Università di Modena e Reggio Emilia, Italy

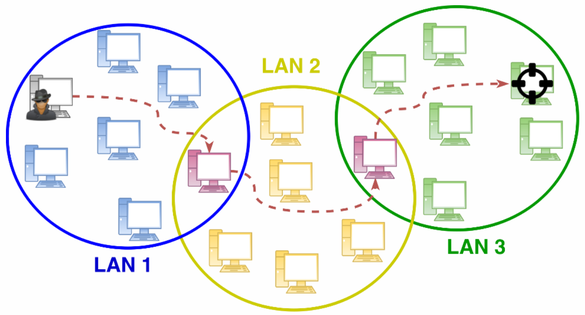
Detection and Threat Prioritization of Pivoting Attacks in Large Networks

Giovanni Apruzzese,
ICT Doctorate school, Cycle XXXII
Course in Computer Engineering and Science

Tutor: Prof. M. Colajanni

Scenario

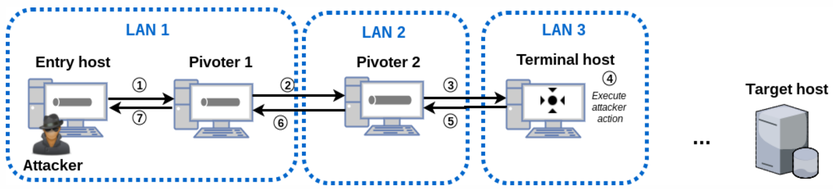
Defending large enterprise systems is an extremely challenging task. Attackers want to control hosts with higher privileges or more valuable data**.**



This goal is achieved by moving laterally in the targeted network, which can be performed by means of *pivoting*. This technique has been employed in many recent advanced cyber attacks, such as Archimedes (2017) or Medjack (2015).

Pivoting Description

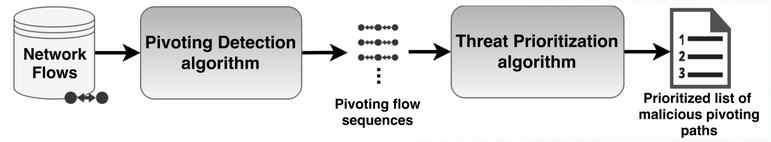
Pivoting: any action in which a *command propagation tunnel* is created among three or more hosts. This tunnel allows to propagate commands to remotely control the last host of the pivoting chain.



Pivoting activities are not necessarily malicious. Attackers rely on pivoting techniques after having already compromised an internal host.

Proposed Approach

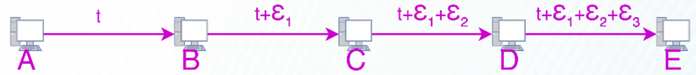
Our proposed approach analyzes the *network flows* generated between the *internal hosts* of a monitored network.
We devise a novel *pivoting detection algorithm* to identify flow sequences related to pivoting activities.
These flow sequences are then processed with an original *threat prioritization algorithm* to determine their maliciousness.



Pivoting Detection Algorithm

This algorithm searches for pivoting flow sequences, characterized by consecutive flows presenting the following characteristics:

- Adjacent
- Chronologically ordered
- Not cyclical
- Short propagation delay ($\varepsilon_i < \varepsilon_{max}$)



Each flow sequence must be composed of at least 2 flows, thus spanning over 3 different hosts.

Threat Prioritization Algorithm

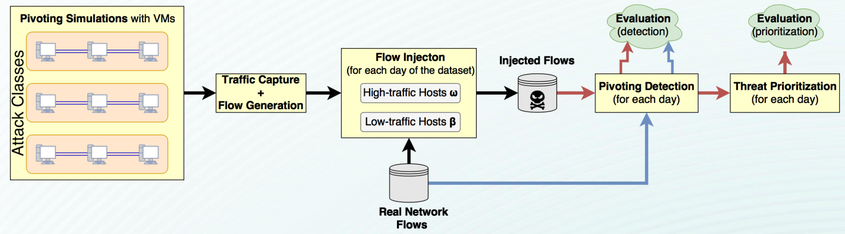
For each detected pivoting flow sequence we compute a risk score representing its maliciousness. This score takes into account the following aspects:

- Novelty
- Reconnaissance Activities
- Uncommon Ports
- LANs involved
- Anomalous Data Transfers

Effective triage of malicious pivoting activities is performed by *ranking* pivoting activities on the basis of their assigned risk score.

Experimental Evaluation

We evaluate the proposed approach with thorough experiments performed on a large enterprise network. We simulate different pivoting attack classes through ad-hoc VMs and inject the generated traffic into the organization real traffic data (spanning ~180 days and amounting to over $500M$ flows). Then we execute the Pivoting Detection and Threat Prioritization algorithms to assess their capability of detecting and correctly prioritizing the malicious pivoting activities.

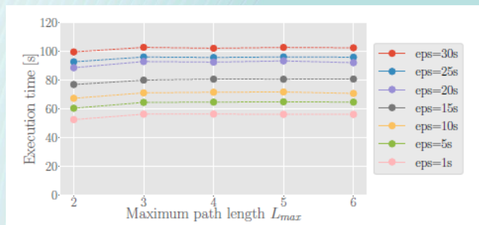


Results

The proposed approach is able to detect all the injected pivoting attacks, which are assigned a stable and high rank, thus showing the combined effectiveness of our algorithms.

Attack Class	average rank	standard deviation
AC1 (ω)	1.38	1.32
AC1 (β)	1.17	0.72
AC2 (ω)	2.01	1.18
AC2 (β)	1.55	1.04
AC3 (ω)	1.00	0.00
AC3 (β)	1.00	0.00
AC4 (ω)	1.13	0.51
AC4 (β)	1.14	0.68
AC5 (ω)	1.15	0.83
AC5 (β)	1.14	0.78

Timely detection of attacks is important, hence we also measured the execution time of the pivoting detection algorithm, which is capable to perform the analysis of 12 hours of traffic in less than 2 minutes.



(b) Analysis of 12 hours of data ($\sigma_{max} = 17.8$s).

Giovanni Apruzzese is with Dipartimento di Ingegneria "Enzo Ferrari", University of Modena and Reggio Emilia, Italy. **Email**: giovanni.apruzzese@unimore.it