Ochrona danych i systemów
Milestone 1

Temat 1: Aktywny Firewall

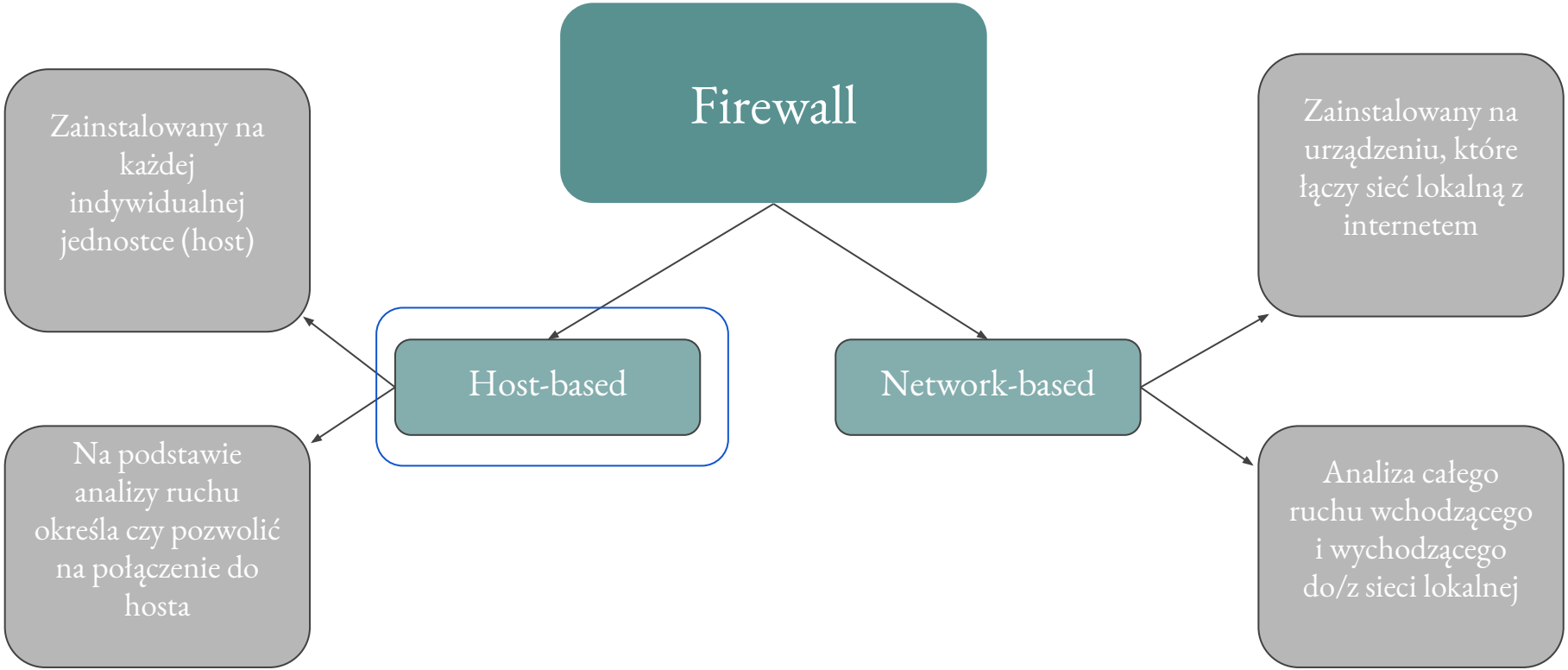
Skład zespołu:

- Alicja Uzar
- Daniel Mynarski
- Dominik Wróbel

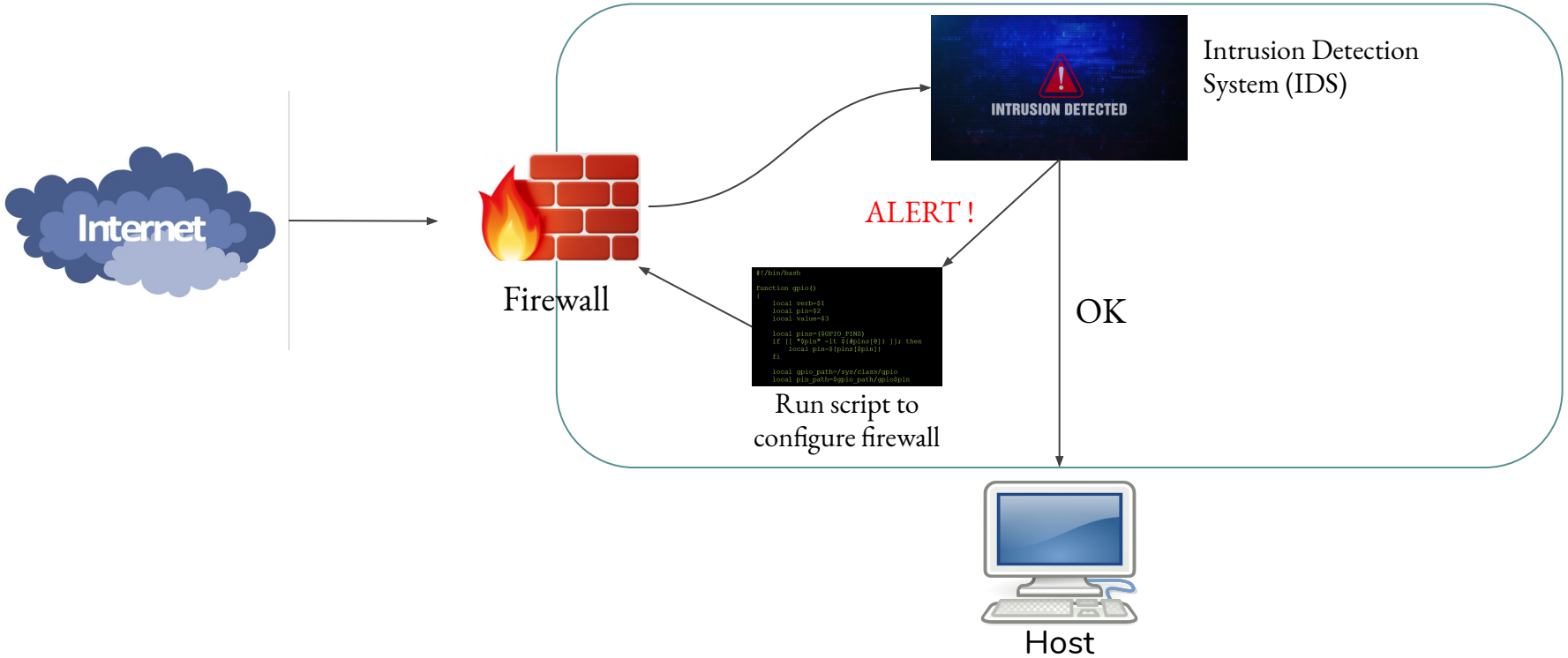
Literatura

1. *Testy penetracyjne w badaniu skuteczności IDS dla środowiska Unix/Linux*, Biuletyn instytutu automatyki i robotyki nr 21, 2004, Adam Klepka, Zbigniew Suski
2. *A Linux-based IDPS using Snort*, Muhammad Shamraiz Bashir
3. *Intrusion detection with snort*, Rafeeq Ur Rehman
4. *How to cheat at securing Linux*, James Stranger
5. *Best Damn Firewall Book Period*, Thomas W. Shnider
6. *IDS Intrusion Detection System*, Part I, Linux Focus 05/2003, Müller K.

Firewalls - podstawowy podział

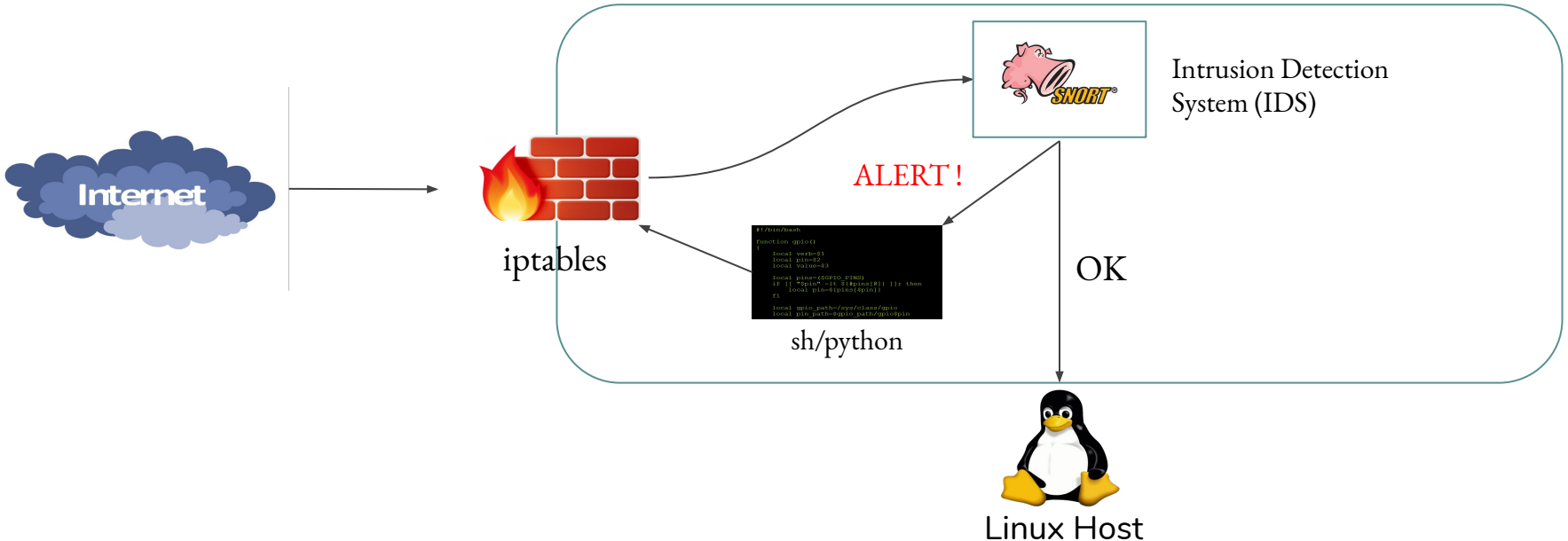


Architektura dla firewalla typu Host-based



Technologie i narzędzia

System operacyjny	IDS	Skrypty	Inne
Linux	Snort	Bash / Python	iptables



Plan testów

Testy przeprowadzone będą wykonując atak na host na którym działa nasz system *Aktywny Firewall,* a oczekiwanym rezultatem będzie blokowanie czasowo dostępu dla adresów prowadzących takie ataki.

W ramach testów przeprowadzimy ataki :

- Port Scanning
- Ping flood
- Land attack
- UDP Flood
- SYN Flood

Harmonogram

- 14.04.2020 - zapoznanie i instalacja narzędzi Snort, iptables, przypomnienie pisania skryptów w środowisku Linux
- 18.04.2020 - próbne generowanie alertów i reakcje na nie z poziomu skryptów sh poprzez konfiguracje iptables
- 22.04.2020 - przeprowadzenie przykładowego ataku i reakcja na atak
- 05.05.2020 - zdefiniowanie większej liczby ataków do testów
- 20.05.2020 - przeprowadzenie testów dla pozostałych ataków
- 25.05.2020 - opracowanie prezentacji i dokumentacji projektu

Dziękujemy za uwagę