Whois – protokół TCP, wysyłanie zapytań do baz danych DNS w celu rozpoznania właściciela domeny, uruchamiany przez wiersz poleceń lub przez skrypt WWW, 2 metody gromadzenia danych: gruby – jeden serwer do wszystkich domen, chudy – jeden serwer do serwerów firm rejestrujących domeny

Traceroute – program do badania trasy pakietów w sieciach IP, oparty na UDP oraz ICMP, najpierw wysyłamy pakiet z polem TTL=1, każdy router zmniejsza wartość o 1. Kiedy osiągnie 0 dzięki ICMP dowiadujemy się o adresie IP pierwszego routera, TTL=2 itd., aż host docelowy zwróci komunikat port nieosiągalny (bo wysyłane są pakiety UDP z wysokim nr portu) lub zwróci odpowiedz Reply na komunikat ICMP (win)

TCP/IP – protokół sieciowy, najpopularniejszy, serwery i usługi sieciowe określone dwoma parametrami: adres sieciowy i nr portu (65536), nr zarejestrowane w IANA, 3 stany portów: otwarty – jest nasłuchiwanie, zamknięty – połączenia są zabronione, zablokowany – brak odpowiedzi od serwera, porty otwarte to zagrożenie dla programu odpowiedzialnego za usługi oraz systemu serwera, zamknięty to tylko dla systemu serwera, zablokowany bezpieczny, wysyłanie danych na otwarty port w celu przepełnienia buforu

Skanowanie SYN (-sS): wysyłanie surowych pakietów IP i monitorowanie odpowiedzi, bez pełnego połączenia TCP, atakujący wysyła pakiety SYN, otwarty port odpowiada SYN-ACK, atakujący zamyka RST

Skanowanie TCP (-sT): za pomocą funkcji sieciowych OS, za pomocą metody connect(), następuje przywitanie lub odrzucenie wraz z kodem błędu.

Skanowanie UDP (-sU): brak odpowiedzi gdy port jest otwarty, odpowiedz nieosiągalny port ICMP gdy w 2 przypadku, a i to można zablokować dzięki zaporze

Skanowanie ACK (-sA): stwierdza czy port jest filtrowany (brak odpowiedzi) czy nie (RST), do wykrycia zapory sieciowej

Skanowanie FIN (-sF): pakiety omijają zapory, zamknięte porty odpowiadają pakietem RST, otwarte je ignorują, Windows wysyła RST zawsze

Skanowanie ICMP (-sP): sprawdza czy serwer odpowiada np. na pingi

DDoS – atak na serwer lub usługę w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów najczęściej przez komputery zombie.

SYN Flood - Serwer odpowiada na pakiety SYN atakującego ale nie otrzymuje od niego pakietów ACK. Powoduje to, że zwykły użytkownik nie otrzymuje odpowiedzi na swoje żądanie, wykorzystywany protokół TCP, wysyłanie dużo pakietów SYN z fałszowanym adresem IP, serwer odpowiada a komputer SYN-ACK, a atakujący nie odpowiada, obciąża łącze, zapełnia tablice stanów połączeń co zablokuje następne przychodzące połączenia, zabezpieczenie firewall limitujący ilość pakietów SYN

UDP Flood – wysłanie dużej ilości pakietów UDP na różne porty hosta, na które ten będzie musiał odpowiedzieć pakietami ICMP

IPsec – to zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy nimi, wykorzystywany w VPN, składa się z 2 kanałów komunikacyjnych: dla kluczy (UDP), dla danych (ESP), pakiety IP są szyfrowane, otrzymują nowy nagłówek, do dystrybucji klucza używamy protokołu IKE (sprawdzenie: hasło po obu stronach, RSA, X.509, umożliwia zmianę klucza co jakiś czas, klucze uzgadniane automatycznie), podsłuchujący dostaje tylko SPI i nr sekwencyjny, IPsec cechuje jednokierunkowość

Tryb transportowy: niewidoczne są dane użytkownika, ale nagłówek IP pozostaje widoczny, IP,ESP,[TCP],[dane]

Tryb tunelowy: IPn, ESP, [IP],[TCP],[dane], umożliwia VPN, niewielki narzut wielkości pakietu

Nmap to skaner aktywny, wykrywalny