**Penetration Testing Assignment 01**

**Threat Model**

**Student ID - 23077080**

**Table of Contents:**

1. **Introduction ------------------------------------------------------------------------------------------------------------ *03***
2. **Company Overview --------------------------------------------------------------------------------------------------- *03*** 
   1. Assumption & Threat Profile -------------------------------------------------------------------------------------------- *03*
   2. Infrastructure -------------------------------------------------------------------------------------------------------------- *04*
3. **Attack Tree**
   1. Software Attack ------------------------------------------------------------------------------------------------------------ *05*
   2. Single Sign-on Attack ----------------------------------------------------------------------------------------------------- *05*
   3. Ransomware-as-a-Service ---------------------------------------------------------------------------------------------- *06*
   4. Keylogger -------------------------------------------------------------------------------------------------------------------- *06*
   5. SYN Flood Attack ---------------------------------------------------------------------------------------------------------- *06*
   6. Smurf Attack --------------------------------------------------------------------------------------------------------------- *06*
4. **Security Recommendations**
   1. Software Attack ------------------------------------------------------------------------------------------------------------ *07*
   2. Single Sign-on Attack ----------------------------------------------------------------------------------------------------- *07*
   3. Ransomware-as-a-Service ---------------------------------------------------------------------------------------------- *07*
   4. Keylogger -------------------------------------------------------------------------------------------------------------------- *07*
   5. SYN Flood Attack ---------------------------------------------------------------------------------------------------------- *07*
   6. Smurf Attack --------------------------------------------------------------------------------------------------------------- *07*
5. **References -------------------------------------------------------------------------------------------------------------- *08***
6. **Introduction**

This report briefs about the attack tree based on the current threat landscape on Glenden Hospital and the methods which can be adopted by an attacker to attack. The report also highlights the consequence on Glenden hospital based each attack node in the attack tree and the mitigations for it.

1. **Company Overview**

Glenden Hospital offers variety of services, including advanced cardiac imaging, pacemaker device implantation and heart surgery.

* 1. **Assumption & Threat Profile**
* The below diagram depicts data flow in Glenden Infrastructure. The hospital architecture consist of FortiExtender Gateway router which manages the packet flow of internal & external environments.
* FortiGate firewall inspects network packets from the router & allows or blocks the traffic on the basis of custom created rules or illegitimate connection.
* After the filtration of network packets, internal FortiGate router routes the packets to the inhouse PM Webserver or Glenden Application Webserver.
* PMA Webserver displays dashboard of respective historical and current health records.
* Management Server & Glenden Application Server is connected to Microsoft SQL Server where the health records & heartbeats data are stored in separate tables namely Health record table & Heartbeat table.
* Management Servers commands actuator in pacemaker to stabilize heartrate. ECG sensor in pacemaker is used to provide live heartbeat data to management server.
* Glenden Application Website provides services to patients like booking appointments, viewing prescriptions, lab reports and ordering medicines.
* Okta Verify is used for single sign-on to the pacemaker dashboard & the admin panel of the Glenden Application Webserver.
* Apache log4j is running on 2.14.1 version.
* The infrastructure consists of DNS server for IP hosting.
  1. **Infrastructure**

Firewall

Public Facing Server

Internal Network Segment

Hospital Staffs

Pacemaker

SQL

Pacemaker Management Application WebServer

ClearHealth Webserver

Okta Identity Access Management

**Figure 01 : Architecture**

1. **Attack Tree**

Breaching CIA

Smurf Attack

SYN-Flood Attack

Keylogger

Software Attack

Ransomware-as-a-service

Malware Attack

Supply Chain Attack

DOS Attack

Single sign-on (SSO) attack

**Fig 02: Attack Tree**

**Root Node**: The diagram depicts the attacks, tactics and techniques that can be used to compromise CIA of Glenden network (*What are Backdoor Attacks? Types & Examples*, 2024).

* 1. **Software Attack**
  + Glenden WebApp is python based application wherein the developer requires python based plotly package to create interactive charts and graphs.
  + Attacker publishes malicious code package named pIOtly containing DarkGate malware in the GitHub repository.
  + Developer accesses DarkGate Malware malicious code, which will leads to credential theft & privilege escalation.
  + This leads to **data breaches**, violating patient privacy & regulatory compliance (e.g., HIPAA, GDPR) (Titterington, 2025).
  1. **Single Sign-on Attack**
  + The attacker posing as a ClearHealth staff sends phishing email to admin team with **Rootkit & keylogger** hybrid code attachment.
  + Once executed itcreates a backdoor & captures admin login credentials. Attacker uses stolen credentials to login to ClearHealth with non-standard user agent (e.g. - “PythonRequests/2.31.0z”) which OKTA classifies unknown.
  + Hence, the attacker will exploit Okta’s single sign-on policy to bypass vulnerabilities allowing attacker to skip MFA and access PMA (Okta, 2025).
  + The attacker gains access to patients sensitive data and health records, leading to a potential **data breach** & violations of regulations (like HIPAA & GDPR) (Okta,2024).
  1. **Ransomware-as-a-Service**
  + The attacker will exploit Apache's Log4Shell vulnerability to open backdoor for remote code execution and deploys TightVNC for persistence.
  + Attacker uses Mimikatz tool to perform pass-the-hash or ticket based attacks.
  + Attacker then uses Advanced Port Scanner software to scan live hosts in network to identify potential victims.
  + After opening backdoor in multiple servers, attacker deploys LockBit ransomware encrypting files and demand ransom for decryption (*Anatomy of a LockBit Ransomware Attack*, 2023).
  1. **Keylogger**
  + Attacker sends a phishing email containing excel file with malicious JavaScript and VBScript that exploits the [CVE-2017-0199](https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0199).
  + The script executes PowerShell command to download and run the snake keylogger payload (sahost.exe).
  + The downloaded .exe file decrypts & extracts additional modules (FGMaker.dll, Tyrone.dll) to deploy core malware.
  + The Tyrone.dll ensures persistence by running “schetasks.exe” command creating new scheduled task and uses process hollowing to inject malicious code into legitimate process.
  + Snake Keylogger traverses all profile files, extracting saved credentials & sending to attacker over SMTP.
  + Attacker can manipulate actuator commands, potentially endangering lives of patients by destabilizing heart-rates (Zhang, 2024).
  1. **SYN Flood Attack**
  + The staff accesses a website to download .pdf file, wherein attacker hides .exe file, which when executed opens a backdoor into target computer.
  + The malicious code searches for SAM file in computer that stores hashed user credentials & takes it offline to decrypt the file (João Carrasqueira, 2021).
  + Using RSA, attacker decrypts the username-password successfully retrieving the admin username-password & uses it to run PowerShell command to execute a scheduled script used to continuously send SYN packets causing a SYN flood attack due to which  PMA Webserver is overwhelmed, disrupting real-time monitoring of pacemakers leading to delay in stabilizing patient’s heart rate (*SYN flood DDoS attack*, 2024).
  1. **Smurf Attack**
  + Attacker uses Google Ads to push MadMxShell backdoor malware, advertising medicine blog websites, tricking hospital staff into clicking the Ad (Tay and Singh, 2024).
  + After successfully creating backdoor, attacker performs ipconfig & nslookup to get the broadcast address & IP of the targeted Pacemaker Management Application WebServer.
  + Attacker installs MiniSMB (TCP/IP packet crafting & traffic generator tool) (*minismb*, 2025).
  + Attacker spoofs the packet’s source IP address with PMA WebServer IP address using MiniSMB (Buxton, 2025).
  + Attacker will then execute ping command using *ping -t* [IP Address of PMA WebServer] to broadcast address.
  + The ICMP response from all the devices in the network will be directed to PMA WebServer (*What Is a Smurf Attack and How to Prevent It*, 2021).
  + This will overwhelm webserver & block genuine traffic delaying monitoring of patients’ heart rhythms & missing critical notifications in real time.

1. **Security Recommendations**
   1. **Software Attack**
      * Deploy antivirus to detect & block known signatures of malware.
      * Test third-party packages in UAT environment before deploying in production.
      * Mandate developers to use a software-bill-of-materials (SBOM) to track dependencies.
      * Keeping track of third-party product’s vulnerabilities and apply patches.
   2. **Single Sign-on Attack**
      * Implement SIEM and configure policies such as if user authenticates application with unknown user agent followed by successful authentication, the alert will be triggered.
      * Implement User behavior analytics to track deviation in geolocations, IPs or time-of-access (Okta, 2024).
      * Implement WebApp Firewall to block unknown user agent strings.
      * Enable .htaccess in apache webserver & add unknown User agents in .htaccess file to block the same (Mattias Geniar, 2015).
   3. **Ransomware-as-a-Service**
      * Managing Local admin accounts by Implementing Microsoft LAPS.
      * Upgrading the Apache's Log4Shell to 2.24.3 version to eradicate log4j vulnerability.
      * Implement EDR to detect & block known signature of RaaS.
      * Block port 5900 in firewall for inbound communication for remote desktop connections (Konstantin Kaplinskiy, 2023).
   4. **Keylogger**
      * FortiGuard’s AntiSPAM, Web Filtering, IPS, and AntiVirus services can be implemented which will detect & restrict Snake Keylogger [8].
      * IT department should restrict the access to PowerShell for local users.
      * Use a Password manager to store passwords for all accounts to avoid repetitive typing of credentials for access & hence mitigating keylogger (Lenaerts-Bergmans, 2024).
      * Software like Keylogger detector can detect unusual typing & character display hence identifying keylogging activity.
   5. **SYN Flood Attack**
      * Deploy Loadbalancer to distribute traffic on detection of DoS.
      * Increasing Backlog will allow server to handle high number of Syn requests.
      * Implement Packet capture tools to identify traffic-flow based attacks like DoS.
      * Implement Syn Cookies which will handle the Syn requests without utilizing the server's resources until handshake completion (Chinnasamy, 2021).
   6. **Smurf Attack**
      * Disable broadcast request in router to prevent network devices from responding to broadcasted ICMP request (*Indusface*, 2024).
      * Configure rate limitation of ICMP packets in router to prevent network being overwhelmed with ICMP traffic (*Indusface*, 2024).
      * Disable ping requests in webserver by editing the /etc/sysctl.conf file (*How to Block Ping (ICMP) Responses in Linux?*, 2024).
      * Allow only admin users to install third-party software’s.
2. **References**
   * Titterington, A., (2025) *Supply-chain attacks in 2024*, *Kaspersky.com*. Kaspersky. Available at: <https://www.kaspersky.com/blog/supply-chain-attacks-in-2024/52965/>. (Accessed: 20 February, 2025)
   * *What are Backdoor Attacks? Types & Examples,* (2024), *SentinelOne*. Available at: <https://www.sentinelone.com/cybersecurity-101/threat-intelligence/backdoor-attacks/>. (Accessed: 20 February 2025)
   * Okta, (2024) *Okta.com*. Available at: <https://trust.okta.com/security-advisories/> (Accessed: 21 February 2025).
   * Okta Trust, (2024) ‘Okta Classic Application Sign-On Policy Bypass - Oct 4, 2024’, *Okta Blog,* 24 October. Available at: <https://trust.okta.com/security-advisories/okta-classic-application-sign-on-policy-bypass-2024> (Accessed: 23 February 2025).

* Mattias Geniar, (2015) *Block User-Agent in htaccess for Apache Webserver*, *Ttias.be*. Available at: <https://ma.ttias.be/block-user-agent-in-htaccess-for-apache-webserver/> (Accessed: 23 February 2025).
* *Anatomy of a LockBit Ransomware Attack*, (2023) *www.varonis.com*, 16 June. Available at: <https://www.varonis.com/blog/anatomy-of-a-ransomware-attack>. (Accessed: 24 February 2025)
* Zhang, X., (2024) *Deep Analysis of Snake Keylogger’s New Variant | FortiGuard Labs*, *Fortinet Blog*. Available at: <https://www.fortinet.com/blog/threat-research/deep-analysis-of-snake-keylogger-new-variant>. (Accessed: 26 February 2025)
* João Carrasqueira, (2021) *Windows 10 vulnerability lets anyone get administrator privileges*, *XDA*. Available at: <https://www.xda-developers.com/windows-10-vulnerability-lets-anyone-get-administrator-privileges/> (Accessed: 26 February 2025).
* SYN flood DDoS attack, (2024), *Cloudflare.com*. Available at: <https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack>. (Accessed: 27 February 2025)
* Konstantin Kaplinskiy, (2023) *TightVNC Frequently Asked Questions*, *Tightvnc.com*. Available at: <https://www.tightvnc.com/faq.php#portfwd> (Accessed: 01 March 2025).
* Chinnasamy, V., (2021) *What is SYN Attack and How to Prevent the Attack? Indusface Blog*, *Indusface*. Available at: <https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/>. (Accessed: 01 March 2025)
* Lenaerts-Bergmans, B., (2023) ‘Keyloggers: How They Work and How to Detect Them’, *CrowdStrike Blog,* 2 February. Available at: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/keylogger/> (Accessed: 02 March 2025)
* Tay, R. and Singh, S., (2024) *Malvertising campaign targeting IT teams with MadMxShell*, *www.zscaler.com*. Available at: <https://www.zscaler.com/blogs/security-research/malvertising-campaign-targeting-it-teams-madmxshell> (Accessed: 02 March).
* *Minismb,* (2025) *GitHub*. Available at: <https://github.com/minismb/minismb>. (Accessed: 03 March 2025).
* Buxton, O., (2025) *IP spoofing: What is it and how does it work?*, *@Norton*. Norton. Available at: <https://us.norton.com/blog/malware/what-is-ip-spoofing>. (Accessed: 04 March 2025).
* *What Is a Smurf Attack and How to Prevent It,* (2021) *Heimdal Security Blog*. Available at: <https://heimdalsecurity.com/blog/smurf-attack-ddos/>. (Accessed: 05 March 2025)
* *Indusface,* (2024) *Indusface*. Available at: <https://www.indusface.com/learning/what-is-a-smurf-attack/>. (Accessed: 6 March 2025)
* *How to Block Ping (ICMP) Responses in Linux?,* (2024) *GeeksforGeeks*. Available at: <https://www.geeksforgeeks.org/how-to-block-ping-icmp-responses-in-linux/>. (Accessed: 7 March 2025)