Abstract

Traditional, perimeter-based protection systems frequently fall short in identifying and thwarting complex, multi-stage assaults that take advantage of weaknesses at several network layers in today's dynamic threat landscape. A innovative and organized three-tiered attack graph model is presented in this study to close this gap and enhance threat modeling, vulnerability assessment, and strategic defense planning. In contrast to traditional flat or binary attackgraphs, ourmodelbreaksdowntheattacksurfaceintothreesemanticallyseparatelayers: connectivity, remote vulnerabilities, and local vulnerabilities. This improves the clarity of adversarial paths and closely resembles the evolution of an actual attack.

At the top of the model is the connectivity layer, which depicts the direct network-level access between the attacker and the target hosts as well as the host-to-host links determined by the network architecture. It records the reachability and visibility based on variables like firewall rules, open ports, and routing setups. The second layer, known as the remote vulnerability layer, simulates all known vulnerabilities on each host, including web server issues, insecure services, and exposed APIs, that can be exploited without previous authentication or access. This layer determines the attacker's capacity to obtain first user-level access and incorporates intra-host relationships between remote vulnerabilities. However, lateral movement requires more than just acquiring such access.

The attacker must first establish a foothold through a remote exploit before the local vulnerability layer, located at the bottom of the model, is activated. It comprises vulnerabilities that need local access, like kernel exploits, privilege escalation flaws, or configuration errors, which allow the attacker to elevate from user-level rights to root or administrative privileges. The attacker can only proceed with the multi-stage attack chain by pivoting to compromise other systems after successfully exploiting these local vulnerabilities. In addition to better supporting automated examination of attack feasibility, this tiered structure imposes a genuine sequential dependency that mirrors true adversarial behavior.

Using a custom-designed enterprise networktopology with four interconnected hostsandknownCVEs retrieved from the NVD database and evaluated using CVSS v3.1 metrics, we validate this model. An external attacker may follow 26 full attack routes that our investigation uncovered, starting from early access and ending with total root-level penetration. Precise mapping of these chains is made possible by the attack graph, which also facilitates quantitative vulnerability evaluation according to severity, exploitability, and lateral movement potential.

Furthermore, the three-tier model's modular architecture enables it to expand to increasingly complex contexts, including Software-Defined Networks (SDNs), cloud infrastructures, and Internet of Things (IoT) ecosystems. It helps with risk propagation analysis, improves situational awareness, and provides information for proactive mitigation planning. In subsequent iterations, this architecture can be combined with automated attack simulation platforms, machine learning-based predictive analytics, and real-time threat intelligence feeds to create a powerful decision-support tool for network defenders and cybersecurity analysts.

Keywords: Attack Graph, SDN, Network Security, Vulnerabilities, Network Defense Techniques, Firewall, Network Topology, Three-Tier Attack Graph.