

### OVERVIEW

The main idea of our project is to conduct penetration tests on the Saint Martin's University cyber infrastructure. This project will follow the guidelines prescribed in the National Institute of Standards and Technology (NIST) Special Publications 800-115. This process will identify possible vulnerabilities that may put the university at risk for a cyber-attack. Test implementation will be done in two ways using both hardware and software tools.

### MOTIVATION

In light of the news last year regarding system hacks and ransomware, cybersecurity has become an increasingly important consideration for organizations of every size. With a large number of staff, faculty, and students continuously going in and out of their physical facilities and digital systems, as well as accessing their systems both on and off-site, universities are more susceptible to attacks than the average organization.

### SCOPE REFERENCES

#### OUT OF SCOPE

- Administrative document review (3.1, 3.2, 3.3, 3.4, 3.6)
- Wireless (4.4)
- Social engineering (5.3)
- Planning, Policy, and legal (Section 6)
- Data Handling (7.4)

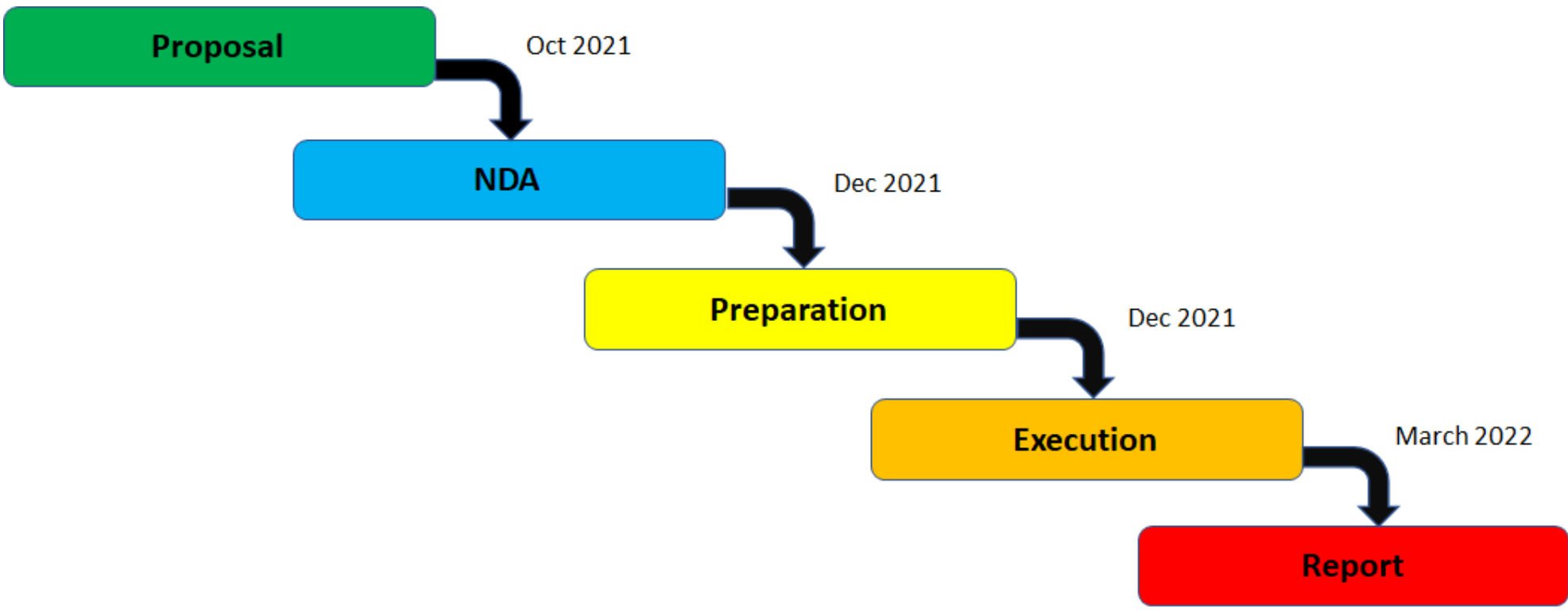
#### IN SCOPE

- Network sniffing (3.5)
- Target identification and analysis (4.1, 4.2, 4.3)
- Validate target vulnerability (5.1, 5.2)
- Security assessment (7.2, 7.3)

### MEMBERS

- Gary Choi (Senior Project):  
Project manager/Programmer
- Micah Au-Haupu (Senior Project):  
Graphic Designer/Programmer
- Kevin Salas (Senior Project):  
Administrator/Programmer
- Mitchell Wommack (Graduate Project):  
Administrator/Programmer

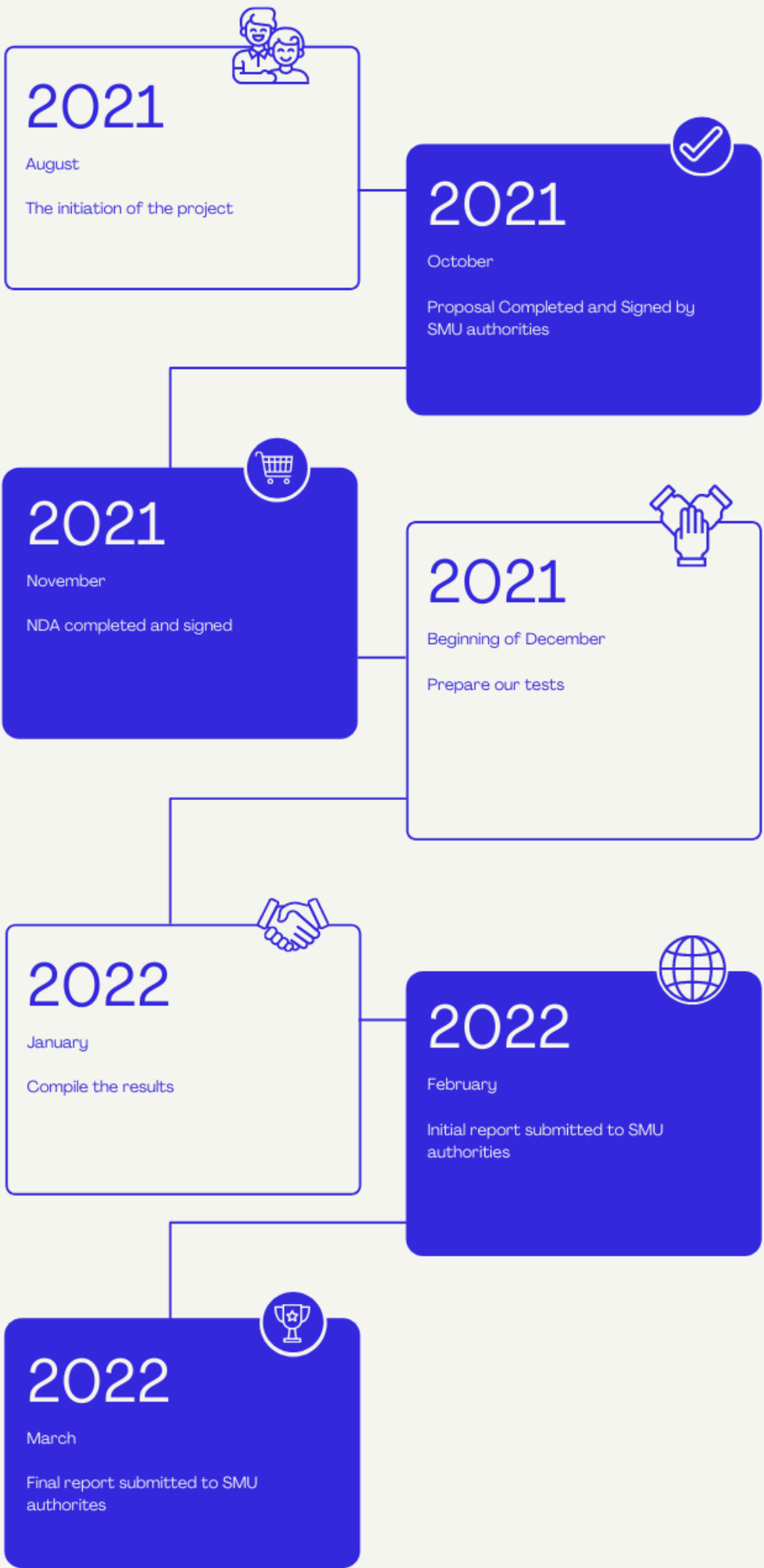
### WATERFALL MODEL



### TIMELINE

### SEVERITY RATING/ DESCRIPTION

#### Timeline of Project



#### Low

- Require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.
- Flaws that are present in a program's source code, but which no current or theoretically possible, but unproven, exploitation vectors exist or were found during the technical analysis of the flaw.

#### Important

- Flaws that can easily compromise the confidentiality, integrity, or availability of resources.
- Allow local or authenticated users to gain additional privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication or other controls, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.

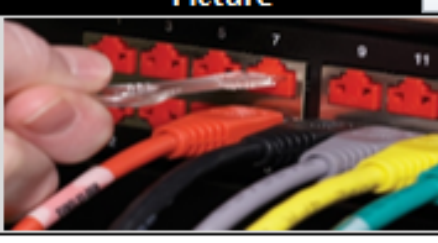



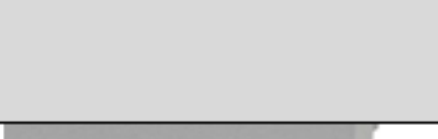

#### Moderate

- Flaws that may be more difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources under certain circumstances.
- Could have had a Critical or Important impact but are less easily exploited based on a technical evaluation of the flaw, and/or affect unlikely configurations.

#### Critical

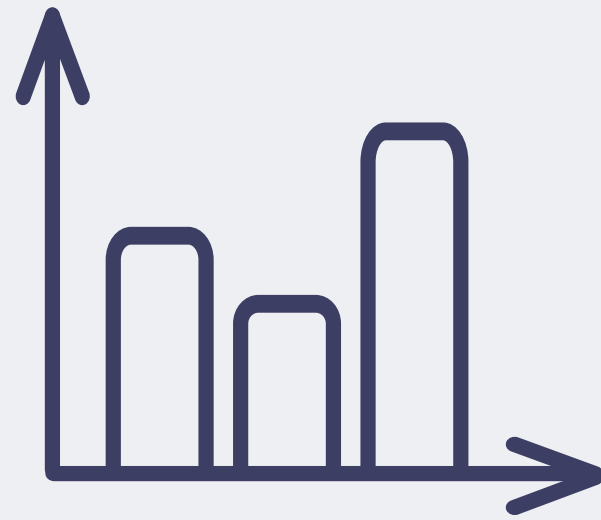
- Flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction.
- Flaws that require authentication, local or physical access to a system, or an unlikely configuration are not classified as Critical impact.

### SYSTEM IMPACTS AND MITIGATIONS

Device	Vulnerabilities	Potential Threat	Level	Suggested Remediation	Picture
Shark Jack	Network Attack Tool used for reconnaissance, data exfiltration, and attack	DHCP Exhaustion Attack, Compromising Other Clients within the Network,	Critical	1. MAC base port security 2. Block communication at ACL between clients in Guest vlan 3. Disable Hard-coding port. (Port accessible to Printer Network in Cebula) 4. RJ45 Port Locks ( <a href="https://www.black-box.de/en-de/fi/1245/13112/LockPORT-Secure-RJ45-Port-Locks/">https://www.black-box.de/en-de/fi/1245/13112/LockPORT-Secure-RJ45-Port-Locks/</a> )	
Bash Bunny	Executes payload	Local Privilege Escalation (LPE), Macro Attack, Payloads	Important	1. Disable Autorun 2. Disable auto driver installation (to prevent LPE Vulnerability). located in System Properties -> Device Installation Settings -> No.	
Key Logger	Captures user key strokes	Credential Compromise, espionage,	Important	CPU Locker ( <a href="https://www.globalindustrial.com/p/datum-small-hanging-cpu-locker-black?infoParam.campaignId=T9F">https://www.globalindustrial.com/p/datum-small-hanging-cpu-locker-black?infoParam.campaignId=T9F</a> )	
Packet Squirrel	Tool to monitor and compromise header of the packet that is being sent between users and server.	ARP Table Poisoning, DHCP Exhaustion Attack, Packet Spoofing	Important	1. RJ45 Plug lock ( <a href="https://www.neobits.com/panduit_psl_dcplrx_bu_recessed_rj45_plug_lock_in_p5772170.html?atc=gb5">https://www.neobits.com/panduit_psl_dcplrx_bu_recessed_rj45_plug_lock_in_p5772170.html?atc=gb5</a> ) 2. Lock box	
PassFab	Software to reset or create new user/admin account and password	Compromising Local Windows system Files and running script on startup with Event Handler	Moderate	Enable BIOS Password	
HDMI Logger	Screen Captures the users' screen	Screen captures and records sensitive information as displayed on the users' screen. This is often placed in conference rooms and used for corporate espionage.	Low	HDMI Cable Lock ( <a href="https://www.technologygalaxy.com/Tripp-Lite-P568-000-LOCK/p/353375?gclid=CjwKCAIAIRSPBhBaEiwAuLSDUa0HTrVotbpiy6JXlzsCsI45gQyeVj93CrLilzikaikvVOA_p5SRVlBoCyLIQAvD_BwE">https://www.technologygalaxy.com/Tripp-Lite-P568-000-LOCK/p/353375?gclid=CjwKCAIAIRSPBhBaEiwAuLSDUa0HTrVotbpiy6JXlzsCsI45gQyeVj93CrLilzikaikvVOA_p5SRVlBoCyLIQAvD_BwE</a> )	

### THE BENEFITS

This project has the potential to benefit the school both academically and financially.



Academically, it will not only showcase the school's resolve to use its facilities as teaching tools (as with Cebula Hall), but if the project is published, it will positively affect the reputation of the school's growing computer science program.

Financially, this project will save the school thousands of dollars it would otherwise have to spend for such tests to be performed. It also has the potential of lowering the school's insurance, particularly in the case of cybersecurity insurance.