Odmowa usługi (DoS)

Cele kształcenia
Ataki Denial of Service (DoS) i Distributed Denial of Service (DDoS) stanowią poważne zagrożenie dla sieci komputerowych. Ataki te mają na celu uniemożliwienie dostępu do komputera lub zasobu sieciowego autoryzowanym użytkownikom. Zwykle ataki DoS/DDoS wykorzystują luki w implementacji modelu Transmission Control Protocol (TCP)/Internet Protocol (IP) lub błędy w określonym systemie operacyjnym (OS).

Koncepcje DoS/DDoS
Aby dobrze zrozumieć ataki DoS/DDoS, należy wcześniej zapoznać się z powiązanymi pojęciami. W tej sekcji zdefiniowano ataki DoS i DDoS oraz omówiono sposób działania ataków DDoS.
Co to jest atak DoS?
Atak DoS to atak na komputer lub sieć, który ogranicza, ogranicza lub uniemożliwia dostęp do zasobów systemowych uprawnionym użytkownikom. Podczas ataku DoS osoby atakujące zalewają system ofiary nieuzasadnionymi żądaniami usług lub ruchem w celu przeciążenia jego zasobów i wyłączenia systemu, co prowadzi do niedostępności strony internetowej ofiary lub przynajmniej znacznego zmniejszenia wydajności systemu lub sieci ofiary. Celem ataku DoS jest uniemożliwienie legalnym użytkownikom korzystania z systemu, a nie uzyskanie nieautoryzowanego dostępu do systemu lub uszkodzenie danych.
Poniżej przedstawiono przykłady typów ataków DoS:
Zalanie systemu ofiary większym ruchem, niż może obsłużyć
Zalewanie usługi (np. Internet Relay Chat (IRC)) większą liczbą zdarzeń, niż może obsłużyć
• Awaria stosu TCP/IP przez wysyłanie uszkodzonych pakietów
• Awaria usługi przez interakcję z nią w nieoczekiwany sposób
• Zawieszenie systemu poprzez wpadnięcie w nieskończoną pętlę

Ataki DoS mają różne formy i są ukierunkowane na różne usługi. Ataki mogą powodować:
Zużycie zasobów
Zużycie przepustowości, miejsca na dysku, czasu procesora lub struktur danych
* Rzeczywiste fizyczne zniszczenie lub zmiana elementów sieci
*Niszczenie oprogramowania i plików w systemie komputerowym
Ogólnie rzecz biorąc, ataki DoS są ukierunkowane na przepustowość sieci lub łączność. Ataki wykorzystujące przepustowość przepełniają sieć dużym ruchem, wykorzystując istniejące zasoby sieciowe, pozbawiając w ten sposób uprawnionych użytkowników tych zasobów. Ataki na łączność przepełniają system dużą liczbą żądań połączeń, pochłaniając wszystkie dostępne zasoby systemu operacyjnego, aby uniemożliwić systemowi przetwarzanie uzasadnionych żądań użytkowników. Weźmy pod uwagę firmę cateringową, która większość swojej działalności prowadzi przez telefon. Jeżeli atakujący chce zakłócić ten biznes, musi znaleźć sposób na zablokowanie firmowych linii telefonicznych, co uniemożliwiłoby firmie prowadzenie działalności. Atak DoS działa na tej samej zasadzie — atakujący wykorzystuje wszystkie sposoby połączenia się z systemem ofiary, uniemożliwiając legalny biznes. Ataki DoS to rodzaj naruszenia bezpieczeństwa, które na ogół nie prowadzi do kradzieży informacji. Jednak ataki te mogą zaszkodzić celowi pod względem czasu i zasobów. Ponadto awaria zabezpieczeń może spowodować utratę usługi, takiej jak poczta e-mail. W najgorszym przypadku atak DoS może spowodować przypadkowe zniszczenie plików i programów milionów ludzi, którzy byli podłączeni do systemu ofiary w momencie ataku.
Co to jest atak DDoS?
Atak DDoS to zakrojony na szeroką skalę, skoordynowany atak na dostępność usług w systemie ofiary lub zasobach sieciowych, przeprowadzany pośrednio przez wiele skompromitowanych komputerów (botnetów) w Internecie. Zgodnie z definicją zawartą w często zadawanych pytaniach dotyczących zabezpieczeń sieci World Wide Web: „Atak rozproszonej odmowy usługi (DDoS) wykorzystuje wiele komputerów do przeprowadzenia skoordynowanego ataku DoS na jeden lub więcej celów.

klient/serwer, sprawca jest w stanie znacznie zwielokrotnić skuteczność ataku typu „odmowa usługi" poprzez wykorzystanie zasobów wielu nieświadomych komputerów współpracujących, które służą jako platformy ataku". w dół, odmawiając w ten sposób usługi uprawnionym użytkownikom. Atakowane usługi należą do „głównej ofiary", podczas gdy skompromitowane systemy użyte do przeprowadzenia ataku nazywane są „ofiarami wtórnymi". Wykorzystanie ofiar wtórnych do przeprowadzenia ataku DDoS umożliwia atakującemu przeprowadzić duży i destrukcyjny atak, jednocześnie utrudniając wyśledzenie pierwotnego atakującego.Głównym celem ataku DDoS jest uzyskanie dostępu administracyjnego do jak największej liczby systemów.Ogólnie rzecz biorąc, osoby atakujące używają dostosowanego skryptu ataku, aby zidentyfikować potencjalnie systemy podatne na ataki Po uzyskaniu dostępu do systemów docelowych atakujący ładuje i uruchamia oprogramowanie DDoS na tych systemach w momencie wybranym do przeprowadzenia ataku. Ataki DDoS stały się popularne ze względu na łatwą dostępność planów exploitów i znikomą ilość pracy umysłowej wymaganej do ich wykonania. Ataki te mogą być bardzo niebezpieczne, ponieważ mogą szybko pochłonąć największe hosty w Internecie, czyniąc je bezużytecznymi. Skutki ataków DDoS obejmują utratę wartości firmy, wyłączenie sieci, straty finansowe i organizacje niepełnosprawnych.

Jak działają ataki DDoS?

Podczas ataku DDoS wiele aplikacji zalewa docelową przeglądarkę lub sieć fałszywymi żądaniami zewnętrznymi, które powodują, że system, sieć, przeglądarka lub witryna są powolne, bezużyteczne, wyłączone lub niedostępne. Atakujący inicjuje atak DDoS, wysyłając polecenie do agentów zombie, które są komputerami podłączonymi do Internetu, narażonymi przez atakującego za pośrednictwem złośliwego oprogramowania, w celu wykonania różnych złośliwych działań za pośrednictwem serwera dowodzenia i kontroli (C&C). Ci agenci zombie wysyłają żądanie połączenia do dużej liczby systemów odbijających ze sfałszowanym adresem IP ofiary, co powoduje, że systemy odbijające zakładają, że te żądania pochodzą z maszyny ofiary, a nie z agentów zombie. W związku z tym systemy reflektorów wysyłają żądane informacje (odpowiedź na żądanie połączenia) do ofiary. W rezultacie maszyna ofiary jest zalewana jednocześnie niechcianymi odpowiedziami z kilku komputerów odzwierciedlających, co może albo obniżyć wydajność, albo spowodować całkowite wyłączenie maszyny ofiary.

Botnety

Termin „bot" jest skrótem słowa „robot" i odnosi się do aplikacji, które wykonują zautomatyzowane zadania przez Internet. Atakujący używają botów do infekowania dużej liczby komputerów, które tworzą sieć lub „botnet", umożliwiając im przeprowadzanie ataków DDoS, generowanie spamu, rozprzestrzenianie wirusów i popełnianie innych rodzajów przestępstw. Ta sekcja dotyczy syndykatów zorganizowanej cyberprzestępczości, schematów organizacyjnych, botnetów i technik rozprzestrzeniania botnetów; ekosystemy botnetów; metody skanowania w celu znalezienia wrażliwych maszyn; i propagacji złośliwego kodu.

Cyberprzestępczość zorganizowana: schemat organizacyjny

Syndykaty przestępczości zorganizowanej

W przeszłości cyberprzestępcy działali niezależnie, ale obecnie działają w zorganizowanych grupach. Coraz częściej są powiązani z syndykatami przestępczości zorganizowanej i wykorzystują wyrafinowane techniki tych syndykatów do angażowania się w nielegalną działalność, zwykle w celu uzyskania korzyści finansowych. Istnieją zorganizowane grupy cyberprzestępców, które działają w hierarchicznej strukturze z predefiniowanym modelem podziału dochodów, co jest rodzajem dużej korporacji oferującej usługi przestępcze. Zorganizowane grupy tworzą i wynajmują botnety oraz oferują różne usługi, począwszy od tworzenia złośliwego oprogramowania i włamań na konta bankowe, a skończywszy na masowych atakach DoS na dowolny cel za odpowiednią opłatą.

Na przykład syndykat przestępczości zorganizowanej może przeprowadzić atak DDoS na bank, aby odwrócić uwagę zespołu bezpieczeństwa banku podczas czyszczenia kont bankowych za pomocą skradzionych danych uwierzytelniających. Rosnące zaangażowanie zorganizowanych syndykatów przestępczych w motywowaną politycznie wojnę cybernetyczną i haktywizm jest przedmiotem troski krajowych agencji bezpieczeństwa. Cyberprzestępczość obejmuje skomplikowaną gamę graczy, a cyberprzestępcy otrzymują wynagrodzenie w zależności od wykonywanego zadania lub zajmowanego stanowiska. Szef organizacji cyberprzestępczej (tj. szef) działa jako przedsiębiorca biznesowy. Szef nie

popełnia bezpośrednio żadnych przestępstw. Bezpośrednio pod szefem w hierarchii organizacyjnej znajduje się „zastępca szefa", który konfiguruje serwer C&C i bazę danych z zestawem narzędzi przestępczych w celu zarządzania wdrażaniem ataków i dostarczania trojanów. Pod zastępcą znajdują się różni „menedżerowie kampanii" z własnymi sieciami afiliacyjnymi do przeprowadzania ataków i kradzieży danych. Wreszcie, sprzedawcy sprzedają skradzione dane.

Botnety

Boty są wykorzystywane do nieszkodliwych działań związanych z gromadzeniem danych lub eksploracją danych, takich jak „przeszukiwanie sieci", a także do koordynowania ataków DoS. Głównym celem bota jest zbieranie danych. Istnieją różne rodzaje botów, takie jak boty internetowe, boty IRC i boty czatujące. Przykładami botów IRC są Cardinal, Sopel, Eggdrop i EnergyMech. Botnet (skrót od „roBOT NETwork") to grupa komputerów „zainfekowanych" przez boty; jednak botnety mogą być wykorzystywane zarówno do celów pozytywnych, jak i negatywnych. Jako narzędzie hakerskie botnet składa się z ogromnej sieci zainfekowanych systemów. Stosunkowo mały botnet składający się z 1000 botów ma łączną przepustowość większą niż przepustowość większości systemów korporacyjnych. Pojawienie się botnetów doprowadziło do ogromnego wzrostu cyberprzestępczości. Botnety stanowią rdzeń centrum aktywności cyberprzestępczej, które łączy i jednoczy różne części cyberprzestępczego świata. Dostawcy usług cyberprzestępczych są częścią sieci cyberprzestępczej. Oferują usługi, takie jak tworzenie złośliwego kodu, kuloodporny hosting, tworzenie exploitów dla przeglądarek oraz szyfrowanie i pakowanie. Złośliwy kod jest podstawowym narzędziem wykorzystywanym przez organizacje przestępcze do popełniania cyberprzestępstw. Właściciele botnetów zlecają zarówno botom, jak i innym szkodliwym programom, takim jak trojany, wirusy, robaki, keyloggery i specjalnie spreparowane aplikacje, aby atakowały komputery zdalne za pośrednictwem sieci. Deweloperzy oferują usługi złośliwego oprogramowania w witrynach publicznych lub zamkniętych zasobach internetowych. Botnety to agenci, których intruz może wysłać do systemu serwera w celu wykonania nielegalnej działalności. Botnety uruchamiają ukryte programy, które umożliwiają identyfikację luk systemowych. Atakujący mogą wykorzystywać botnety do wykonywania żmudnych zadań związanych z badaniem systemu pod kątem znanych luk w zabezpieczeniach.

Atakujący mogą wykorzystywać botnety do wykonywania następujących czynności:

Ataki DDoS: Botnety mogą generować ataki DDoS, które zużywają przepustowość komputerów ofiary. Botnety mogą również przeciążać system, marnując cenne zasoby systemu hosta i niszcząc łączność sieciową.

Spamowanie: osoby atakujące używają serwera proxy SOCKS do rozsyłania spamu. Zbierają adresy e-mail ze stron internetowych lub innych źródeł.

Sniffing ruchu: Sniffer pakietów obserwuje ruch danych wchodzących do zaatakowanej maszyny. Umożliwia atakującemu zbieranie poufnych informacji, takich jak numery kart kredytowych i hasła. Sniffer umożliwia również atakującemu kradzież informacji z jednego botnetu i wykorzystanie ich przeciwko innemu botnetowi. Innymi słowy, botnety mogą okradać się nawzajem.

Keylogging: Keylogging to metoda rejestrowania klawiszy wpisywanych na klawiaturze, która dostarcza poufnych informacji, takich jak hasła systemowe. Atakujący używają keyloggera do zbierania danych logowania do konta w usługach takich jak PayPal.

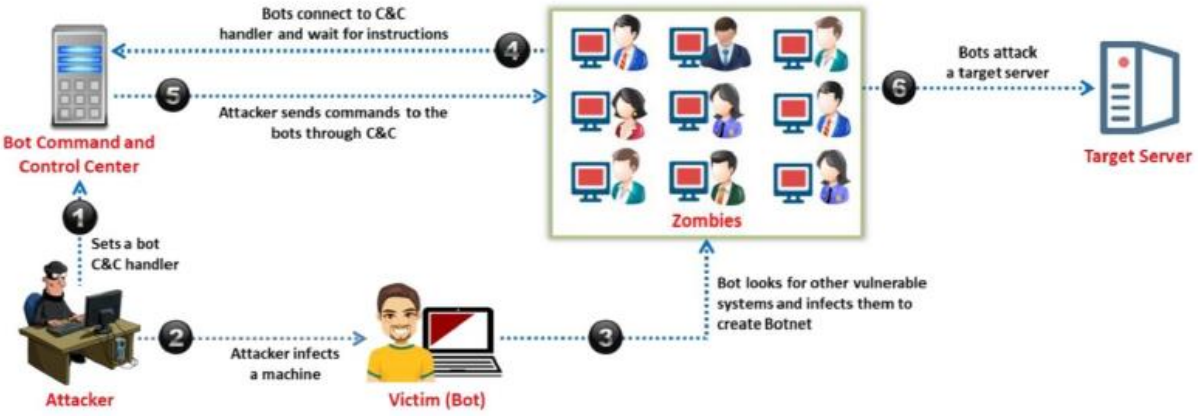
Rozpowszechnianie nowego złośliwego oprogramowania: Botnety mogą być wykorzystywane do rozprzestrzeniania nowych botów.

Instalowanie dodatków reklamowych: Botnety mogą być wykorzystywane do „oszustwa związanego z kliknięciami" poprzez automatyzację kliknięć.

Nadużycia Google AdSense: niektóre firmy zezwalają na wyświetlanie reklam Google AdSense w swoich witrynach internetowych w celu uzyskania korzyści ekonomicznych. Botnety pozwalają intruzowi zautomatyzować kliknięcia reklamy, powodując procentowe zwiększenie kolejki kliknięć.

Ataki na sieci czatów IRC: Nazywane również atakami klonowania, ataki te są podobne do ataków DDoS. Główny agent instruuje każdego bota, aby łączył się z tysiącami klonów w sieci IRC, co może zalać sieć.

Manipulowanie ankietami i grami online: każdy botnet ma unikalny adres, co umożliwia mu manipulowanie ankietami i grami online.
Masowa kradzież tożsamości: botnety mogą wysyłać dużą liczbę e-maili, podszywając się pod renomowaną organizację, taką jak eBay. Ta technika pozwala atakującym na kradzież informacji o kradzieży tożsamości.
Poniższy rysunek ilustruje sposób, w jaki osoba atakująca przeprowadza atak DoS oparty na botnecie na docelowy serwer. Atakujący tworzy centrum C&C bota, po czym infekuje maszynę (bota) i naraża ją na szwank. Później używają tego bota do infekowania i naruszania bezpieczeństwa innych podatnych na ataki systemów dostępnych w sieci, w wyniku czego powstaje botnet. Boty (znane również jako zombie) łączą się z centrum C&C i czekają na instrukcje. Następnie atakujący wysyła szkodliwe polecenia do botów za pośrednictwem centrum C&C. Na koniec, zgodnie z instrukcjami atakującego, boty przeprowadzają atak DoS na serwer docelowy, uniemożliwiając dostęp do jego usług uprawnionym użytkownikom w sieci.



Metody skanowania w celu znalezienia wrażliwych maszyn
Poniżej omówiono metody skanowania wykorzystywane przez atakującego w celu znalezienia wrażliwych maszyn w sieci:
Losowe skanowanie
W tej technice zainfekowana maszyna (maszyna atakującego lub zombie) losowo sonduje adresy IP w zakresie adresów IP sieci docelowej i sprawdza ich podatność na ataki. Po znalezieniu podatnej maszyny włamuje się i próbuje ją zainfekować, instalując ten sam szkodliwy kod, który jest na niej zainstalowany. Ta technika generuje znaczny ruch, ponieważ wiele zainfekowanych maszyn sonduje i sprawdza te same adresy IP. Złośliwe oprogramowanie rozprzestrzenia się szybko w początkowej fazie, a prędkość rozprzestrzeniania się maleje wraz ze zmniejszaniem się liczby dostępnych nowych adresów IP w miarę upływu czasu.
Skanowanie listy trafień
Poprzez skanowanie osoba atakująca najpierw zbiera listę potencjalnie podatnych na ataki maszyn, a następnie tworzy armię zombie. Następnie atakujący skanuje listę, aby znaleźć podatną na ataki maszynę. Po znalezieniu atakujący instaluje na nim złośliwy kod i dzieli listę na pół. Atakujący kontynuuje skanowanie jednej połowy, podczas gdy druga połowa jest skanowana przez nowo skompromitowaną maszynę. Ten proces ciągle się powtarza, powodując wykładniczy wzrost liczby zainfekowanych maszyn. Technika ta zapewnia instalację złośliwego kodu na wszystkich potencjalnie podatnych na ataki komputerach znajdujących się na liście trafień w krótkim czasie.
Skanowanie topologiczne
Technika ta wykorzystuje informacje uzyskane z zainfekowanej maszyny w celu znalezienia nowych podatnych na ataki maszyn. Zainfekowany host sprawdza adresy URL na dysku twardym komputera, który chce zainfekować. Następnie tworzy krótką listę adresów URL i celów oraz sprawdza ich

podatność na ataki. Ta technika daje dokładne wyniki, a jej wydajność jest podobna do techniki skanowania listy trafień.

Skanowanie lokalnej podsieci

w tej technice zainfekowana maszyna wyszukuje nowe podatne maszyny w swojej sieci lokalnej, za zaporą ogniową, wykorzystując informacje ukryte w lokalnych adresach. Atakujący wykorzystują tę technikę w połączeniu z innymi mechanizmami skanowania.

Skanowanie permutacyjne

W tej technice atakujący dzielą wspólną listę pseudolosowych permutacji adresów IP wszystkich maszyn. Lista jest tworzona przy użyciu 32-bitowego szyfru blokowego i wstępnie wybranego klucza. Jeśli zaatakowany host zostanie zainfekowany podczas skanowania listy trafień lub skanowania podsieci lokalnej, lista jest skanowana bezpośrednio za punktem zaatakowanego hosta w celu zidentyfikowania nowych celów. Jeśli zagrożony host zostanie zainfekowany podczas skanowania permutacyjnego, skanowanie zostanie wznowione od losowego punktu. Jeśli zostanie napotkana już zainfekowana maszyna, skanowanie zostanie wznowione od nowego losowego punktu początkowego na liście permutacji. Proces skanowania zatrzymuje się, gdy zaatakowany host kolejno napotyka predefiniowaną liczbę już zainfekowanych maszyn i nie znajduje nowych celów. Następnie generowany jest nowy klucz permutacji w celu zainicjowania nowej fazy skanowania. Skanowanie permutacyjne ma następujące zalety:

o Unika się ponownej infekcji celu.

o Nowe cele są skanowane losowo, co zapewnia wysoką prędkość skanowania.

W jaki sposób rozprzestrzenia się złośliwy kod?

Poniżej omówiono trzy techniki wykorzystywane przez atakującego do rozprzestrzeniania złośliwego kodu i budowania sieci ataku:

Propagacja centralnego źródła

W tej technice atakujący umieszcza zestaw narzędzi do ataku w centralnym źródle, a kopia zestawu narzędzi do ataku jest przesyłana do nowo odkrytego podatnego systemu. Gdy atakujący znajdzie podatną na ataki maszynę, instruuje centralę, aby przeniosła kopię zestawu narzędzi do ataku na nowo zaatakowaną maszynę, na której narzędzia do ataku są automatycznie instalowane pod zarządzaniem przez mechanizm skryptowy. To inicjuje nowy cykl ataku, w którym nowo zainfekowana maszyna szuka innych wrażliwych maszyn i powtarza proces instalacji zestawu narzędzi ataku. Ogólnie ta technika wykorzystuje protokoły HTTP, FTP i RPC.

Propagacja łańcuchów wstecznych

W tej technice osoba atakująca umieszcza zestaw narzędzi ataku we własnym systemie, a jego kopia jest przesyłana do nowo odkrytego systemu podatnego na atak. Narzędzia atakujące zainstalowane na atakującej maszynie używają specjalnych metod w celu zaakceptowania połączenia z zaatakowanego systemu, a następnie przesłania do niego pliku zawierającego narzędzia ataku. Proste nasłuchiwanie portów zawierające kopię tego pliku lub serwery sieciowe w pełni zainstalowane przez intruza, z których oba korzystają z protokołu Trivial File Transfer Protocol (TFTP), obsługują tę kopię pliku kanału zwrotnego.

Propagacja autonomiczna

W przeciwieństwie do wcześniej omówionych mechanizmów, w których zewnętrzne źródło plików przesyła zestaw narzędzi do ataku, w przypadku autonomicznej propagacji atakujący host sam przesyła zestaw narzędzi do ataku do nowo wykrytego podatnego systemu dokładnie w momencie włamania się do tego systemu.

Techniki ataków DoS/DDoS

Atakujący stosują różne techniki przeprowadzania ataków typu „odmowa usługi" (DoS)/rozproszona „odmowa usługi" (DDoS) na docelowe komputery lub sieci. W tej sekcji omówiono podstawowe kategorie wektorów ataków DoS/DDoS, różne techniki ataków oraz różne narzędzia do ataków DoS/DDoS wykorzystywane do przejęcia jednego lub wielu systemów sieciowych w celu wyczerpania zasobów obliczeniowych lub uczynienia ich niedostępnymi dla zamierzonych użytkowników.

Podstawowe kategorie wektorów ataków DoS/DDoS

Ataki DDoS mają głównie na celu zmniejszenie przepustowości sieci poprzez wyczerpanie zasobów sieciowych, aplikacji lub usług, ograniczając w ten sposób legalnym użytkownikom dostęp do zasobów systemowych lub sieciowych. Ogólnie wektory ataków DoS/DDoS są podzielone na następujące kategorie:

Ataki wolumetryczne

Ataki te wyczerpują przepustowość w docelowej sieci/usłudze lub między docelową siecią/usługą a resztą Internetu, powodując blokadę ruchu, uniemożliwiając dostęp uprawnionym użytkownikom. Wielkość ataku jest mierzona w bitach na sekundę (bps). Ataki wolumetryczne DDoS generalnie celują w protokoły, takie jak Network Time Protocol (NTP), Domain Name System (DNS) i Simple Service Discovery Protocol (SSDP), które są bezstanowe i nie mają wbudowanych funkcji unikania zatorów. Generowanie dużej liczby pakietów może spowodować zużycie całej przepustowości w sieci. Pojedyncza maszyna nie może wykonać wystarczającej liczby żądań, aby przeciążyć sprzęt sieciowy. Dlatego w atakach DDoS atakujący używa kilku komputerów do zalania ofiary. W takim przypadku atakujący może kontrolować wszystkie maszyny i poinstruować je, aby kierowały ruch do systemu docelowego. Ataki DDoS zalewają sieć, powodując istotne statystyczne zmiany w ruchu sieciowym, które przeciążają sprzęt sieciowy, taki jak przełączniki i routery. Atakujący wykorzystują moc obliczeniową dużej liczby rozproszonych geograficznie maszyn do generowania ogromnego ruchu skierowanego do ofiary, dlatego taki atak nazywany jest atakiem DDoS.

Istnieją dwa rodzaje ataków powodujących wyczerpanie przepustowości:

o Podczas ataku typu flood zombie wysyłają duże ilości ruchu do systemów ofiary, aby wyczerpać przepustowość tych systemów.

o W przypadku ataku wzmacniającego atakujący lub zombie przesyłają wiadomości na rozgłoszony adres IP. Ta metoda wzmacnia szkodliwy ruch, który zużywa przepustowość systemów ofiary.

Atakujący wykorzystują botnety i przeprowadzają ataki DDoS poprzez zalewanie sieci. Cała przepustowość jest wykorzystywana przez atakujących i nie pozostaje żadna przepustowość do legalnego użytku. Poniżej przedstawiono przykłady technik ataku wolumetrycznego:

o Atak powodziowy protokołu datagramów użytkownika (UDP).
o Atak typu Internet Control Message Protocol (ICMP).
o Atak Ping of Death (PoD).
o Atak Smerfów
o Atak fali tętna
o Atak dnia zerowego
o Zniekształcony atak powodziowy pakietów IP
o Fałszywy atak powodziowy pakietów IP

Ataki na protokół

Atakujący mogą również uniemożliwić dostęp do celu, zużywając zasoby inne niż przepustowość, takie jak tabele stanu połączenia. Ataki DDoS oparte na protokole wyczerpują zasoby dostępne w celu lub na określonym urządzeniu między celem a Internetem. Ataki te wykorzystują tablice stanu połączeń obecne w urządzeniach infrastruktury sieciowej, takich jak moduły równoważenia obciążenia, zapory ogniowe i serwery aplikacji. W związku z tym żadne nowe połączenia nie będą dozwolone, ponieważ urządzenie będzie czekać na zamknięcie lub wygaśnięcie istniejących połączeń. W tym przypadku wielkość ataku jest mierzona w pakietach na sekundę (pps) lub połączeniach na sekundę (cps). Ataki te mogą nawet przejąć stan milionów połączeń utrzymywanych przez urządzenia o dużej pojemności. Poniżej przedstawiono przykłady technik ataku na protokół:

o Synchronizacja (SYN) ataku powodziowego
o Atak fragmentacyjny
o Sfałszowany atak z powodzią sesji
o Zalew potwierdzenia (ACK).
o Atak powodziowy SYN-ACK
o Atak powodziowy ACK i PUSFI ACK
o Atak zalewania połączenia TCP

o Atak na wyczerpanie stanu TCP
o Atak RST
o Atak paniki TCP SACK
Ataki warstwy aplikacji
W tych atakach osoba atakująca próbuje wykorzystać luki w protokole warstwy aplikacji lub w samej aplikacji, aby uniemożliwić uprawnionym użytkownikom dostęp do aplikacji. Ataki na niezałatane, podatne na ataki systemy nie wymagają tak dużej przepustowości, jak ataki protokołowe lub wolumetryczne DDoS, aby odnieść sukces. W atakach aplikacyjnych DDoS warstwa aplikacji lub zasoby aplikacji są zużywane przez otwieranie połączeń i pozostawianie ich otwartych, dopóki nie będzie można nawiązać nowych połączeń. Te ataki niszczą określony aspekt aplikacji lub usługi i mogą być skuteczne w przypadku jednej lub kilku maszyn atakujących, które generują niski ruch. Ponadto ataki te są bardzo trudne do wykrycia i złagodzenia. Wielkość ataku jest mierzona w żądaniach na sekundę (rps). Ataki typu flood na poziomie aplikacji skutkują utratą usług danej sieci, takich jak e-maile i zasoby sieciowe, lub tymczasowym wyłączeniem aplikacji i usług. Za pomocą tego ataku osoby atakujące wykorzystują słabości kodu źródłowego oprogramowania, aby uniemożliwić aplikacji przetwarzanie uzasadnionych żądań. Kilka rodzajów ataków DoS opiera się na exploitach związanych z oprogramowaniem, takich jak przepełnienie bufora. Atak polegający na przepełnieniu bufora wysyła nadmiar danych do aplikacji, która albo ją zamyka, albo wymusza uruchomienie danych wysłanych do aplikacji w systemie hosta. Atak zdalnie powoduje awarię podatnego na ataki systemu, wysyłając nadmierny ruch do aplikacji. Czasami osoby atakujące mogą również wykonać dowolny kod w systemie zdalnym poprzez przepełnienie bufora. Wysyłanie zbyt dużej ilości danych do aplikacji nadpisuje dane kontrolujące program, umożliwiając hakerowi wykonanie kodu.
Korzystając z ataków typu flood na poziomie aplikacji, osoby atakujące próbują wykonać następujące czynności:
o Zalewaj aplikacje internetowe legalnym ruchem użytkowników
o Zakłócać działanie określonego systemu lub osoby, na przykład blokując dostęp użytkownika poprzez wielokrotne nieprawidłowe próby logowania
o Blokowanie połączenia z bazą danych aplikacji poprzez tworzenie złośliwych zapytań w języku SQL (Structured Query Language).
Ataki typu flood na poziomie aplikacji mogą spowodować znaczną utratę pieniędzy, usług i reputacji organizacji. Ataki te mają miejsce po nawiązaniu połączenia. Ponieważ połączenie jest nawiązywane, a ruch wchodzący do celu wydaje się prawidłowy, wykrycie tych ataków jest trudne. Flowever, jeśli użytkownik zidentyfikuje atak, może go zatrzymać i prześledzić do źródła łatwiej niż inne rodzaje ataków DDoS. Poniżej przedstawiono przykłady technik ataku w warstwie aplikacji:
o Atak powodziowy Flypertext Transfer Protocol (HTTP).
o Atak Slowlorisa
o Atak typu flood w warstwie aplikacji UDP
o Atak wymuszony DDoS

Techniki ataków DoS/DDoS
Następnie zostaną omówione następujące techniki ataków DoS/DDoS:
Atak powodziowy UDP
Atak powodziowy ICMP
Atak PodD
Atak smerfów
Atak fali pulsacyjnej
Atak dnia zerowego
Atak powodziowy SYN
Atak fragmentacyjny
Atak powodziowy ACK
Atak HTTPS GET/POST
Atak Slowlorisa

Atak typu flood w warstwie aplikacji UDP
Atak wielowektorowy
Atak równorzędny
Stały atak DoS (PDoS).
Rozproszony atak DoS (DRDoS).
Atak paniki TCP SACK
Atak wyczerpania stanu TCP
Atak wymuszenia DDoS
Sfałszowany atak z powodzią sesji

Atak powodziowy UDP

W przypadku ataku UDP flood osoba atakująca wysyła sfałszowane pakiety UDP z bardzo dużą szybkością przesyłania pakietów do zdalnego hosta na losowych portach serwera docelowego, używając dużego źródłowego zakresu adresów IP. Zalew pakietów UDP powoduje, że serwer wielokrotnie sprawdza nieistniejące aplikacje na portach. W rezultacie legalne aplikacje stają się niedostępne dla systemu, a wszelkie próby uzyskania do nich dostępu zwracają odpowiedź o błędzie z pakietem ICMP „Destination Unreachable". Atak ten zużywa zasoby sieciowe i dostępną przepustowość, wyczerpując sieć do momentu przejścia w tryb offline.

Atak powodziowy ICMP

Administratorzy sieci używają protokołu ICMP głównie do operacji IP, rozwiązywania problemów i przesyłania komunikatów o błędach w przypadku niedostarczonych pakietów. W tym ataku napastnicy wysyłają duże ilości pakietów żądań echa ICMP do systemu ofiary bezpośrednio lub przez sieci refleksyjne. Pakiety te sygnalizują systemowi ofiary konieczność odpowiedzi, a duży ruch powoduje nasycenie przepustowości połączenia sieciowego ofiary, powodując jego przeciążenie, a następnie przestając odpowiadać na uzasadnione żądania TCP/IP. Aby chronić się przed atakami ICMP flood, konieczne jest ustawienie progu, który po przekroczeniu wywołuje funkcję ochrony przed atakami ICMP flood. Po przekroczeniu progu ICMP (domyślnie wartość progowa wynosi 1000 pakietów/s), router odrzuca dalsze żądania echa ICMP ze wszystkich adresów w tej samej strefie bezpieczeństwa przez pozostałą część bieżącej sekundy oraz następną sekundę.

Ping of Death Attack

W ataku Ping of Death (PoD) osoba atakująca próbuje zawiesić, zdestabilizować lub zamrozić docelowy system lub usługę, wysyłając zniekształcone lub przewymiarowane pakiety za pomocą prostego polecenia ping. Załóżmy, że osoba atakująca wysyła pakiet o rozmiarze 65 538 bajtów do docelowego serwera WWW. Ten rozmiar przekracza limit rozmiaru określony w dokumencie RFC 791 IP, który wynosi 65 535 bajtów. Proces ponownego składania wykonywany przez system odbierający może spowodować awarię systemu. W takich atakach tożsamość atakującego można łatwo sfałszować, a atakujący może nie potrzebować szczegółowej wiedzy o docelowej maszynie, z wyjątkiem jej adresu IP.

Atak Smerfów

W ataku Smurf atakujący fałszuje źródłowy adres IP z adresem IP ofiary i wysyła dużą liczbę pakietów żądań ICMP ECHO do sieci rozgłoszeniowej IP. Powoduje to, że wszystkie hosty w sieci rozgłoszeniowej odpowiadają na odebrane żądania ICMP ECHO. Te odpowiedzi są wysyłane do komputera ofiary, ponieważ adres IP został sfałszowany przez atakującego, powodując znaczny ruch na komputerze ofiary i ostatecznie powodując jego awarię.

Atak DDoS na fali pulsacyjnej

Ataki DDoS wykorzystujące falę pulsacyjną to najnowszy rodzaj ataków DDoS wykorzystywanych przez cyberprzestępców do zakłócania standardowych operacji celów. Ogólnie rzecz biorąc, wzorce ataków DDoS to ciągłe przepływy ruchu przychodzącego. Jednak w przypadku ataków DDoS wykorzystujących falę pulsacyjną wzorzec ataku jest okresowy, a atak jest ogromny i pochłania całą przepustowość docelowych sieci. Atakujący wysyłają wysoce powtarzalną serię pakietów w postaci impulsów do ofiary co 10 minut, a sesja ataku trwa około godziny lub kilku dni. Pojedynczy impuls (300 Gb/s lub więcej) w

zupełności wystarcza do zatłoczenia rury sieciowej. Odzyskiwanie po takich atakach jest bardzo trudne, a czasami niemożliwe.

Atak DDoS dnia zerowego

Ataki DDoS dnia zerowego to ataki, w których luki w zabezpieczeniach DDoS nie mają łat ani skutecznych mechanizmów obronnych. Dopóki ofiara nie zidentyfikuje strategii ataku cyberprzestępcy i nie wdroży łaty usuwającej wykorzystywaną lukę DDoS, atakujący aktywnie blokuje wszystkie zasoby ofiary i kradnie jej dane. Ataki te mogą spowodować poważne szkody w infrastrukturze sieciowej i zasobach ofiary. Obecnie nie ma uniwersalnego podejścia do ochrony sieci przed tego typu atakami.

Atak powodzi SYN

W ataku SYN atakujący wysyła dużą liczbę żądań SYN do serwera docelowego (ofiary) z fałszywymi źródłowymi adresami IP. Atak tworzy niekompletne połączenia TCP, które zużywają zasoby sieciowe. Zwykle, gdy klient chce nawiązać połączenie TCP z serwerem, klient i serwer wymieniają następującą serię komunikatów:

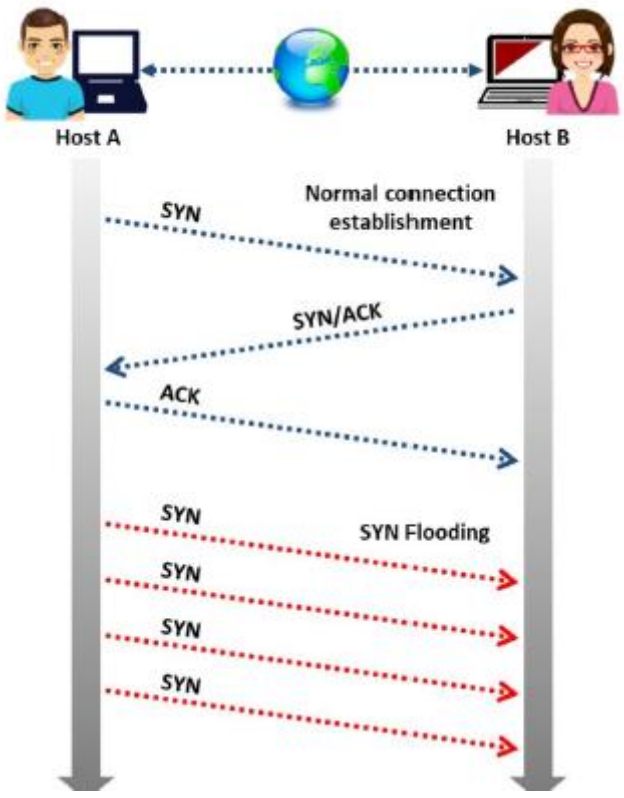
Pakiet żądania TCP SYN jest wysyłany do serwera.

Serwer wysyła SYN/ACK (potwierdzenie) w odpowiedzi na żądanie.

Klient wysyła odpowiedź ACK do serwera, aby zakończyć konfigurację sesji.

Ta metoda to „trójstronny uścisk dłoni”.

W ataku SYN atakujący wykorzystuje metodę trójstronnego uzgadniania. Najpierw atakujący wysyła fałszywe żądanie TCP SYN do serwera docelowego. Po tym, jak serwer wyśle SYN/ACK w odpowiedzi na żądanie klienta (atakującego), klient nigdy nie wysyła odpowiedzi ACK. Powoduje to, że serwer oczekuje na zakończenie połączenia. Zalewanie SYN wykorzystuje wadliwy sposób, w jaki większość hostów implementuje trójstronne uzgadnianie TCP. Ten atak ma miejsce, gdy atakujący wysyła nieograniczoną liczbę pakietów SYN (żądań) do systemu hosta. Proces przesyłania takich pakietów jest szybszy niż system może obsłużyć. Zwykle połączenie jest nawiązywane za pomocą trójstronnego uzgadniania TCP. Host śledzi częściowo otwarte połączenia podczas oczekiwania na pakiety odpowiedzi ACK w kolejce nasłuchującej. Jak pokazano na rysunku, gdy host B otrzymuje żądanie SYN od hosta A, musi śledzić częściowo otwarte połączenie w „kolejce nasłuchiwania” przez co najmniej 75 sekund.



Złośliwy host może wykorzystać inny host, zarządzając wieloma częściowymi połączeniami, wysyłając jednocześnie wiele żądań SYN do hosta docelowego. Gdy kolejka jest pełna, system nie może otwierać nowych połączeń, dopóki nie usunie niektórych wpisów z kolejki połączeń w wyniku przekroczenia limitu czasu uzgadniania. Ta zdolność do wstrzymywania każdego niepełnego połączenia przez 75 s może zostać wykorzystana łącznie w ataku DoS. Atak wykorzystuje fałszywe adresy IP, co utrudnia śledzenie źródła. Osoba atakująca może wypełnić tabelę połączeń nawet bez fałszowania źródłowego adresu IP. Oprócz ataków typu SYN flood, osoby atakujące mogą również wykorzystywać ataki typu SYN-ACK i ACK/PUSH ACK w celu zakłócenia działania maszyn docelowych. Wszystkie te ataki mają podobną funkcjonalność z niewielkimi różnicami.

Atak powodziowy SYN-ACK

Ten typ ataku jest podobny do ataku SYN flood, z tą różnicą, że w tym typie ataku atakujący wykorzystuje drugi etap trójstronnego uzgadniania, wysyłając dużą liczbę pakietów SYNACK do maszyny docelowej w celu wyczerpania jej zasobów.

ACK i PUSH ACK Atak powodziowy

Podczas aktywnej sesji TCP flagi ACK i PUSH ACK są używane do przesyłania informacji do iz serwera i komputerów klienckich do zakończenia sesji. W ataku typu „ACK and PUSH ACK flood" atakujący wysyłają dużą liczbę sfałszowanych pakietów ACK i PUSH ACK do maszyny docelowej, co powoduje, że przestaje ona działać.

Środki zaradcze dla ataków powodziowych SYN

Właściwe filtrowanie pakietów jest realnym rozwiązaniem dla ataków typu SYN flood. Administrator może również dostroić stos TCP/IP, aby zmniejszyć wpływ ataków SYN, jednocześnie zezwalając na legalny ruch klientów. Niektóre ataki SYN nie mają na celu zakłócania pracy serwerów; zamiast tego próbują wykorzystać całą przepustowość połączenia internetowego. Dwa narzędzia do przeciwdziałania temu atakowi to pliki cookie SYN i SynAttackProtect. Aby uchronić się przed próbą wykorzystania przepustowości łącza internetowego przez osobę atakującą, administrator może zastosować dodatkowe środki bezpieczeństwa; na przykład mogą skrócić limit czasu, w którym oczekujące połączenie jest utrzymywane w kolejce w stanie „SYN RECEIVED". Normalnie, jeśli klient nie wyśle odpowiedzi ACK, serwer ponownie prześle pierwszy pakiet ACK. Lukę tę można usunąć, skracając czas retransmisji pierwszego pakietu, zmniejszając liczbę retransmisji pakietów lub całkowicie wyłączając retransmisje pakietów.

Atak fragmentacyjny

Ataki te niszczą zdolność ofiary do ponownego złożenia pofragmentowanych pakietów poprzez zalanie ich fragmentami TCP lub UDP, co skutkuje obniżeniem wydajności. W atakach fragmentacyjnych atakujący wysyła dużą liczbę pofragmentowanych (ponad 1500 bajtów) pakietów do docelowego serwera WWW ze stosunkowo małą szybkością przesyłania pakietów. Ponieważ protokół umożliwia fragmentację, pakiety te nie są zwykle sprawdzane, gdy przechodzą przez sprzęt sieciowy, taki jak routery, zapory ogniowe i system wykrywania włamań (IDS)/system zapobiegania włamaniom (IPS). Ponowne składanie i sprawdzanie tych dużych, pofragmentowanych pakietów pochłania nadmierne zasoby. Ponadto zawartość fragmentów pakietów jest losowo wybierana przez atakującego, co powoduje, że ponowne składanie i sprawdzanie pochłania więcej zasobów, co z kolei powoduje, że system łamie się.

Fałszywy atak powodzi sesji

W tego typu ataku atakujący tworzą fałszywe lub sfałszowane sesje TCP, przenosząc wiele pakietów SYN, ACK i RST lub FIN. Atakujący wykorzystują ten atak do ominięcia zapór ogniowych i przeprowadzania ataków DDoS na sieci docelowe, wyczerpując ich zasoby sieciowe. Poniżej przedstawiono przykłady sfałszowanych ataków typu session flood:

Wielokrotny atak sfałszowanej sesji SYN-ACK

W tego typu atakach typu flood atakujący tworzą fałszywą sesję z wieloma pakietami SYN i wieloma pakietami ACK oraz jednym lub kilkoma pakietami RST lub FIN.

Wielokrotny atak sfałszowanej sesji ACK

W tego rodzaju ataku typu flood atakujący tworzą fałszywą sesję, całkowicie pomijając pakiety SYN i używając tylko wielu pakietów ACK wraz z jednym lub kilkoma pakietami RST lub FIN. Ponieważ pakiety SYN nie są wykorzystywane, a zapory ogniowe używają głównie filtrów pakietów SYN do wykrywania nieprawidłowego ruchu, współczynnik wykrywania DDoS przez zapory ogniowe jest bardzo niski w przypadku tego typu ataków.

Atak HTTP GET/POST

Ataki HTTP to ataki warstwy 7. Klienci HTTP, na przykład przeglądarki internetowe, łączą się z serwerem WWW za pośrednictwem protokołu HTTP w celu wysyłania żądań HTTP, które mogą mieć postać HTTP GET lub HTTP POST. Atakujący wykorzystują te żądania do przeprowadzania ataków DoS. W ataku HTTP GET atakujący używa opóźnionego w czasie nagłówka HTTP, aby zatrzymać połączenie HTTP i wyczerpać zasoby serwera WWW. Atakujący nigdy nie wysyła pełnego żądania do serwera docelowego. W rezultacie serwer zachowuje połączenie HTTP i czeka, co czyni je niedostępnym dla uprawnionych użytkowników. W tego typu atakach wszystkie parametry sieci wyglądają na zdrowe, podczas gdy usługa pozostaje niedostępna. W ataku HTTP POST osoba atakująca wysyła żądania HTTP z pełnymi nagłówkami, ale niepełną treścią wiadomości do docelowego serwera WWW lub aplikacji. Ponieważ treść wiadomości jest niekompletna, serwer czeka na resztę treści, przez co serwer WWW lub aplikacja internetowa jest niedostępna dla uprawnionych użytkowników. Atak HTTP GET/POST to wyrafinowany atak warstwy 7, który nie wykorzystuje zniekształconych pakietów, spoofingu ani technik odbicia. Ten rodzaj ataku wymaga mniejszej przepustowości niż inne ataki, aby doprowadzić do awarii docelowej witryny lub serwera WWW. Atak ten ma na celu zmusić serwer do przydzielenia jak największej ilości zasobów do obsługi ataku, odmawiając w ten sposób uprawnionym użytkownikom dostępu do zasobów serwera.

Ataki typu HTTP flood mające na celu wyczerpanie przepustowości sieci docelowej:

Pojedynczy atak HTTP Flood : w tego typu ataku typu flood atakujący wykorzystuje luki w protokole HTTP 1.1, aby bombardować cel wieloma żądaniami w jednej sesji HTTP.

Atak typu HTTP Flood z pojedynczym żądaniem : W tego typu ataku typu flood atakujący wykonują kilka żądań HTTP z jednej sesji HTTP, maskując te żądania w jednym pakiecie HTTP. Ta technika pozwala atakującym być anonimowymi i niewidocznymi podczas przeprowadzania ataków DDoS.

Rekurencyjny atak HTTP GET Flood

Pozostanie niewykrytym jest kluczowe dla atakujących. Osoba atakująca udająca uprawnionego użytkownika i wykonująca uzasadnione działania może oszukać zaporę ogniową, aby uwierzyła, że źródło jest legalne, podczas gdy tak nie jest. Rekurencyjny GET zbiera listę stron lub obrazów i wygląda na to, że przechodzi przez te strony lub obrazy. Jednak ukradkiem wykonuje zalewające ataki na cel. Rekursywny GET w połączeniu z atakiem HTTP flood może spowodować ogromne szkody dla celu.

Losowy rekurencyjny atak GET Flood

Ten typ ataku jest ulepszoną wersją rekurencyjnego ataku GET flood. Jest przeznaczony dla forów, blogów i innych stron internetowych, które mają strony w sekwencji. Podobnie jak w rekurencyjnym ataku GET flood, w tym ataku rekurencyjny GET udaje przeglądanie stron. Ponieważ celem ataku są fora, grupy i inne blogi, osoba atakująca wykorzystuje losowe liczby z prawidłowego zakresu stron, aby udawać uprawnionego użytkownika i za każdym razem wysyła nowe żądanie GET. Zarówno w rekurencyjnych atakach GET, jak i losowych rekurencyjnych atakach typu GET, cel jest bombardowany dużą liczbą żądań GET, co wyczerpuje jego zasoby.

Atak Slowlorisa

Slowloris to narzędzie ataku DDoS używane do przeprowadzania ataków DDoS warstwy 7 w celu zniszczenia infrastruktury sieciowej. Wyraźnie różni się od innych narzędzi tym, że wykorzystuje całkowicie legalny ruch http do usunięcia serwera docelowego. W atakach Slowloris atakujący wysyła częściowe żądania HTTP do docelowego serwera WWW lub aplikacji. Po otrzymaniu częściowych żądań serwer docelowy otwiera wiele połączeń i czeka na zakończenie żądań. Jednak żądania te pozostają niekompletne, co powoduje zapełnienie maksymalnej puli jednoczesnych połączeń serwera docelowego i odrzucenie dodatkowych prób połączenia.

Atak powodziowy warstwy aplikacji UDP

Chociaż ataki typu flood UDP są znane ze swojego charakteru ataków wolumetrycznych, niektóre protokoły warstwy aplikacji, które opierają się na protokole UDP, mogą być wykorzystywane przez osoby atakujące do przeprowadzania ataków typu flood na sieci docelowe.
Poniżej przedstawiono przykłady protokołów warstwy aplikacji opartych na protokole UDP, które atakujący mogą wykorzystać do zalewania docelowych sieci:
Protokół generatora znaków (CHARGEN)
Proste zarządzanie siecią
Protokół w wersji 2 (SNMPv2)
Cytat dnia (QOTD)
Zdalne wywołanie procedury (RPC)
SSDP
Bezpołączeniowy Lekki
Protokół dostępu do katalogu (CLDAP)
Trywialny protokół przesyłania plików (TFTP)
Sieciowy podstawowy system wejścia/wyjścia
(NetBIOS)
NTP
Protokół sieciowy Quake'a
Protokół parowy
Voice over Internet Protocol (VoIP)

Atak wielowektorowy

W wielowektorowych atakach DDoS osoba atakująca wykorzystuje kombinację ataków wolumetrycznych, protokołów i warstwy aplikacji w celu usunięcia docelowego systemu lub usługi. Atakujący szybko zmienia jedną formę ataku DDoS (np. pakiety SYN) na inną (warstwa 7). Ataki te są przeprowadzane albo za pośrednictwem jednego wektora na raz, albo za pośrednictwem wielu wektorów równolegle, aby zdezorientować dział IT firmy, zmuszając go do wydawania wszystkich zasobów i złośliwego odwracania uwagi.

Atak peer-to-peer

Atak peer-to-peer to forma ataku DDoS, w której atakujący wykorzystuje szereg błędów w serwerach peer-to-peer, aby zainicjować atak DDoS. Atakujący wykorzystują luki wykryte w sieciach korzystających z protokołu Direct Connect (DC++), który umożliwia wymianę plików między klientami komunikatorów internetowych. Ten rodzaj ataku nie wykorzystuje botnetów. W przeciwieństwie do ataku opartego na botnecie, atak peer-to-peer eliminuje potrzebę komunikowania się atakujących z klientami, których atakują. W tym przypadku atakujący instruuje klientów dużych centrów udostępniania plików peer-to-peer, aby odłączyli się od ich sieci peer-to-peer i zamiast tego połączyli się ze stroną internetową ofiary. W rezultacie kilka tysięcy komputerów może agresywnie próbować połączyć się z docelową witryną, powodując spadek wydajności docelowej witryny. Łatwo jest zidentyfikować ataki typu peer-to-peer na podstawie sygnatur. Korzystając z tej metody, osoby atakujące przeprowadzają masowe ataki DoS w celu przejęcia witryn internetowych. Ataki typu peer-to-peer DDoS można zminimalizować, określając porty do komunikacji typu peer-to-peer. Na przykład określenie portu 80 w celu uniemożliwienia komunikacji peer-to-peer minimalizuje możliwość ataków na strony internetowe.

Stały atak typu „odmowa usługi”.

Permanentne ataki DoS (PDoS), znane również jako phlashing, są ukierunkowane wyłącznie na sprzęt i powodują nieodwracalne uszkodzenia sprzętu. W przeciwieństwie do innych rodzajów ataków DoS sabotuje sprzęt systemowy, wymagając od ofiary wymiany lub ponownej instalacji sprzętu. Atak PDoS wykorzystuje luki w zabezpieczeniach urządzenia, aby umożliwić zdalną administrację interfejsami zarządzania sprzętu ofiary, takim jak drukarki, routery i inne urządzenia sieciowe. Ten rodzaj ataku jest szybszy i bardziej destrukcyjny niż konwencjonalne ataki DoS. Działa z ograniczoną ilością zasobów, w przeciwieństwie do ataku DDoS, w którym atakujący uwalniają zestaw zombie na cel. Atakujący przeprowadzają ataki PDoS przy użyciu metody zwanej „murowaniem” systemu. W tej metodzie

atakujący wysyła e-maile, czaty IRC, tweety lub filmy z oszukańczą zawartością w celu aktualizacji sprzętu do ofiary. Aktualizacje sprzętu są modyfikowane i uszkodzone z powodu luk w zabezpieczeniach lub wadliwego oprogramowania układowego. Gdy ofiara kliknie na
link lub wyskakujące okienko odnoszące się do oszukańczej aktualizacji sprzętu, ofiara instaluje ją w swoim systemie. W rezultacie atakujący uzyskuje pełną kontrolę nad systemem ofiary.

Atak paniki TCP SACK

Atak paniki z selektywnym potwierdzeniem TCP (SACK) to zdalny wektor ataku, w którym atakujący próbują zawiesić docelową maszynę z systemem Linux, wysyłając pakiety SACK ze zniekształconym maksymalnym rozmiarem segmentu (MSS). Ten atak wykorzystuje lukę w zabezpieczeniach Linux Socket Buffer (SKB), która może prowadzić do paniki jądra. Ogólnie rzecz biorąc, systemy Linux wykorzystują metodę TCP SACK, w której nadawca jest informowany o pakietach, które zostały pomyślnie potwierdzone przez odbiorcę. Dlatego nadawca może retransmitować tylko te pakiety, które nie zostały pomyślnie potwierdzone przez odbiorcę. Tutaj Linux używa struktury danych połączonej listy zwanej buforem gniazd do przechowywania danych, dopóki nie zostaną potwierdzone lub odebrane. Bufor gniazda może przechowywać maksymalnie 17 segmentów. Następnie potwierdzone pakiety są natychmiast usuwane z połączonej struktury danych. Jeśli gniazdo bufora próbuje zapisać więcej niż 17 segmentów, może to spowodować panikę jądra. Atak paniki TCP SACK wykorzystuje tę lukę w zabezpieczeniach bufora gniazda. Aby to osiągnąć, osoby atakujące wysyłają kolejno specjalnie zaprojektowane pakiety SACK do serwera docelowego, ustawiając MSS na najniższą wartość (48 bajtów). Najniższa wartość MSS zwiększa liczbę segmentów TCP, które należy ponownie przesłać. Ta selektywna retransmisja powoduje, że bufor gniazda serwera docelowego przekracza limit 17 segmentów. W ten sposób bufor gniazda przekracza limit i wyzwala przepełnienie całkowitoliczbowe, powodując panikę jądra, która prowadzi do DoS. Ponieważ luka leży w stosie jądra, osoby atakujące mogą również przeprowadzić ten atak na kontenery i maszyny wirtualne

Środki zaradcze

- Zaimplementuj łatanie luk w zabezpieczeniach
- Zaimplementuj regułę zapory, aby blokować żądania pakietów za pomocą najdłuższego MSS

Atak typu Distributed Reflection Denial of Service (DRDoS).

Atak DoS z rozproszonym odbiciem (DRDoS), znany również jako atak „sfałszowany”, obejmuje użycie wielu maszyn pośredniczących i pomocniczych, które przyczyniają się do ataku DDoS na docelową maszynę lub aplikację. Atak DRDoS wykorzystuje lukę w zabezpieczeniach protokołu TCP dotyczącą trójstronnego uzgadniania. Atak obejmuje maszynę atakującą, ofiary pośrednie (zombie), ofiary drugorzędne (reflektory) i maszynę docelową. Atakujący rozpoczyna ten atak, wysyłając żądania do hostów pośredniczących, które z kolei odzwierciedlają ruch związany z atakiem do celu. Proces ataku DRDoS wygląda następująco. Najpierw atakujący nakazuje ofiarom pośredniczącym (zombie) wysłanie strumienia pakietów (TCP SYN) z adresem IP głównego celu jako źródłowym adresem IP do innych nienaruszonych maszyn (ofiar drugorzędnych lub reflektorów) w celu nakłonienia ich do nawiązać połączenie z głównym celem. W związku z tym reflektory wysyłają ogromny ruch (SYN/ACK) do głównego celu, aby nawiązać z nim nowe połączenie, ponieważ uważają, że zażądał tego host. Główny cel odrzuca pakiety SYN/ACK odebrane z reflektorów, ponieważ nie wysłały pakietu SYN. Tymczasem reflektory czekają na odpowiedź ACK od głównego celu. Zakładając, że pakiet został utracony, maszyny odbijające ponownie wysyłają pakiety SYN/ACK do głównego celu w celu ustanowienia połączenia, aż do upłynięcia limitu czasu. W ten sposób maszyna docelowa jest zalewana dużym ruchem z maszyn odbijających. Połączona przepustowość tych maszyn odbijających przytłacza maszynę docelową. Atak DRDoS jest atakiem inteligentnym, ponieważ namierzenie atakującego jest bardzo trudne lub wręcz niemożliwe. Zamiast rzeczywistego napastnika, drugorzędne ofiary (reflektory) wydają się atakować bezpośrednio główny cel. Ten atak jest bardziej skuteczny niż typowy atak DDoS, ponieważ wiele ofiar pośrednich i wtórnych generuje ogromną przepustowość ataku.

Środki zaradcze

o Wyłącz usługę Character Generator Protocol (CHARGEN), aby zatrzymać tę metodę ataku
o Pobierz najnowsze aktualizacje i poprawki dla serwerów

Atak DDoS z wymuszeniem/okupem DDoS (RDDoS).

Atak wymuszający DDoS jest również określany jako DDoS z żądaniem okupu (RDDoS). W tym przypadku osoby atakujące grożą docelowym organizacjom atakiem DDoS i nalegają na zapłacenie określonej kwoty okupu. Atakujący albo wysyła żądanie okupu, albo inicjuje przykładowy atak DDoS przy użyciu botnetu na określone zasoby organizacji, aby przekonać je, że atak jest prawdziwy. W rezultacie ofierze dostarczany jest e-mail z żądaniem okupu lub wymuszeniem z opcją płatności, terminem itp. i ostrzeżeniem, że pierwotny atak może zostać przeprowadzony w dowolnym momencie. Żądanie okupu może również zawierać krótkie wiadomości lub serię wiadomości grożących ofierze lukami w zabezpieczeniach, ujawnionymi zasobami lub danymi, po których następuje instrukcja zapłaty okupu za pośrednictwem waluty cyfrowej. Ogólnie rzecz biorąc, osoby atakujące udają te ataki, twierdząc, że dysponują narzędziami DDoS o dużej pojemności, które mogą spowodować potencjalne szkody dla działalności organizacji.

Środki zaradcze

Wdrażaj skuteczne narzędzia obrony przed atakami DDoS
Po otrzymaniu żądania okupu natychmiast zgłoś się do organów ścigania i zespołów bezpieczeństwa
Często oceniaj aktywa pod kątem tolerancji ryzyka
Wdrażaj strategie łagodzenia skutków, takie jak BGP/DNS swing i usługa ochrony zawsze włączona

HOIC

HOIC to aplikacja do ataków sieciowych i ataków DoS/DDoS napisana w języku BASIC. Jest przeznaczony do jednoczesnego atakowania do 256 docelowych adresów URL. Wysyła żądania HTTP POST i GET do komputera korzystającego z GUI inspirowanego lulz. Jego cechy są podsumowane w następujący sposób:
Szybkie, wielowątkowe zalewanie HTTP
Jednoczesne zalewanie do 256 stron internetowych
Wbudowany system skryptów umożliwiający wdrażanie „boosterów/7, które są skryptami
zaprojektowany, aby udaremnić środki zaradcze DDoS i zwiększyć wydajność DoS
Przenośność do systemu Linux/Mac z kilkoma poprawkami błędów
Możliwość wyboru liczby wątków w trwającym ataku
Możliwość indywidualnego dławienia ataków za pomocą trzech ustawień: NISKI, ŚREDNI i WYSOKI

LOIC

LOIC to aplikacja do testowania warunków skrajnych sieci i ataków DoS. Ataki LOIC można nazwać atakami DOS opartymi na aplikacjach, ponieważ ich celem są głównie aplikacje internetowe. LOIC może być używany w witrynie docelowej do zalewania serwera pakietami TCP, pakietami UDP lub żądaniami HTTP z zamiarem zakłócenia działania usługi.
Oto niektóre z dodatkowych narzędzi ataku DoS/DDoS:

- XOIC (http://anonhacktivism.blogspot.com)
- HULK (https://github.com)
- Metasploit (https://www.metasploit.com)
- Młot Tora (https://sourceforge.net)
- Slowloris (https://github.com)
- PyLoris (https://sourceforge.net)

Narzędzia ataków DoS/DDoS na urządzenia mobilne

LOIC

Wersja Androida oprogramowania LOIC służy do zalewania pakietów, co umożliwia atakującemu do przeprowadzenia ataku DDoS na organizację docelową. Ta aplikacja może przeprowadzać ataki typu UPD, HTTP lub TCP flood.

AnDOSid

AnDOSid pozwala atakującemu zasymulować atak DoS (a dokładnie atak HTTP POST flood) oraz atak DDoS na serwer WWW z telefonów komórkowych.

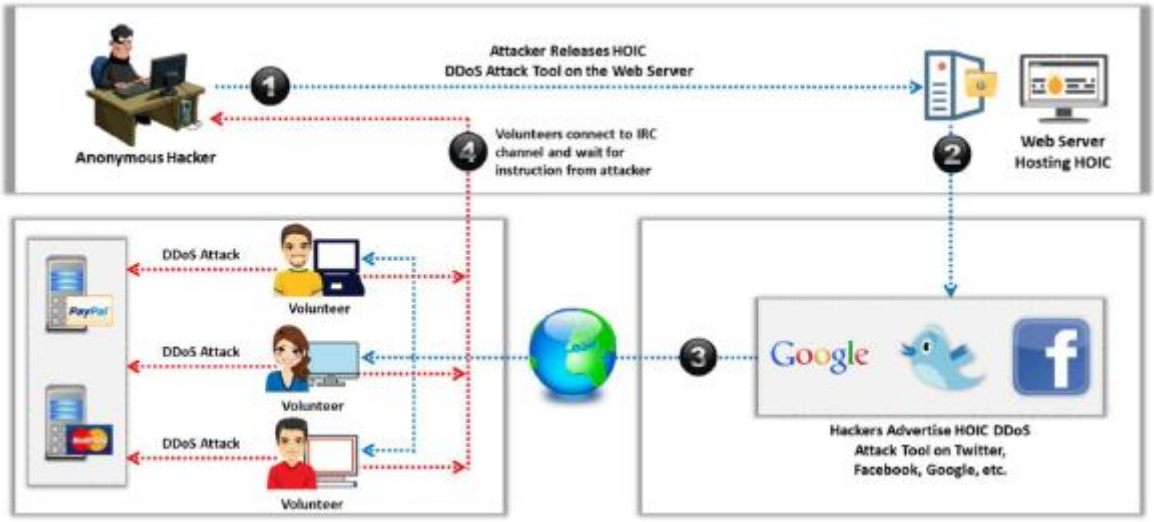
Studium przypadku ataków DDoS

Ataki DDoS to wyrafinowane i złożone ataki oparte na DoS i wielu rozproszonych źródłach ataków. Podczas ataku DDoS duża liczba skompromitowanych komputerów (zombie) przerywa lub zawiesza usługi sieciowe. W tej sekcji przedstawiono studium przypadku ataku DDoS.

Atak DDoS

W ataku DDoS napastnicy wykorzystują grupę skompromitowanych systemów (botów lub zombie), zwykle zainfekowanych trojanami, do przeprowadzenia ataku DoS na docelowy system lub zasób sieciowy.

Jak pokazano na rysunku, anonimowy haker udostępnia narzędzie do ataku DDoS (High Orbit Ion Cannon (HOIC)) na należącym do niego serwerze sieciowym lub na zaatakowanym serwerze sieciowym. Następnie haker reklamuje narzędzie do ataku HOIC DDoS na portalach społecznościowych lub w wyszukiwarkach, takich jak Twitter, Facebook i Google, za pomocą złośliwego łącza do pobrania.



Użytkownicy, którzy chcą przeprowadzić atak DDoS, mogą pobrać narzędzie do ataku HOIC DDoS, klikając złośliwy link do pobrania dostarczony przez hakera. Ci użytkownicy są określani jako „wolontariusze". Wszyscy ochotnicy łączą się przez kanał IRC z anonimowym hakerem i czekają na dalsze instrukcje. Haker instruuje ochotników, aby zalali docelowy serwer sieciowy (np. PayPal, MasterCard i PAYBACK) wieloma żądaniami. Po otrzymaniu instrukcji wolontariusze postępują zgodnie z nimi. W rezultacie serwer docelowy zostaje przeciążony i przestaje odpowiadać na żądania nawet legalnych użytkowników.

Hakerzy reklamują linki do pobierania botnetów

Hakerzy reklamują botnety na różnych blogach, wyszukiwarkach, portalach społecznościowych, w wiadomościach e-mail itd. za pomocą linków do pobierania. Hakerzy używają również fałszywych aktualizacji i alertów bezpieczeństwa, aby nakłonić ofiarę do pobrania złośliwego oprogramowania. Celem takiego działania jest rozprzestrzenienie botnetu i zwiększenie rozmiaru sieci atakującej. Ta metoda ataku jest bardzo szybka i skuteczna. Poniższy rysunek przedstawia przykłady reklam hostowanych przez hakerów w Internecie w celu pobierania botnetów.

Wykorzystanie urządzeń mobilnych jako botnetów do przeprowadzania ataków DDoS

Urządzenia z Androidem są pasywnie podatne na różne złośliwe oprogramowanie, takie jak trojany, boty, trojany dostępu zdalnego (RAT) itd., które często można znaleźć w zewnętrznych sklepach z aplikacjami. Te niezabezpieczone urządzenia z Androidem stają się głównymi celami atakujących, którzy chcą rozszerzyć swoją sieć botnetów, ponieważ są bardzo podatne na złośliwe oprogramowanie. Złośliwa aplikacja na Androida znaleziona w sklepie Google Play i pobrana jako drive-by download to przykłady metod infekcji. Atakujący wiąże złośliwy serwer z plikiem pakietu aplikacji Android (APK),

szyfruje go i usuwa niechciane funkcje i uprawnienia przed dystrybucją złośliwego pakietu do zewnętrznego sklepu z aplikacjami, takiego jak Google Play Store. Gdy ofiary zostaną nakłonione do pobrania i zainstalowania takich aplikacji, urządzenie ofiary jest przejmowane przez atakującego i integrowane z mobilnym botnetem atakującego w celu wykonywania złośliwych działań, takich jak ataki DDoS i wstrzykiwanie sieciowe.

Analiza przypadku DDoS: Atak DDoS na platformę Microsoft Azure

Microsoft Azure to platforma przetwarzania w chmurze przeznaczona do zarządzania aplikacjami w chmurze z centrów danych firmy Microsoft. W sierpniu 2021 r. firma Microsoft napotkała niszczycielski atak DDoS o przepustowości 2,4 Tb/s, w wyniku którego jej usługa była niedostępna dla klientów platformy Azure przez ponad 10 minut. Ten atak był o 140% większy niż poprzedni atak 1 Tb/s, który został wykryty i złagodzony na platformie Azure w trzecim kwartale 2020 r.

Oś czasu ataku

Atak DDoS miał miejsce w ostatnim tygodniu sierpnia 2021 r. Ten atak odbicia UDP spowodował, że usługi platformy Azure były niedostępne dla klientów z Europy w godzinach od 14:30 do 14:40. Chociaż atak był krótkotrwały, zaatakowana organizacja europejska doświadczyła nieoczekiwanego napływu ruchu UDP, który zepsuł usługę. Jednak platforma ochrony przed atakami DDoS platformy Azure ograniczała atak w sposób ciągły

monitorowanie infrastruktury w wielu punktach w sieci. Wykrył anomalię w stosunku ruchu przychodzącego i zaalarmował specjalistów ds. bezpieczeństwa. Poniższy zrzut ekranu pokazuje porównawczą przepustowość przychodzącą ataków DDoS w 2020 i 2021 roku. Pierwsza część ataku osiągnęła najwyższy poziom 2,4 Tb/s z 70 000 źródeł o 14:30, następnie nastąpił drugi wzrost o 0,55 Tb/s około 14:35 i trzeci wzrost o 1,7 Tb/s nieco po 14:40. Poniższy rysunek przedstawia trzy różne szczyty w ciągu 10 minut.

Mechanizm ataku

Był to atak odbiciowy UDP zainicjowany z dużej liczby sfałszowanych pakietów UDP, których maksymalna prędkość wynosiła 2,4 Tb/s. Nadużywane lub sfałszowane pakiety UDP zawierały fałszywe adresy IP, które przypominały źródłowy adres IP, co razem zwiększało rozmiar ataku. Sfałszowane pakiety UDP zostały wysłane do serwera pośredniczącego, który zaczął odpowiadać na źródłowe adresy IP powodując opóźnienie usługi. Atak pochodził z różnych krajów Azji i Pacyfiku, w tym z Malezji, Wietnamu, Tajwanu, Japonii i Chin, a także ze Stanów Zjednoczonych. Atak miał na celu wywołanie spustoszenia poprzez przytłoczenie docelowej sieci Azure ogromnym ruchem w celu zmniejszenia przepustowości sieci. Atakujący wykorzystali do przeprowadzenia tego ataku typowe obciążenia sieciowe atakowanej organizacji. Ten duży współczynnik wzmocnienia spowodował druzgocący napływ danych z prędkością 2,4 Tb/s do usługi w chmurze Azure i zakłócił jej normalne działanie.

Odpowiedź Microsoftu

Microsoft twierdzi, że platforma ochrony DDoS platformy Azure, która została zaprojektowana z myślą o przyszłych atakach DDoS, była w stanie wyśledzić i złagodzić ten atak. Twierdzi również, że usługa ochrony może wchłonąć dużą liczbę ataków DDoS, zanim dotrą one do klientów. Firma twierdzi również, że jej platforma ochrony zapewnia dodatkowe zabezpieczenia wykraczające poza wystarczające możliwości łagodzenia skutków. Na przykład, jeśli normalny ruch bazowy zmienia się w większym stopniu, ich logika płaszczyzny kontrolnej DDoS szybko inicjuje wszystkie możliwe kroki wykrywania wymagane w przypadku powodzi o małej lub dużej objętości, co natychmiast rozpoczyna proces łagodzenia skutków. Zapewnia to szybsze łagodzenie skutków i zapobiega uszkodzeniom zasobów [przeciw dużyme atakom.

Środki zaradcze przed atakami DoS/DDoS

DoS/DDoS to jedno z głównych zagrożeń bezpieczeństwa w Internecie; w związku z tym istnieje wielka potrzeba rozwiązań łagodzących te ataki. W tej sekcji omówiono metody wykrywania, różne środki zapobiegawcze, reakcje na ataki DoS/DDoS oraz sprzętowe/programowe narzędzia ochrony DoS/DDoS, które skutecznie chronią sieci przed atakami DoS/DDoS.

Techniki wykrywania

Techniki wczesnego wykrywania pomagają zapobiegać atakom DoS/DDoS. Wykrywanie ataku DoS/DDoS to trudne zadanie. Wykrywacz ruchu atakującego DoS/DDoS musi rozróżnić autentyczny i

fałszywy pakiet danych, co nie zawsze jest możliwe. Dlatego stosowane w tym celu techniki nie są doskonałe. Zawsze istnieje ryzyko pomylenia ruchu generowanego przez legalnego użytkownika sieci z ruchem generowanym przez atak DoS/DDoS. Techniki wykrywania opierają się na identyfikowaniu i rozróżnianiu nielegalnego wzrostu ruchu i zdarzeń flash z legalnego ruchu pakietowego. Jednym z problemów związanych z filtrowaniem fałszywego ruchu z legalnego ruchu jest wielkość ruchu. Niemożliwe jest przeskanowanie każdego pakietu danych w celu zapewnienia bezpieczeństwa przed atakiem DoS/DDoS. Wszystkie stosowane obecnie techniki wykrywania definiują atak jako nienormalne i zauważalne odchylenie w statystykach i charakterystyce ruchu sieciowego. Techniki te obejmują analizę statystyczną odchyleń w celu kategoryzowania złośliwego i prawdziwego ruchu. Poniżej przedstawiono trzy rodzaje technik wykrywania:

Profilowanie aktywności

Profilowanie aktywności odbywa się na podstawie średniej szybkości przesyłania pakietów dla przepływu sieciowego, która składa się z następujących po sobie pakietów z podobnymi informacjami nagłówkowymi. Informacje nagłówka pakietu obejmują adresy IP miejsca docelowego i nadawcy, porty i używane protokoły transportowe. Atak jest wskazany przez

o Wzrost aktywności wśród klastrów przepływów sieciowych

o Wzrost ogólnej liczby odrębnych klastrów (atak DDoS)

Dla wyższej średniej szybkości pakietów lub poziomu aktywności strumienia, czas pomiędzy kolejnymi pasującymi pakietami jest krótszy. Losowość średniej szybkości przesyłania pakietów lub poziomu aktywności może wskazywać na podejrzaną aktywność. Metoda obliczania entropii mierzy losowość poziomów aktywności. Jeśli sieć jest atakowana, entropia poziomów aktywności sieci wzrasta. Jedną z głównych przeszkód w metodzie profilowania aktywności jest ogromne natężenie ruchu. Ten problem można przezwyciężyć, grupując przepływy pakietów o podobnych właściwościach. Ponieważ ataki DoS generują dużą liczbę pakietów danych, które są bardzo podobne, wzrost średniej szybkości przesyłania pakietów lub wzrost różnorodności pakietów może oznaczać atak DoS.

Sekwencyjne wykrywanie punktu zmiany

W technice sekwencyjnego wykrywania punktów zmiany ruch sieciowy jest filtrowany według adresów IP, docelowych numerów portów i używanych protokołów komunikacyjnych, a dane dotyczące przepływu ruchu są zapisywane na wykresie, który przedstawia natężenie przepływu ruchu w funkcji czasu. Algorytmy wykrywania punktów zmiany izolują zmiany w statystykach ruchu sieciowego i szybkości przepływu ruchu spowodowane atakami. Jeśli nastąpi drastyczna zmiana natężenia ruchu, może wystąpić atak DoS. Technika ta wykorzystuje algorytm sumy skumulowanej (CUSUM) do identyfikowania i lokalizowania ataków DoS. Algorytm oblicza odchylenia między rzeczywistą a oczekiwaną średnią lokalną w szeregach czasowych ruchu. Technika sekwencyjnego wykrywania punktów zmiany identyfikuje typowe czynności skanowania robaków sieciowych.

Analiza sygnału oparta na falkach

Technika analizy falkowej analizuje ruch sieciowy pod kątem składowych widma. Dzieli przychodzące sygnały na różne częstotliwości i osobno analizuje różne składowe częstotliwości. Analiza energii każdego okna widmowego ujawnia obecność anomalii. Techniki te sprawdzają składowe częstotliwości obecne w określonym czasie i dostarczają opisu tych składowych. Obecność nieznanej częstotliwości wskazuje na podejrzaną aktywność sieciową. Sygnał sieciowy składa się ze zlokalizowanego w czasie sygnału przepływu pakietów danych i szumu tła. Analiza sygnału oparta na falkach odfiltrowuje sygnały wejściowe nieprawidłowego przepływu ruchu z szumu tła. Normalny ruch sieciowy to na ogół ruch o niskiej częstotliwości. Podczas ataku wzrastają składowe sygnału o wysokiej częstotliwości.

Strategie przeciwdziałania DoS/DDoS

• Absorpcja ataku: W tej strategii dodatkowa pojemność jest wykorzystywana do absorpcji ataku, co wymaga wcześniejszego planowania. Wymaga to również dodatkowych zasobów. Wadą tej strategii jest koszt dodatkowych zasobów, który jest ponoszony nawet wtedy, gdy nie są przeprowadzane żadne ataki.

• Degradacja usług: Jeśli nie jest możliwe utrzymanie działania wszystkich usług podczas ataku, dobrym pomysłem jest utrzymanie funkcjonalności przynajmniej usług krytycznych. W tym celu najpierw

identyfikowane są usługi krytyczne, po czym projekty sieci, systemów i aplikacji są dostosowywane w celu ograniczenia usług niekrytycznych. Ta strategia może pomóc w utrzymaniu funkcjonalności krytycznych usług.
• Zamykanie usług: w tej strategii wszystkie usługi są wyłączane do czasu ustania ataku. Chociaż może to nie być idealny wybór, w niektórych przypadkach może być rozsądną reakcją.
Zaproponowano wiele rozwiązań ograniczających skutki ataku DDoS. Jednak nie istnieje żadne kompletne rozwiązanie, które chroniłoby wszystkie znane formy ataków DDoS. Ponadto osoby atakujące nieustannie opracowują nowe metody przeprowadzania ataków DDoS w celu obejścia zastosowanych rozwiązań bezpieczeństwa.
Poniżej przedstawiono przykłady środków zaradczych przeciwko atakom DDoS:
• Chroń wtórne ofiary
• Wykrywaj i neutralizuj opiekunów
• Zapobiegaj potencjalnym atakom
• Odbijaj ataki
• Łagodzenie ataków
• Kryminalistyka po ataku

Użytkownicy indywidualni

Najlepszą metodą zapobiegania atakom DDoS jest uniemożliwienie systemom ofiar drugorzędnych wzięcia udziału w ataku. Wymaga to zintensyfikowanej świadomości bezpieczeństwa i technik zapobiegawczych. Wtórne ofiary muszą regularnie monitorować swoje bezpieczeństwo, aby zachować ochronę przed oprogramowaniem agenta DDoS. Należy upewnić się, że system nie instaluje żadnego programu agenta DDoS; ponadto ruch agenta DDoS nie może być przenoszony do sieci. Należy regularnie instalować i aktualizować oprogramowanie antywirusowe i antytrojańskie, a także łatki do oprogramowania usuwające znane luki w zabezpieczeniach. Ponadto należy zwiększyć świadomość w zakresie bezpieczeństwa i technik prewencyjnych wśród wszystkich użytkowników Internetu. Ważne jest, aby wyłączyć niepotrzebne usługi, odinstalować nieużywane aplikacje i przeskanować wszystkie otrzymane pliki ze źródeł zewnętrznych. Ponieważ zadania te mogą wydawać się zniechęcające dla przeciętnego użytkownika sieci, podstawowy sprzęt i oprogramowanie systemów komputerowych są wyposażone w zintegrowane mechanizmy chroniące przed wstawieniem złośliwego kodu. Dlatego mechanizmy obronne wbudowane w podstawowy sprzęt i oprogramowanie systemów muszą być odpowiednio skonfigurowane i regularnie aktualizowane, aby uniknąć ataków DDoS. Zastosowanie powyższych środków zaradczych pozostawi atakujących bez sieci ataków DDoS, za pośrednictwem której mogliby przeprowadzać ataki DDoS.

Dostawcy usług sieciowych

Dostawcy usług i administratorzy sieci mogą ustalać dynamiczne ceny za korzystanie z sieci, aby pobierać opłaty od potencjalnych ofiar drugorzędnych za dostęp do Internetu, a tym samym zachęcać je do większej aktywności w zapobieganiu staniu się częścią ataku DDoS.

Ograniczanie szybkości

Ograniczanie szybkości to technika używana do kontrolowania szybkości ruchu wychodzącego lub przychodzącego kontrolera interfejsu sieciowego. Ta technika skutecznie zmniejsza duży ruch przychodzący, który powoduje atak DDoS. Szczególnie ważne jest zastosowanie tej techniki w urządzeniach sprzętowych, w których technika ta jest skonfigurowana tak, aby ograniczać szybkość żądań w warstwach 4 i 5 modelu Open Systems Interconnection (OSI).

Odbijaj ataki

Systemy skonfigurowane z ograniczonym bezpieczeństwem, znane również jako honeypoty, działają jako przynęta dla atakującego. Ostatnie badania pokazują, że honeypot może imitować wszystkie aspekty sieci, w tym jej serwery WWW, serwery poczty i klientów. Honeypoty są celowo konfigurowane z niskim poziomem bezpieczeństwa, aby przyciągnąć uwagę atakujących DDoS i służyć jako sposób na uzyskanie informacji o atakujących, technikach ataku i narzędziach poprzez przechowywanie rejestru działań systemowych. Atakujący DDoS zwabieni przez honeypot instalują moduły obsługi lub kod agenta w honeypot. Pozwala to uniknąć kompromitowania systemów, które

są bardziej wrażliwe. Honeypoty nie tylko chronią system przed atakującymi, ale także śledzą szczegóły działań atakujących, rejestrując informacje o aktywności. W związku z tym właściciel honeypota może prowadzić rejestr czynności obsługi i/lub agenta. Użytkownicy mogą wykorzystać tę wiedzę do obrony przed wszelkimi przyszłymi atakami instalacyjnymi DDoS. Podejście dogłębnej obrony z Internet Protocol Security (IPsec) może być stosowane w różnych punktach sieci w celu przekierowania podejrzanego ruchu DoS do kilku honeypotów. Istnieją dwa różne typy honeypotów:

- Honeypoty o niskiej interakcji
- Honeypoty o wysokiej interakcji

Przykładem honeypotów o wysokiej interakcji jest honeynet. Honeynets tworzą infrastrukturę bezpieczeństwa; innymi słowy, symulują pełny układ sieci komputerowej, ale pierwotnie są przeznaczone do „przechwytywania" ataków. Celem jest stworzenie sieci, w której wszystkie działania są kontrolowane i śledzone. Ta sieć zawiera potencjalne wabiki ofiar, a nawet prawdziwe komputery z prawdziwymi aplikacjami.

Czujnik KFS

KFSensor to oparty na systemie Windows system wykrywania włamań typu honeypot (IDS). Działa jak honeypot zaprojektowany do przyciągania i wykrywania hakerów i robaków poprzez symulowanie wrażliwych usług systemowych i trojanów. Reagując emulacją prawdziwej usługi, KFSensor może ujawnić naturę ataku, zachowując jednocześnie całkowitą kontrolę i unikając ryzyka naruszenia bezpieczeństwa. Działając jako serwer wabiący, może odwrócić ataki od krytycznych systemów i zapewnić wyższy poziom informacji, niż można osiągnąć przy użyciu samych zapór ogniowych i sieciowego IDS (NIDS).

Poniżej przedstawiono przykłady dodatkowych narzędzi do przeciwdziałania atakom DoS/DDoS (garnek miodu):

SSHHiPot (https://github.com)
Artyleria (https://github.com)
Cowrie (https://github.com)

Łagodzenie ataków

Równoważenie obciążenia

Dostawcy przepustowości mogą zwiększyć przepustowość na krytycznych połączeniach w przypadku ataku DDoS, aby zapobiec wyłączeniu ich serwerów. Korzystanie z replikowanego modelu serwera zapewnia dodatkową ochronę przed awarią. Zreplikowane serwery pomagają w lepszym zarządzaniu obciążeniem, równoważąc obciążenia na każdym serwerze w architekturze wieloserwerowej; zwiększają również normalną wydajność sieci i łagodzą skutki ataku DDoS.

Ograniczanie

Ograniczanie polega na konfigurowaniu routerów w celu uzyskania dostępu do serwera z logiką ograniczania poziomów ruchu przychodzącego, które są bezpieczne dla serwera. Przepustnice „min-max fair server-centric router" (kontrola minimalnej i maksymalnej przepustowości) pomagają użytkownikom zapobiegać wyłączaniu ich serwerów. Ograniczanie przepustowości pomaga zapobiegać uszkodzeniom serwerów poprzez kontrolowanie ruchu DoS. Ta metoda pomaga routerom zarządzać dużym ruchem przychodzącym, aby serwer mógł go obsłużyć. Filtruje również legalny ruch użytkowników z fałszywego ruchu związanego z atakami DDoS i można go rozszerzyć, aby ograniczać ruch związany z atakami DDoS, jednocześnie zezwalając na legalny ruch użytkowników w celu uzyskania lepszych wyników. Głównym ograniczeniem tej metody jest to, że może ona wywołać fałszywe alarmy. Czasami może przepuszczać szkodliwy ruch, jednocześnie odrzucając część legalnego ruchu.

Odrzuć żądania

Inną metodą jest odrzucanie pakietów, gdy wzrasta obciążenie. Zwykle zadanie to wykonuje router lub serwer. Jednak przed kontynuowaniem żądania system skłania wnioskodawcę do odrzucenia żądania, zmuszając go do rozwiązania trudnej zagadki, która wymaga dużo pamięci lub mocy obliczeniowej. W rezultacie użytkownicy systemów zombie wykrywają spadek wydajności i mogą być zniechęceni do udziału w przekazywaniu ruchu związanego z atakami DDoS.

Kryminalistyka po ataku

Analiza wzorców ruchu

Podczas ataku DDoS narzędzie wzorców ruchu przechowuje dane po ataku, które użytkownicy analizują w celu zidentyfikowania cech unikalnych dla atakującego ruchu. Dane te są pomocne w aktualizowaniu środków zaradczych dotyczących równoważenia obciążenia i ograniczania przepustowości w celu zwiększenia ich wydajności i możliwości ochrony. Co więcej, wzorce ruchu związanego z atakami DDoS mogą pomóc administratorom sieci w opracowaniu nowych technik filtrowania, aby zapobiegać przedostawaniu się i opuszczaniu ruchu związanego z atakami DDoS. Analiza wzorców ruchu DDoS może również pomóc administratorom sieci w upewnieniu się, że osoba atakująca nie może wykorzystać ich serwerów jako platformy DDoS do włamania się do innych witryn.

Śledzenie pakietów

Śledzenie wsteczne pakietów odnosi się do śledzenia wstecznego ruchu związanego z atakami. Jest to podobne do inżynierii odwrotnej. W tej metodzie docelowa ofiara działa wstecz, śledząc pakiet do jego źródła. Gdy ofiara zidentyfikuje prawdziwe źródło, może podjąć kroki w celu zablokowania dalszych ataków z tego źródła, opracowując niezbędne techniki zapobiegawcze. Ponadto śledzenie wsteczne pakietów może pomóc w zdobyciu wiedzy na temat różnych narzędzi i technik używanych przez atakującego. Informacje te mogą pomóc w opracowaniu i wdrożeniu różnych technik filtrowania w celu blokowania ataków.

Analiza dziennika zdarzeń

Dzienniki zdarzeń DDoS pomagają w dochodzeniach kryminalistycznych i egzekwowaniu prawa, co jest pomocne, gdy atakujący powoduje poważne straty finansowe. Dostawcy mogą używać pułapek typu honeypot i innych mechanizmów bezpieczeństwa sieci, takich jak zapory ogniowe, sniffery pakietów i dzienniki serwerów, aby przechowywać wszystkie zdarzenia, które miały miejsce podczas konfigurowania i przeprowadzania ataku. Dzięki temu administratorzy sieci mogą rozpoznać typ ataku DDoS lub kombinację zastosowanych ataków. Routery, zapory ogniowe i dzienniki IDS mogą być analizowane w celu zidentyfikowania źródła ruchu DoS. Ponadto administratorzy sieci mogą próbować prześledzić wstecz adres IP atakującego z pomocą pośredniczących dostawców usług internetowych i organów ścigania.

Techniki obrony przed botnetami

Istnieją cztery techniki obrony przed botnetami:

Filtrowanie zgodne z RFC 3704

RFC 3704 to podstawowy filtr listy kontroli dostępu (ACL), który ogranicza wpływ ataków DDoS poprzez blokowanie ruchu ze sfałszowanymi adresami. Ten filtr wymaga źródła pakietów z prawidłowej, przydzielonej przestrzeni adresowej, która jest zgodna z topologią i alokacją przestrzeni. „Bogon list" zawiera wszystkie nieużywane lub zarezerwowane adresy IP, które nie powinny pochodzić z Internetu. Jeśli pakiet pochodzi z dowolnego adresu IP z listy bogon, pakiet pochodzi ze sfałszowanego źródłowego adresu IP i filtr powinien go odrzucić. Administratorzy systemu powinni sprawdzić, czy ISP przeprowadza filtrowanie RFC 3704 w chmurze, zanim ruch wejdzie do systemu. Ponieważ lista bogonów zmienia się regularnie, w przypadku gdy dostawca usług internetowych nie przeprowadza filtrowania RFC 3704, administrator systemu musi zarządzać własnymi regułami bogon ACL lub przełączyć się na innego dostawcę usług internetowych.

Cisco IPS Filtrowanie reputacji źródłowego adresu IP

Usługi oceny reputacji pomagają określić, czy adres IP lub usługa jest źródłem zagrożenia. Cisco Global Correlation, nowa funkcja bezpieczeństwa Cisco IPS 7.0, wykorzystuje ogromną inteligencję bezpieczeństwa. Sieć Cisco SensorBase Network zawiera informacje o wszystkich znanych zagrożeniach w Internecie, takich jak botnety, epidemie złośliwego oprogramowania, ciemne sieci i zbieracze botnetów. Cisco IPS wykorzystuje tę sieć do filtrowania ruchu DoS, zanim uszkodzi on krytyczne zasoby. Aby jeszcze wcześniej wykrywać złośliwą aktywność i zapobiegać jej, włącza do swojego systemu dane o globalnych zagrożeniach.

Filtrowanie czarnych dziur

Filtrowanie czarnych dziur jest powszechną techniką obrony przed botnetami, a tym samym zapobiegania atakom DoS. Czarne dziury odnoszą się do węzłów sieci, w których ruch przychodzący

jest odrzucany lub porzucany bez poinformowania źródła, że dane nie dotarły do zamierzonego odbiorcy. Niepożądany ruch może zostać odrzucony, zanim dostanie się do chronionej sieci, za pomocą techniki zwanej zdalnie wyzwalanym filtrowaniem czarnej dziury (RTBH). Ponieważ jest to proces uruchamiany zdalnie, filtrowanie musi być przeprowadzone we współpracy z dostawcą usług internetowych. Wykorzystuje trasy hosta Border Gateway Protocol (BGP) do kierowania ruchu do serwerów ofiary do następnego przeskoku „nullO".

Oferty ochrony przed atakami DDoS oferowane przez dostawcę usług internetowych lub usługę DDoS
Ta metoda skutecznie zapobiega fałszowaniu adresów IP na poziomie usługodawcy internetowego. W tym przypadku dostawca usług internetowych oczyszcza/czyści ruch przed zezwoleniem mu na wprowadzenie łącza internetowego użytkownika. Ponieważ ta usługa działa w chmurze, ataki DDoS nie przeciążają łączy internetowych. Ponadto niektóre strony trzecie oferują usługi zapobiegania atakom DDoS w chmurze. IP Source Guard (w CISCO) lub podobne funkcje można włączyć w innych routerach w celu filtrowania ruchu w oparciu o bazę danych powiązań DHCP snooping lub powiązania źródła IP, które uniemożliwiają botom wysyłanie sfałszowanych pakietów.

Dodatkowe środki zaradcze DoS/DDoS

Wdrażanie mechanizmów obronnych w odpowiednich miejscach poprzez stosowanie odpowiednich środków pozwala na podniesienie bezpieczeństwa sieci organizacyjnej. Poniżej znajduje się lista środków zaradczych do zwalczania ataków DoS/DDoS:
Użyj silnych mechanizmów szyfrowania, takich jak WPA2 i AES 256 dla sieci szerokopasmowych, aby chronić się przed podsłuchem
Upewnij się, że oprogramowanie i protokoły są aktualne, i dokładnie przeskanuj maszyny, aby wykryć wszelkie nietypowe zachowania
Zaktualizuj jądro do najnowszej wersji i wyłącz nieużywane i niezabezpieczone usługi
Blokuj wszystkie pakiety przychodzące pochodzące z portów usługi, aby zablokować ruch z serwerów odbicia
Włącz ochronę plików cookie TCP SYN
Zapobiegaj transmisji oszukańczo adresowanych pakietów na poziomie ISP
Zaimplementuj radia kognitywne w warstwie fizycznej, aby poradzić sobie z atakami zagłuszania i szyfrowania
Skonfiguruj zaporę tak, aby odmawiała dostępu do ruchu zewnętrznego protokołu ICMP (Internet Control Message Protocol).
Bezpieczna zdalna administracja i testowanie łączności
Przeprowadź dokładną weryfikację danych wejściowych
Zapobiegaj używaniu niepotrzebnych funkcji, takich jak pobiera i strcpy
Zapobiegaj nadpisywaniu adresów zwrotnych
Korzystaj z zaawansowanych technologii nadzoru na poziomie sieci, aby monitorować granice sieci
Upewnij się, że połączenia częściowo dostępne są włączone z asertywnymi funkcjami limitu czasu
Zaimplementuj model serwera rozproszonego i usługi kolokacji jako model usługi tworzenia kopii zapasowych, aby zmniejszyć przeciążenie serwera podczas ataków DDoS
Upewnij się, że serwery są wolne od wąskich gardeł i punktów awarii
Korzystaj z usług ochrony innych firm, aby zapewnić zwiększone bezpieczeństwo przed wieloma poważnymi atakami DDoS
Używaj modeli wdrażania w wielu chmurach dla głównych aplikacji, aby zapewnić prawidłowe tworzenie kopii zapasowych podczas ataków DDoS na platformę chmurową
Przeprowadzaj obszerne symulacje ataków DoS/DDoS, aby uniknąć nagłych skoków i utrzymywać odpowiednią strategię przeciwdziałania przyszłym atakom

Ochrona DoS/DDoS na poziomie ISP

Jednym z najlepszych sposobów obrony przed atakami DoS jest blokowanie ich na bramie. To zadanie jest wykonywane przez zakontraktowanego ISP. Dostawcy usług internetowych oferują umowę dotyczącą poziomu usług „czystych rur", która zapewnia gwarantowaną przepustowość prawdziwego ruchu, a nie całkowitą przepustowość całego ruchu. Większość dostawców usług internetowych po

prostu blokuje wszystkie żądania podczas ataku DDoS, odmawiając dostępu do usługi nawet legalnemu ruchowi. Jeśli dostawca usług internetowych nie świadczy usług typu „clean-pipe", można skorzystać z usług subskrypcji oferowanych przez wielu dostawców usług w chmurze. Usługi abonamentowe pełnią rolę pośrednika, odbierają ruch kierowany do sieci, filtrują go, a następnie przekazują tylko zaufane połączenia. Dostawcy tacy jak Imperva i VeriSign oferują usługi ochrony chmury przed atakami DoS. Dostawcy usług internetowych oferują ochronę DDoS w chmurze dla łączy internetowych, aby uniknąć nasycenia z powodu ataku. Ten typ ochrony podczas ataku przekierowuje ruch związany z atakiem do dostawcy usług internetowych. Administratorzy mogą zażądać od dostawców usług internetowych zablokowania pierwotnego adresu IP, którego dotyczy problem, i przeniesienia witryny na inny adres IP po przeprowadzeniu propagacji DNS.

Włączanie TCP Intercept w oprogramowaniu Cisco IOS

Przechwytywanie TCP można włączyć, wykonując polecenia podane w poniższej tabeli w trybie konfiguracji globalnej.

Step	Command	Purpose
1	`access-list access-list-number {deny | permit} tcp any destination destination-wildcard`	Defines an IP extended access list
2	`ip tcp intercept list access-list-number`	Enables TCP intercept

Lista dostępu spełnia trzy cele:

1. Przechwytywanie wszystkich żądań
2. Przechwytywanie tylko żądań pochodzących z określonych sieci
3. Przechwytywanie tylko żądań kierowanych do określonych serwerów

Zazwyczaj lista dostępu definiuje źródło jako dowolne źródło, a miejsce docelowe jako określone sieci lub serwery. Ponieważ nie ma znaczenia, od kogo przechwytywać pakiety, adresy źródłowe nie są filtrowane. Zamiast tego identyfikowany jest docelowy serwer lub sieć, która ma być chroniona. Przechwytywanie TCP może działać w trybie aktywnego przechwytywania lub w trybie pasywnego nasłuchu. Domyślnym trybem jest tryb przechwytywania.

W aktywnym trybie przechwytywania oprogramowanie Cisco IOS aktywnie przechwytuje wszystkie przychodzące żądania połączeń (SYN) i odpowiada za pomocą SYN-ACK w imieniu serwera, po czym czeka na potwierdzenie (ACK) od klienta. Po otrzymaniu potwierdzenia ACK od klienta serwer wysyła oryginalny pakiet SYN, a oprogramowanie nawiązuje z serwerem trójstronny uścisk dłoni. Po zakończeniu trójstronnego uzgadniania dwie połówki połączeń są połączone. W trybie czuwania pasywnego użytkownik wysyła żądania połączenia, które przechodzą przez serwer, ale musi czekać, aż połączenie zostanie nawiązane. Jeśli żądanie połączenia nie zostanie ustanowione w ciągu 30 s, oprogramowanie wysyła żądanie zresetowania do serwera w celu wyczyszczenia jego stanu. Poniższa tabela przedstawia polecenie ustawienia trybu przechwytywania TCP w trybie konfiguracji globalnej.

Cel polecenia ip tryb przechwytywania tcp {przechwyt | watch} Ustaw tryb przechwytywania TCP

Zaawansowane urządzenia zabezpieczające przed atakami DDoS

Poniżej przedstawiono przykłady urządzeń zapewniających zaawansowaną ochronę przed atakami DDoSi.

FortiDDoS 200F, 1500E, 1500E-DC, 1500F, 2000E, 2000E-DC i VM04/08/16

FortiDDoS to masowo równoległa architektura uczenia maszynowego, która zapewnia najbardziej zaawansowaną ochronę przed atakami DDoS z najniższymi opóźnieniami, bez kompromisów w zakresie wydajności zwykle związanych z systemami opartymi na procesorach. FortiDDoS sprawdza zarówno przychodzące, jak i wychodzące pakiety warstwy 3, 4 i 7 do najmniejszych rozmiarów, co zapewnia najszybsze i najdokładniejsze wykrywanie i łagodzenie skutków.

Ochrona przed atakami DDoS

•Check Point DDoS Protector blokuje ataki DDoS dzięki wielowarstwowej ochronie. Jego zalety są wymienione w następujący sposób:

• Blokuje szeroką gamę ataków dzięki dostosowanej, wielowarstwowej ochronie
• Ochrona behawioralna obejmująca wiele elementów i blokująca nienormalny ruch
• Automatycznie generowane i predefiniowane podpisy
• Stosowanie zaawansowanych technik wyzwanie/odpowiedź
• Szybki czas reakcji w celu ochrony przed atakami w ciągu kilku sekund
• Automatycznie chroni przed zalewem sieci i atakami warstwy aplikacji
• Dostosowana ochrona zoptymalizowana pod kątem potrzeb bezpieczeństwa określonego środowiska sieciowego
• Szybko filtruje ruch, zanim dotrze on do zapory, aby chronić sieci i serwery oraz blokować exploity
• Elastyczne opcje wdrażania w celu ochrony każdej firmy
• Zintegrowany z Check Point Security Management

Terabitowy system ochrony DDoS

Terabit DDoS Protection System (DPS) to rozwiązanie do wykrywania i późniejszego leczenia ataków DDoS. Terabit DPS pomaga zapewnić maksymalną dostępność sieci i eliminuje wszelkie zakłócenia spowodowane atakami DoS/DDoS. Może być stosowany w dużych sieciach o przepustowości do 1Tbps. Może również zapewnić ochronę przepustowości do 6,4 Tb/s.

TPS A10 Thunder

A10 Thunder Threat Protection System (TPS) zapewnia niezawodny dostęp do kluczowych usług sieciowych poprzez wykrywanie i blokowanie zewnętrznych zagrożeń, takich jak DDoS i inne cyberataki, zanim przerodzą się one w kosztowne przerwy w świadczeniu usług. Jego funkcje są wymienione w następujący sposób:

o Utrzymanie dostępności usługi
o Pokonuj narastające ataki
o Skalowalna ochrona
o Zmniejsz bezpieczeństwo OpEx

Narzędzia ochrony DoS/DDoS

Strażnik Anty DDoS

Anti DDoS Guardian to narzędzie do ochrony przed atakami DDoS. Chroni serwery IIS, serwery Apache, serwery gier, serwery Camfrog, serwery pocztowe, serwery FTP, VOIP PBX, serwery SIP i inne podobne systemy. Anti DDoS Guardian monitoruje każdy pakiet przychodzący i wychodzący w czasie rzeczywistym. Wyświetla adres lokalny, adres zdalny i inne informacje o każdym przepływie w sieci. Anti DDoS Guardian ogranicza liczbę przepływów sieciowych, przepustowość klienta, liczbę jednoczesnych połączeń TCP klienta i szybkość połączenia TCP. Ogranicza również przepustowość UDP, szybkość połączenia UDP i szybkość pakietów UDP.

Poniżej przedstawiono przykłady innych narzędzi do ochrony przed atakami DDoS:

Ochrona przed atakami DDoS (https://www.innperyo.com)
Usługa ochrony DDoS firmy DOSarrest (https://www.dosorrest.com)
DDoS-GUARD (https://ddos-guord.net)
Cloudflare (https://www.doudflare.com)
Ochrona przed atakami F5 DDoS (https://www.f5.com)

Usługi ochrony DoS/DDoS

Ochrona przed atakami DDoS firmy Akamai

Akamai zapewnia ochronę przed atakami DDoS dla przedsiębiorstw, które regularnie są celem ataków DDoS. Poniżej wymieniono różne rozwiązania ochrony Akamai DDoS:

o Ochrona aplikacji i interfejsów API: natychmiast odrzucaj ataki DDoS w warstwie sieciowej. Reaguj na ataki w warstwie aplikacji w ciągu kilku sekund.

o Prolexic: Spójne stosowanie zasad ograniczania ataków DDoS, niezależnie od tego, gdzie hostowane są aplikacje.
o Web Application Protector: Automatycznie sprawdza żądania JSON i XML pod kątem złośliwych ładunków.
o Edge DNS: Polegaj na wysoce bezpiecznym systemie DNS zapewniającym nieprzerwaną dostępność aplikacji internetowych i interfejsów API.
Poniżej przedstawiono przykłady innych usług ochrony przed atakami DDoS:
Narzędzie Kaspersky DDoS Protection Tool (https://www.kospersky.com)
Stormwall PRO (https://stormwall.pro)
Ochrona Corero DDoS (https://www.corero.com)
Nexusguard (https://www.nexusguord.com)
BlockDoS (https://www.blockdos.net)

Podsumowanie modułu

W tym module omówiliśmy koncepcje związane z atakami typu „odmowa usługi" (DoS) i rozproszoną odmową usługi (DDoS). Omówiliśmy również koncepcje związane z botnetami wraz z ekosystemem botnetu. Ponadto zilustrowaliśmy różne narzędzia ataku DoS/DDoS, a także omówiliśmy różne typy ataków DoS/DDoS. Ponadto przedstawiono szczegółowe studium przypadku ataku DDoS na platformę Microsoft Azure. Zakończyliśmy szczegółową dyskusją na temat różnych środków zaradczych zapobiegających atakom DoS/DDoS, wraz z różnymi sprzętowymi i programowymi narzędziami do ochrony DoS/DDoS. W następnym module szczegółowo omówimy, w jaki sposób atakujący, a także etyczni hakerzy i testerzy pióra wykonują przejmowanie sesji w celu kradzieży prawidłowego identyfikatora sesji.