Poniższa tabela przedstawia przykładowe rodzaje zag, które net.soc jest w stanie wykryć. Nasz sposób postępowania z atakami jest zgodny z frameworkiem MITRE ATT&CK (https://attack.mitre.org/), który szczegółowo opisuje techniki wykorzystywane do zainfekowania systemów. Doktryna ta jest znana na całym świecie wśród bezpieczników i my również stosujemy ten sprawdzony w boju model.

Rekonesans, skanowanie, footprinting	Enumeration, social engineering, system hacking	System hacking	Zagrożenia malware	Ataki na warstwę L2	Web & database attacks	Eskalacja uprawnień	System design
Skanowanie portów **Skanowanie podatności** **Użycie NMAP** **Skanowanie podsieci**	NetBIOS/LDAP enumeration SNMP enumeration Użycie keyloggerów software'owych Phishing	Komunikacja w Internecie z hostami/krajami blacklisted Użycie narzędzi hakerskich (np. Kali Linux) Użycie USB Buffer overflow Logowania w nietypowych godzinach Brute-force Ataki na DNS Wykorzystywanie podatności	Wirusy Robaki Ransomware Rootkity Trojany Backdoory Spyware Adware **Dzięki integracji z AV**	Ataki na serwer DHCP MAC flooding ARP poisoning	SQL injection XSS Command injection XML injection Password cracking Clear-text passwords	Utworzenie nowego konta administratora Użycie konta administratora w nietypowych godzinach	Wykrywanie podatności Dane przesyłane w formie clear-textu (hasła, wrażliwe dane osobowe)