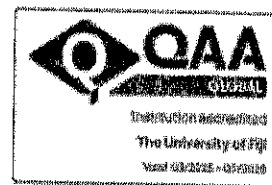


The University of Fiji
(An Entity of Arya Pratinidhi Sabha of Fiji)



SCHOOL OF SCIENCE AND TECHNOLOGY
Semester 2, 2025

FINAL EXAMINATION PAPER

ITC333: DISTRIBUTED SYSTEMS TECHNOLOGY

Important Instructions to Students:

1. Read the questions, instructions carefully and answer the questions.
2. You are allowed an **extra 10 minutes reading time** (during this time, you are not allowed to write with pen) and **180 minutes (3 Hours) to complete this paper**.
3. Silent, non-programmable calculators are allowed, but not supplied.
4. Write all your answers in the answer booklet provided. If you need extra sheets, please ask from the supervisor. Write your name, course code and student identification number in the answer booklet and in the attendance sheet.
5. This paper contains four (4) sections A, B, C and D. All questions are compulsory to answer.
6. Write all your answers legibly. The marker has the right to award zero for answers that are not legible.
7. This is a **Closed Book Examination**. The University views plagiarism, cheating and dishonest practice as serious offences and if found, offenders are penalized.

Examination Paper Content (Format):

<u>Section</u>	<u>Question</u>	<u>Content</u>	<u>Marks</u>	<u>Suggested Time</u>
A	1-5	True or False Questions	10	18 minutes
B	6-10	Multiple Choice	10	18 minutes
C	11	Matching	40	72 minutes
D	12-18	Case Studies	40	72 minutes
		TOTAL	100	180 Minutes

Registered with the Fiji Higher Education Commission as a University under the Higher Education Act 2008.
Registration Certificate Number (RGN0020/11)

Section A: True/False (10 Marks)

Instructions: Choose True or False for each statement.

1. The Blue Team is responsible for launching authorized attacks against an organization's systems.
(True / False)
2. Dumpster diving is considered an example of passive information gathering.
(True / False)
3. Passive reconnaissance techniques include methods like social engineering and phishing.
(True / False)
4. WEP is still considered a secure wireless encryption protocol for business use.
(True / False)
5. Tailgating is a form of physical security attack where an unauthorized person follows an authorized person into a restricted area.
(True / False)

Section B: Multiple Choice (10 Marks)

Instructions: Choose the letter of the correct answer.

6. Penetration testing should be performed under which of the following circumstances? Choose all that apply.
 - A. A new computer system has been installed.
 - B. A new software system or an update to a software system has been installed.
 - C. Following a regular schedule to make sure no unknown changes have impacted security.
 - D. Performed as dictated by compliance standards such as PCI DSS.
7. During vulnerability scanning, the process of entering random data into all the input fields of applications to make sure input is validated is known as which of the following?
 - A. Fuzzing
 - B. Stress testing
 - C. FIPS
 - D. SQL injection
8. What are some of the ways of building a list of valid user accounts? Choose all that apply.
 - A. Gathering usernames and email addresses using OSINT tools
 - B. Using brute-force tools
 - C. Extracting usernames from /etc/passwd or c:\users
 - D. Guessing
9. What type of wireless attack attempts to force systems to disconnect from an AP?
 - A. Jamming
 - B. Eavesdropping
 - C. Spoofing
 - D. Deauthentication
10. During vulnerability scanning, the process of entering random data into application input fields to check input validation is called:
 - A. Fuzzing
 - B. Stress testing
 - C. FIPS
 - D. SQL injection

Section C: Matching (40 Marks)

11. Match the descriptions of the penetration testing tool/library with the letter of tool/library from the last table (each matching is worth 1 mark). Here is an example answer:

a) G

Pre-engagement & Legal / Ethics

Description	Tool / Library
a) A formal, signed agreement that defines what testing is authorized (assets, time windows, prohibited activities such as DoS), legal protections for both parties, and contact/escalation paths. Keep versioned copies and store signatures.	
b) A concise written document that lists the in-scope and out-of-scope assets, permitted techniques, reporting expectations, and approved test hours. Use it to prevent ambiguity and accidental boundary-crossing.	
c) A communication & scheduling system (Jira ticket, dedicated test email, or phone contact list) used to schedule testing windows, coordinate outage windows and report urgent findings. Include an incident contact and escalation chain.	
d) A repeatable pre-test checklist covering legal checks, backups, whitelisting test IPs, data handling rules, and rollback procedures. Must be completed before any intrusive activity.	
e) A standardised calculator or reference (CVSS calculator, severity matrix) to assign objective severity scores and prioritise findings in the final report.	

Lab Setup & Target Configuration

Description	Tool / Library
f) Debian-based penetration testing distribution preloaded with hundreds of security tools (Nmap, Metasploit, Burp, Aircrack, John). Use OVA/ISO images for repeatable attacker VMs; keep snapshots and isolate network interfaces for safety.	
g) Deliberately vulnerable Ubuntu-based VM provided by Rapid7 for safe exploit practice; contains intentionally misconfigured services and example credentials. Use only in isolated lab networks and restore snapshots after exercises.	
h) Type-2 virtualization host widely used for labs; supports host-only/internal networks, multiple VM snapshots, and OVA import — useful for isolating attacker and target VMs from the host network.	
i) Legacy Windows desktop OS image used as a vulnerable target for compatibility and legacy-OS testing; useful to demonstrate risks from unsupported systems. Run as isolated VM and snapshot before tests.	
j) Modern Windows desktop OS image representing current endpoint configurations; useful as a realistic target for client-facing scenarios and patch/hardening exercises.	
k) Server OS image for domain controller and AD testing; use trial licenses in labs, create realistic AD objects (users, GPOs), and isolate from production.	
l) Intentionally insecure PHP/MySQL web application used to practise web attacks (SQLi, XSS). Install in an isolated webserver VM and use it for safe hands-on labs.	
m) Full-featured mail server appliance used as a target for mail-flow, authentication, and spam/phishing simulation labs; keep as an isolated VM and monitor logs for exercises.	

Reconnaissance (Passive & Light Active)

Description	Tool / Library
n) OSINT collection tool that queries public sources (search engines, PGP, LinkedIn, certificate transparency logs) to harvest subdomains, email addresses, and hostnames. Outputs CSV/text for recon logs. Use passive mode initially.	
o) Internet-of-Things / service search engine that indexes banners and exposed devices; use to discover externally reachable services (e.g., Elasticsearch, exposed SSH) and to validate whether devices are internet-exposed.	
p) Registrar and domain record lookup that returns registrant, registrar, creation & expiry dates and name servers; useful to identify administrative contacts or overlapping domains.	
q) Subdomain discovery tool that aggregates DNS records and OSINT sources to enumerate subdomains (wordlists, certificate transparency). Useful before active checks — helps scope assets to test.	
r) Technique of crafting focused Google search queries (filetype:, inurl:, site:) to locate exposed files, backup directories, credentials in public index, or sensitive pages; log queries and results.	
s) Command-line DNS tools used for light active DNS validation: <code>nslookup</code> / <code>dig</code> to retrieve A, MX, TXT, SOA records and to test for DNS zone misconfigurations; document queries and rate-limit requests.	

Scanning & Enumeration

Description	Tool / Library
t) Network discovery and port/service scanner. Common uses: ping sweeps (<code>-sn</code>), TCP SYN scans (<code>-ss</code>), service/version detection (<code>-sv</code>), OS fingerprinting (<code>-o</code>), and scripting engine (NSE) for additional checks. Save XML/grepable outputs for reporting.	
u) Packet capture and protocol analyzer for inspecting traffic, reconstructing HTTP/TCP sessions, and verifying unexpected transport behavior. Use pcap captures for proof-of-concept and to validate false positives from scanners.	
v) Web server scanner that checks common CGI, server misconfigs, plugin versions and known issues (not exhaustive). Good as a fast surface scan; follow-up manual verification recommended.	
w) Network vulnerability scanner that performs authenticated/unauthenticated checks, CVE correlation and reporting. Use for higher-level vulnerability discovery and to prioritise remediation.	
x) Simple TCP/UDP socket utility for banner grabbing, port listening, simple file transfers, and manual interaction with services; handy for quick verification when scripting or tool output is ambiguous.	

Exploitation (Web & Service Exploits)

Description	Tool / Library
y) Comprehensive exploitation framework with a large module library, payloads, and post-exploitation helpers. Use for validated, scoped exploits and for building PoC payloads in red-team style exercises — always document module, options and why it was chosen.	
z) Web application proxy and scanner that intercepts HTTP(S) traffic, supports manual tampering (Intruder/Repeater), automated scanning (Scanner — pro), and extensions (Burp Extender). Central tool for web testing and proof-of-concept generation.	
aa) Automated SQL injection detection and exploitation tool; supports DB enumeration, data extraction and various injection techniques. Use read-only or non-destructive options in production; always get permission.	
bb) Target web application intentionally full of web vulnerabilities; used as a practice ground for payload crafting, parameter tampering and learning mitigation techniques.	

Post-Exploitation & Lateral Movement

Description	Tool / Library
cc) Credential-dumping utility that extracts plaintext passwords, NTLM hashes, and Kerberos tickets from Windows memory; useful to demonstrate credential exposure. Use only with explicit permission and document exactly what was retrieved.	
dd) Collection of PowerShell scripts and modules for Windows post-exploitation tasks (discovery, privilege escalation checks, persistence helpers). Use with caution, log all commands, and avoid destructive payloads.	
ee) Graphing and query tool that takes AD data (collected with SharpHound) to map relationships, expose privilege paths, and prioritise lateral-movement opportunities. Produces clear visualisations for reports.	
ff) Lightweight remote shell/transfer tool useful for establishing reverse/forward shells in lab contexts and for moving files during post-exploitation.	

Password Attacks & Cracking

Description	Tool / Library
gg) Flexible offline password-cracking suite that supports many hash formats, hybrid/dictionary/rule-based attacks and incremental modes. Good for CPU-based cracking and pre/post-processing of results.	
hh) High-performance GPU-accelerated password recovery tool supporting many hash formats and advanced rule engines; ideal for large-scale or complex hash cracking when GPUs are available. Requires appropriate hardware and careful license/usage considerations.	
ii) Parallelized network login cracker for online services (SSH, FTP, HTTP(s), etc.); useful for testing lockout and rate-limiting policies. Use only in-scope and during agreed windows because it may trigger alarms or lock accounts.	

Wireless & Network Attacks

Description	Tool / Library
jj) Suite for wireless auditing: <code>airodump-ng</code> to capture frames/handshakes, <code>ai replay-ng</code> for injection/deauth (only if allowed), and <code>ai rcrack-ng</code> to perform offline cracking against captured handshakes using wordlists.	
kk) Wireless monitoring and intrusion detection tool that passively discovers APs and clients, detects rogue APs and collects statistics; useful for site surveys and defensive discovery of misconfigurations.	

Social Engineering & Physical Security

Description	Tool / Library
ll) Toolkit for building social-engineering payloads: phishing webpages, email templates, USB-based payloads and more. Integrates template libraries and supports safe testing flows — always operate with signed client consent and an exclusion list.	
mm) Open-source phishing platform for designing, sending, and tracking simulated phishing campaigns with user-friendly dashboards and landing pages. Use for controlled awareness tests with immediate remediation/education workflows.	
nn) Used to test client-side (browser) vulnerabilities by hooking browsers and executing payloads or scripts through them. Enables ethical testers to assess web-based security controls, session handling, and user awareness — should only be used in isolated, authorized lab environments.	

List of Tools/Libraries

Letter	Tool / Library
A	Nmap
B	Kali Linux
C	Retest checklist
D	PowerSploit
E	WHOIS
F	DVWA (Damn Vulnerable Web App)
G	Rules of Engagement / Authorization letter
H	Aircrack-ng
I	Metasploitable2
J	Burp Suite
K	OpenVAS / Greenbone
L	Hashcat
M	theHarvester
N	Netcat (nc)
O	Windows Server 2019
P	Google dorking
Q	Axigen Mail Server
R	CVSS / Severity scoring tools
S	Sublist3r
T	Nikto
U	Shodan
V	Communication plan / Ticketing (Jira / email)
W	Mimikatz
X	Wireshark
Y	Scope document
Z	John the Ripper
AA	SQLmap
BB	Kismet
CC	Hydra
DD	Technical finding template
EE	Metasploit Framework
FF	Engagement checklist
GG	GoPhish
HH	Windows 10
II	Social Engineering Toolkit (SET)
JJ	Executive summary template
KK	Oracle VirtualBox
LL	Remediation tracker / Jira
MM	Nslookup / dig
NN	Microsoft Windows 7
OO	BloodHound

Section D: Case Studies (40 Marks)

12. Case Project: Determining Legal Requirements for Penetration Testing

(6 marks)

Bongo Island Properties Ltd, a large real estate and tourism management company based in Solovi, Nadi, has contracted your cybersecurity consulting firm to conduct a penetration test on its corporate computer network. The company manages luxury resorts, golf courses, marinas, and fine-dining restaurants across Fiji's western division.

You are only authorized to interact with Mr *Charfar Singh*, the company's Chief Operating Officer (COO). To preserve the realism of the test, no internal IT staff or other employees will be informed or involved. Charfar wants to assess how much information you can uncover about the company's network infrastructure, topology, and any potential vulnerabilities without internal support or credentials.

Based on this scenario, write a **brief** version of a pre-engagement report that outlines the key steps you must take before beginning the penetration testing project. Ensure the report demonstrates a solid understanding of:

- Legal authorization
- Consent and contractual obligations
- Data privacy and handling protocols in Fiji

13. Creating a Pre-vulnerability Scanning Report

(5 marks)

Bongo Island Properties Ltd has contracted your computer consulting company again to perform a penetration test on its computer network. The company owns property that houses a five-star hotel, golf courses, tennis courts, and restaurants.

Charfar Singh has agreed that your findings so far warrant continuing your penetration-testing project on to the vulnerability scanning phase. Before you begin vulnerability scanning, Charfar wants you to provide a documented outline of the tools you plan to use and the types of tests you plan to perform. Your pen testing has identified a group of three web servers, two web applications, and one SQL database server that you recommend should be scanned for vulnerabilities.

Based on this information, write a **brief** report outlining the vulnerability tools and tests to perform on each target and the types of vulnerabilities you might find.

14. Creating a Target Exploitation Plan

(5 marks)

Bongo Island Properties Ltd, has again contracted your computer consulting company to perform a penetration test on its computer network.

Charfar Singh, is again your current contact for this stage of the project. Your pen testing identified a group of three web servers, two web applications, and one SQL database server, which you have scanned for vulnerabilities. Your scan results have revealed a number of vulnerabilities that you would like to attempt to exploit. Charfar has agreed that your findings warrant performing further testing on these systems, but before authorizing you to begin, Charfar wants you to provide a documented outline of the tools you plan to use and the types of exploits you plan to perform.

Based on this information, write a **brief** report outlining the types of exploits you would like to attempt and the tools you would like to use.

15. Case Project: Creating a Wireless Attack Plan Report

(6 marks)

Bongo Island Properties Ltd, has once again contracted your cybersecurity consulting firm to conduct a penetration test on its corporate computer network. The company manages luxury resorts, golf courses, marinas, and fine-dining restaurants across Fiji's western division.

The project has reached the stage where you would like to perform some network-based attacks to test the security of the systems you have identified. Charfar Singh is again your current contact for this stage of the project. He wants you to provide him with a similar report outlining your plans for pen testing her organization's wireless infrastructure. Your pen testing identified three areas of concern:

- The presence of several wireless network SSIDs, some of which do not follow the organization's standard naming convention
- Weak encryption protocols being used on some of these wireless networks
- WPS seems to be enabled on some WAPs

Based on this information, write a **brief** report outlining the types of wireless network attacks you would like to perform and the tools you would like to use.

16. Case Project: Web Application Testing

(6 marks)

The head of network security at Bongo Island Properties Ltd, Charfar Singh now wants you to provide a similar report outlining your plans for pen testing the organization's web applications.

Your pen testing identified three areas of concern:

- Several web servers running older versions of Apache software
- Several SQL servers running older versions of MySQL
- No indications that secure programming practices are part of the software development team's culture.

Based on this information, write a **brief** paragraph, listing the main application tests you would run for these concerns (old Apache, old MySQL, lack of secure coding) and name the primary tools you would use.

17. Creating a Host Attack Plan Report

(6 marks)

Bongo Island Properties Ltd has again contracted your computer consulting company to perform a penetration test on its computer network. The project has reached the stage where they would like to perform some pen testing directly targeting specific host computers you have identified in your reconnaissance phase.

Some of these hosts are real computers, some are virtual machines, and some are hosted in the cloud. Charfar Singh, the company's cloud specialist, is again your current contact for this stage of the project and now wants you to provide a similar report outlining your plans for this stage of pen testing. Your pen testing identified three areas of concern:

- Some cloud-based resources may be using default settings.
- You suspect that the company's password policy is weak, and you may be able to crack passwords and gain access to systems.
- When you asked how many hosts were virtual machines and how many were real computers, nobody could give you a definitive answer.

In one **short** paragraph, describe the three main host checks you would perform for the identified risks (cloud defaults, weak password policy, unknown VM vs physical hosts) and name one or two primary tools you would use for each check.

18. Creating A Social Engineering Attack Plan Report

(6 marks)

Bongo Island Properties Ltd has again contracted your computer consulting company as they would like to perform some social engineering pen testing to discover if the organization is vulnerable to social engineering attacks. Charfar Singh wants you to provide a similar report outlining your plans for this stage of pen testing. Your pen testing identified three areas of concern:

- The company email system does not seem to have any anti-phishing features or phishing reporting capabilities.
- Your research has indicated that the majority of staff seem to use the same social media website several times a day.
- You have observed employees from a variety of delivery companies being allowed entry to the building with little or no security checks.

In one **short** paragraph, describe the social-engineering tests you would run for the identified risks (no anti-phishing features, frequent staff social-media use, and lax delivery-person entry) and name the main tools or techniques you would use.

THE END

