Financial Services Industry Threat Landscape

According to a recent report by Accenture the current threat landscape for the financial services industry consists of the following main and emerging threats.

- Interconnected attack surface due to introduction of financial services supply chain
- Credential and identity theft
- Data theft and data manipulation
- Emerging technologies, i.e., 5G, deep fakes, AI, crypto.

STRIDE threat model

STRIDE Threat categories	Testing Tools / Method
Spoofing of Identity	
Financial services industry uses PKI (Public Key Infrastructure) for establishing identity, trust, and confidentiality (encryption) e.g., CA, certificate signing, revocation, validation etc.	*Nessus vulnerability assessment tool*
Non multifactor secured financial online web applications can be using insecure authentication mechanisms, weak password security, lack of authentication session state security e.g., timeouts.	*Kali Linux brute force password attack*
Network connection security e.g., ARP spoofing, IP route redirection, domain spoofing.	w*hois, nslookup*
Tampering with Data	
Financial web applications are vulnerable to both data in transit as well as data in motion threats, for e.g., malware injection and tampering user request data or server reply data can potentially have negative impact.	*Nessus vulnerability assessment tool*
Repudiation	
Inadequate log data resulting in malicious users denying carrying out illegal transactions. For e.g., financial payment card information compliance	Security audits to determine appropriate controls are in place for log generation and log archiving/retrieval.
Information Disclosure	
Effectiveness of confidentiality by encryption and obfuscation at a network level is provided by tools network security protocols such as SSL, HTTPS etc.	Kali Linux, Nmap tool
Social engineering such as user fishing, fake misleading site can result in financial fraud	Audits and checks performed to validate the effectiveness of privacy and security training programs.
Denial of service	

Overwhelm network infrastructure responsible for providing connectivity services to financial web applications by attacking the network control plane e.g., abnormal high traffic destined for network device IP addresses.	Nmap, HPING, TRACEROUTE
Overwhelm the compute infrastructure hosting the web application e.g., SYN, HTTP flood	HPING
Overwhelm application user and data handling capacity e.g., create large number of accounts, enter large data for processing	Kali Linux, whatweb, wget

Table 1. STRIDE threats and testing tools

Scanning and reconnaissance tools:

The table below outlines a brief description of some of the tools used and their application. Additional tools may be used during analysis at the pen-test team's discretion (Muniz and Lakhani, 2013, pp.34–72).

Tool Name	Description
Kali Linux	Linux distribution with suite of reconnaissance and pen test tools. Many of the tools used in our analysis is prebuilt into this operating system
HPing	A ping tool with greater control over packet generation and analysis. Ping requests can be tailored to suit several idle scanning tests
Traceroute	Show's packet travel path from source to destination. Valuable firewall information can be gleaned from hop latency as well as timeouts/failures in transit
Nmap	A broad and highly tailorable tool used in scanning networks. Our team primarily uses this tool to scan for open ports as well as active open ports.
Nikto	Nikto is a web server and web app vulnerability scanning tool effective at finding web server information as well as actionable vulnerabilities on the server. The drawback to Nikto is that it is loud and will appear in logs
SSLScan	SSLScan is a powerful scan in querying and analyzing secure socket layer (SSL) and transport layer security (TLS) protocols. Even a failure with this tool is valuable as it tells the test team whether incoming and outgoing traffic from the site is secure.
Whois	Queries domain name systems (DNS) for information regarding domain and domain registration information. Valuable site and locational information can be obtained using this tool
Nessus	A comprehensive vulnerability scanner used to identify a range of actionable attack surfaces including default password checks, DoS vulnerabilities and unauthorized access holes.

Business impacts on use of tools and methods

The task will be completed in four weeks as scheduled below:

	Timeline of the completion of the task.	
Planning	1 week	Gathering all resources to be used
Execution	2 weeks	Actual testing in all scope targets
Analysis and Documentation	1 week	Preparing a summary report of the findings

Following are the limitations and assumptions

	Limitation and assumptions
Limitation of scope	Testing a website is not done on the whole website but only selected parts
Limitation of access	Testers are not allowed to access the whole website when testing.
Penetration testers expertise	Testers are considered subject matter experts in more than one area but not all. It is assumed that tools used are current and have been prior tested to achieve desired results
Availability of tools	Many of the tools described throughout are freely available across many operating systems, this is reflective of current attacker profile

Following are the potential business impact of scanning web application environments

	Impacts on normal operations caused by network scanning tools
Passive network scanning	Network scans and assessments are pre-planned to minimize the operational impact. However, due to the nature of these assessments, whenever an assessor interacts with an IT system or network environment, there is a possibility of system overload or similar disruptive conditions. During initial planning, specifically related to tools, techniques and processes, organizations must define their tolerance levels for intrusiveness.
Active Network Discovery	Tools used for active network discovery can generate network noise which may result in network latency and packet drops. Additional network activities generated by active discovery queries could negatively impact the normal business traffic. Since active discovery reveals its origination point, it can also trigger IDS alerts (NIST, 2008).

REFERENCES:

A. Shebli and B. D. Beheshti, (2018) A study on penetration testing process and tools. *Proceedings of the IEEE Long Island Systems, Applications and Technology Conference (LISAT).* pp. 1-7, doi:10.1109/LISAT.2018.8378035.

NF Awang, A Abd Manaf (2012) Detecting vulnerabilities in web applications using automated blackbox and penetration testing *A study of penetration testing tools and approaches TP Chiem,* Available from http://openrepository.aut.ac.nz [Accessed 6th June 2021]

NIST. (2008) Technical Guide to Information Security Testing and Assessment. [Online] Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf [Accessed 7 June 2021].

Muniz, J. and Lakhani, A. (2013). *Web Penetration Testing with Kali Linux*. Livery St, Birmingham, UK: Packt Publishing Ltd, pp.34–72 [Accessed 10 June 2021].

Abend, V. (2019) Future cyber threats: Extreme but plausible threat scenarios in Financial Services. [Online] Available from https://www.accenture.com/us-en/blogs/cyber-defense/cyber-future-for-financial-services. [Accessed June 4 2021]