite**: either on your Kali Linux or your host system
- **Lab 1A**: Slides on VirtualBox, Kali Linux, Burp Suite intro
- **Lab 1B**: Test your Kali machine by **inspecting web data** using command, browser DevTools, browser extension

- **Your To-Do (as your 1st lab session)**:
  Do set up your pen-testing environment before next week!

Next Week's Lecture by Ensign

- Lecture & discussion on **pen-testing methodology**
- Some **interesting questions** to ask about the methodology:
  - Can we use 3-rd party hosted apps? Any privacy concerns?
  - Is a good vulnerability scanner (e.g. Nessus, Burp Suite's Scanner/Audit) sufficient for a pen-testing?
  - How many reported vulnerabilities are too many?
  - What if your client challenges you that your reported exploit did not actually exist/apply?
  - How do you record your vulnerability information in your workflow before you explain them in your report?
  - …
- A **Google Sheets spreadsheet** to pool the questions to ask

Some Useful References

- "*Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*", 2nd Edition, Edward Skoudis and Tom Liston, Prentice Hall, 2006
- "*Penetration Testing: A Hands-On Introduction to Hacking*", Georgia Weidman, No Starch Press, 2014
- "*CompTIA PenTest+*", Raymond Nutting, McGraw-Hill Education, 2018
- "*Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems*", 1st Edition, Ric Messier, Apress, 2016 (electronic resource is available at NUS library)
- *[More on Web pen-testing later]*

Other Reading & Resource

- "*UNDER THE HOODIE: Lessons from a Season of Penetration Testing*", Rapid7 Global Consulting, July 2018
  (a copy has been uploaded to Canvas Files' Resources folder)
  - **Goal**: to demystify the practice of penetration testing by **surveying those who are in the field** & conducting the investigations on what they **most commonly see** during client engagements
  - **Content**: the results of 268 engagements, conducted from early September 2017 through mid-June 2018
  - *Please read the article before your next lecture*
- You can also watch the associated videos of "*True Stories from Rapid7 Pen Testers*"

Questions?

Lab 1A & Lab 1B

Thanks!
See you next week
(together with our Consultant Team)!