Temasek Defence Systems Institute

Detecting Malicious Traffic Concealed within Common Network Flows via Socket Layer Monitoring

Tan Shao Jie (ST Engineering)
Advisor: Dr Geoffrey G. Xie |Second Reader: Christopher S. Eagle

Background & Motivation

Keeping organizations' computer network safe from intrusion is one of the most vital parts of network security. The common practice is to use intrusion detection system (IDS) as the first line of defence, to get insights into potential malicious activities and prevent their network and/or systems from getting compromised. Most IDS struggle to classify anomalies against adversarial AI which use polymorphism to disguise specific exploits. We discuss the challenges of detecting intrusion and the feasibility of IDS, particularly host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS), to detect certain anomalies. In this thesis, we analyse if it is feasible to monitor and/or modify packet payload at socket layer masked under common network protocols to detect intrusion. It will also assess the feasibility of embedding additional bytes in packet payload at the socket layer for the purpose of differentiating legitimate and malicious traffic.

Research Ideas

- What are these common application layer protocols hijacked by cyberattacks?
- What are the advantages using the method of socket layer monitoring effective to detect anomalies? Can it improve the current HIDS?
- By embedding signature data to the data packet at the socket layer, can we differentiate legitimate and malicious traffic? Can it improve the current NIDS?

Scope

Kernel modification research via the socket layer is currently being performed by Daniel Lukaszewski in his dissertation study. Daniel Lukaszewski designs and develops the source code required to embed data into typical application payloads. Additions or modifications to this source code are minimal and only related to the data and application protocols being utilized for intrusion detection. The focus for this study will be on collecting relevant data and metrics to evaluate the feasibility and effectiveness of monitoring socket layer to detect intrusion masked under common protocols. The experimental network will feature a simple point-to-point topology and attempt to emulate a proprietary network with open-source security controls implemented specifically to detect anomalies and compare it with a list of attack signatures. This is to differentiate legitimate and malicious traffic. In addition, the investigation will focus on examining common application protocols and the feasibility of embedding data in their associated payloads before sending it out to the network. Specific attention will be paid to socket layer and the characteristics of application layer protocols are ideal for malicious attacks.

Methodology

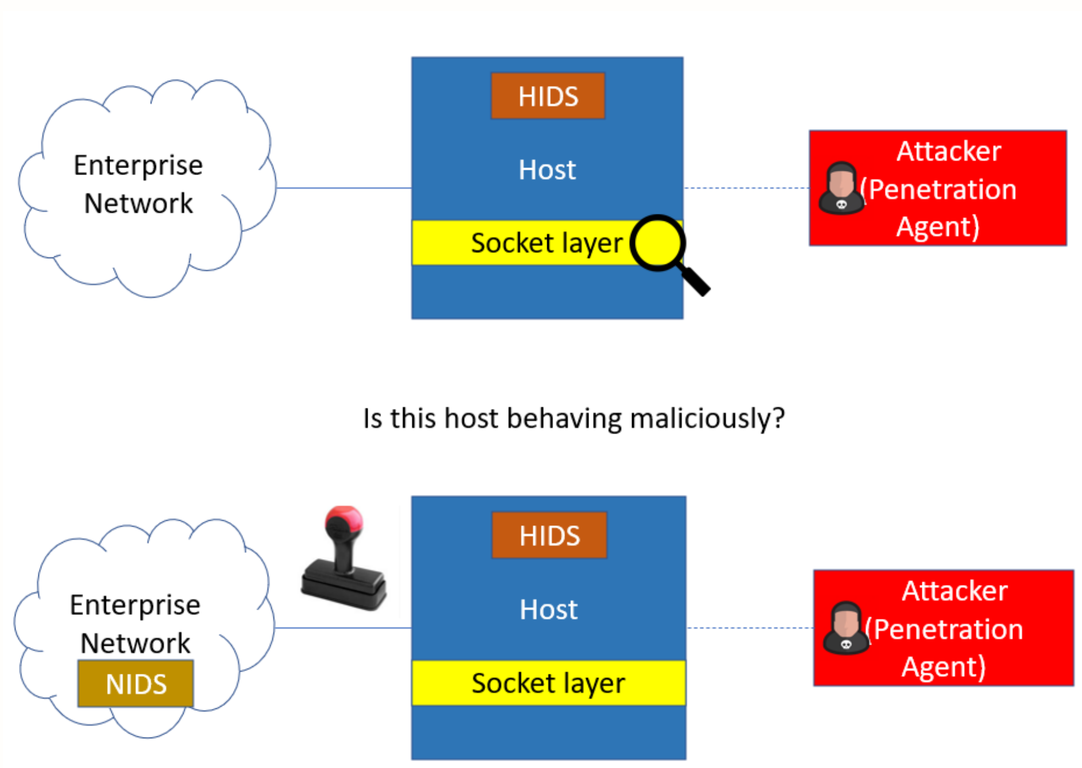

Figure 1(a), 1(b): Experimental Testbed, a virtual environment consisting of a legitimate client machine, a server and a penetration agent using a simple point-to-point topology.

Benefits of Research

- Examining packet payloads at the socket layer may provide another vantage point to detect anomalies on a monitored host.
- Presents a potential new method of detecting intrusion masked under common network protocols by utilizing socket layer monitoring.
- If this method is proven effective, the research in this thesis could illuminate potential new vulnerability exploits that organizations could use to design and implement more effective intrusion detection system

NUS National University of Singapore