Reconnaissance Mitigation Through NGFW (Next Generation Firewall)

By: Denzel Martin & Favour Agho
Advisors: Jorge Crichigno & Ali Mazloum
University of South Carolina

Department of Integrated Information Technology
December 1, 2023

Agenda

- Reconnaissance
- Next Generation Firewalls (NGFW)
- Palo Alto Firewall Systems
- Demo
- Conclusion

Reconnaissance

Reconnaissance refers to the process of gathering information about a target network or system to identify vulnerabilities and potential points of entry.

Types of Reconnaissance Attacks:

- Passive Reconnaissance: Collecting information without directly interacting with the target.
- Active Reconnaissance: Involves engaging with the target system, like scanning for open ports and services.

Importance of Detection and Prevention:

- Early detection of reconnaissance activities is crucial to thwart potential cyber threats.
- A robust security strategy should include measures to prevent and mitigate reconnaissance attempts.

NGFW (Next Generation Firewall)

Definition and Characteristics:

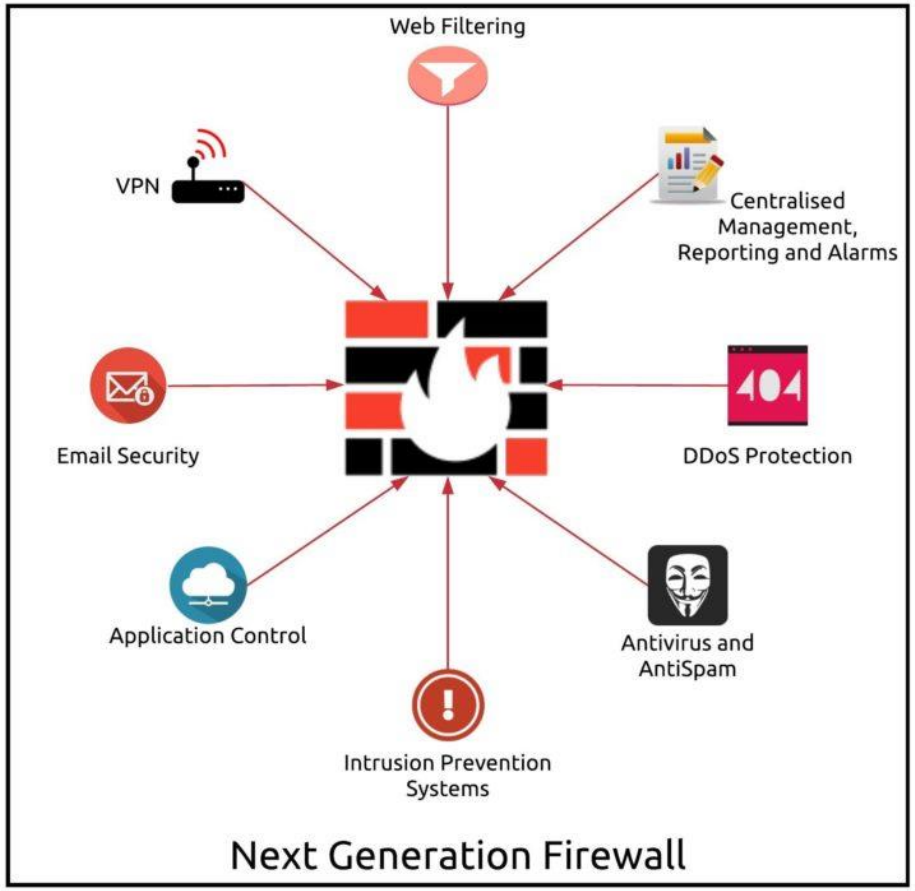
- NGFWs combine traditional firewall capabilities with advanced security technologies.
- They offer deep inspection of network traffic, allowing granular control over applications and user activities.

Capabilities Beyond Traditional Firewalls:

- Intrusion Prevention System (IPS) capabilities for real-time threat prevention.
- Application-layer filtering to control and monitor application usage.
- SSL and TLS inspection to detect threats hidden within encrypted traffic.

Integration of Advanced Security Features:

- NGFWs often include features like antivirus, sandboxing, and threat intelligence integration.
- These advanced features enhance the firewall's ability to identify and block sophisticated threats.



Palo Alto Firewall Systems

Overview of Palo Alto Networks:

- Palo Alto Networks is a leading cybersecurity company known for its cutting-edge firewall technologies.
- The company's commitment to innovation is reflected in its comprehensive security platforms.

Unique Features and Capabilities:

- Their approach emphasizes the importance of a prevention-first mindset, disrupting threats before they can cause harm.

Role in Protecting Against Reconnaissance:

- Palo Alto Firewalls play a vital role in detecting and preventing reconnaissance activities.
- The integration of threat intelligence and continuous updates ensures Palo Alto's systems stay ahead of emerging threats.

Demo

1) Practical Demonstration of NGFW in Action
2) Showcase of Reconnaissance Prevention

Conclusion

- Reconnaissance is the first phase of cyber attacks
- NGFW provides the means to detect and mitigate Reconnaissance
- This project utilized Palo Alto NGFW to detect and mitigate Reconnaissance