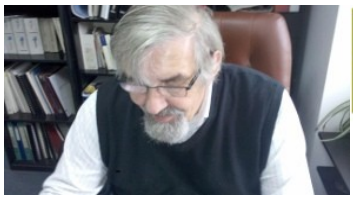


Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się, że mam coś ciekawego lub pożytecznego do napisania...

Numer 29/2012 28 maj 2012

Pozwolę sobie postawić następującą tezę:

Hacker jest przyjacielem administratora systemu i osób odpowiedzialnych za bezpieczeństwo danych.

Mam na myśli oczywiście prawdziwego hackera, a nie okazjonalnego „script kiddie" lub przestępcę czy bandytę komputerowego.

Prawdziwy hacker informuje zaatakowanego o tym, że został „zhakowany" oraz nie uszkadza atakowanego systemu.

Hacker jest więc obiektywnym testerem zabezpieczeń systemu, który swoje testy penetracyjne wykonuje nieodpłatnie. Działalność hackerów przyczyniła się niewątpliwie do wzrostu zainteresowania wprowadzaniem zabezpieczeń systemów komputerowych.

Przestępca (bandyta) komputerowy to pod wieloma względami przeciwieństwo hackera. **Przede wszystkim bandyta stara się ukryć ślady swego działania.** Motywy działania bandyty komputerowego są często „komercyjne" (chodzi o wykradzenie określonych danych lub uzyskanie dostępu do zastrzeżonych informacji) lub „osobiste" (zemsta zwolnionego pracownika na swej organizacji). O ile hacker stara się ukryć jedynie swoją tożsamość to bandycie zależy często na tym, aby jego działania pozostały niewykryte, lub aby zostały wykryte możliwie jak najpóźniej.

Administrator (lub inna osoba odpowiedzialna za zarządzanie bezpieczeństwem systemów teleinformatycznych) powinien więc dysponować skutecznymi narzędziami monitorującymi jego pracę. Regułą w centrach danych, a nawet w serwerowniach jest stosowanie zaawansowanych metod monitoringu fizycznego, który jest instalowany niezależnie od systemów kontroli dostępu.

Bandytom komputerowym pozostaje więc w zasadzie jedna droga ataku – sieć komputerowa. Współczesny bandyta komputerowy różni się znacznie od powszechnie kreowanego obrazu młodego człowieka ślęczącego w nocy nad klawiaturą komputera, który usiłuje odgadnąć hasła dostępu. Bandyci (i niestety niektórzy hackerzy) stosują o wiele bardziej wyrafinowane i zautomatyzowane metody. Monitorowanie takich działań wymaga również wykorzystywania bardziej zaawansowanych metod.

Spróbujmy się zastanowić, jakie warunki powinien spełniać skuteczny monitoring sieci komputerowej.

Po pierwsze - Monitoring powinien być ciągły.

Atak sieciowy może nastąpić w każdej chwili i może trwać przez dłuższy czas. Każdy klasyczny system monitorowania (np. za pomocą kamer) jest wyposażony w urządzenia umożliwiające zapis danych w celu ich późniejszego odtworzenia.

Podobną możliwość powinien zapewniać system monitoringu pracy sieci komputerowej. O tym, że nastąpił atak dowiadujemy się na ogół po fakcie. Im później – tym gorzej. Wspomniałem już o tym, że o ile prawdziwy hacker stara się pozostawić ślad swojego dostępu do systemu (np. zmienioną stronę WWW), a ukryć jedynie wykorzystywane metody to bandyta będzie starał się ukryć wszystkie ślady swej obecności. Szanse wykrycia ataku i określenia jego skutków „w czasie rzeczywistym" są praktycznie zerowe. Dopiero analiza pracy sieci na podstawie zapisu systemu monitorującego może dać nam kompletną informację o przebiegu i skutkach ataku.

Po drugie – Monitoring powinien być całkowicie niezależny od stosowanych systemów zabezpieczających.

Zasada ta, przyjmowania jako oczywistość przy projektowaniu systemów zabezpieczeń wartości materialnych dość trudno przebija się do świadomości osób odpowiedzialnych za bezpieczeństwo systemów teleinformatycznych. Zamek nie jest częścią systemu monitorowania – tak samo nie jest jego częścią router filtrujący, firewall czy szyfrator. Zadaniem systemu monitorowania jest obiektywny zapis zdarzeń (np. realizowanych transmisji sieciowych), a w konsekwencji także kontrola pracy i skuteczności stosowanych zabezpieczeń.

Po trzecie – Dane z monitoringu muszą być skutecznie zabezpieczone.

Dane zapisywane przez system monitoringu powinny być bezwzględnie dostępne jedynie osobom uprawnionym. Urządzenie monitorujące nie powinno w żaden sposób osiągalne z monitorowanej sieci i nie powinno w żaden sposób sygnalizować swej obecności w tej sieci. Interfejs sieciowy urządzenia monitorującego powinien jedynie odbierać dane (capture-only device). Większość współczesnych sieci komputerowych transmituje dane dwoma niezależnymi kanałami (Tx i Rx) w trybie Full Duplex – urządzenie monitorujące powinno odbierać i zapisywać dane z obu tych kanałów – powinno być więc wyposażone w co najmniej dwa porty sieciowe przystosowane jedynie do odbioru danych, które powinny być pobierane bezpośrednio z kabla sieciowego, a nie z portu urządzenia (które przecież może być zaatakowane!).

Komunikacja z urządzeniem monitorującym musi być realizowana przez niezależny, fizycznie zabezpieczony kanał transmisyjny.

Tylko przy spełnieniu tych warunków możemy mieć pewność, że zapisane dane odpowiadają rzeczywistym transmisjom sieciowym.

Po czwarte – wydajność urządzenia monitorującego musi zapewnić zapis wszystkich danych.

Odtworzenie przebiegu nawiązywania połączeń (lub ich prób) wymaga dysponowania zapisem obu kanałów komunikacyjnych. Ponieważ każdy kanał (Tx i Rx) może wykorzystać pełne pasmo sieci (np. 1 Gbps , 10 Gbps) urządzanie monitorujące musi zapewnić zapis z dwukrotnie większą prędkością – np. 2 Gbps lub 20 Gbps. Tylko w takim przypadku uzyskamy pewność, że żadne dane transmitowane siecią nie pozostały niezauważone przez system monitorujący.

Po piąte – rozdzielczość i znaczniki czasu.

Atakujący bandyta komputerowy będzie oczywiście maskować swe ślady wszelkimi metodami. Aby odtworzyć przebieg transmisji konieczne jest dysponowanie obiektywnymi oraz dokładnymi znacznikami czasowymi. Znaczniki te powinny być nadawane przez urządzenie monitorujące i zapewniać odpowiednią (zależną od prędkości sieci) rozdzielczość czasową. W przypadku sieci 10 Gbps i szybszych może być konieczna precyzyjna synchronizacja zewnętrzna (np. z systemu GPS).

Po szóste – czas zapisu.

Aby zapisać wszystkie transmisje realizowane przez sieć 1 Gbps w trybie Full Duplex w ciągu 1 godziny przy 100% obciążeniu sieci potrzebna jest pojemność pamięci 1 TB. Oczywiście przy typowych obciążeniach sieci pojemność ta będzie odpowiednio mniejsza. Przy typowym obciążeniu (30%) sieci 1 Gbps do całodobowego monitoringu wystarczy nam 8 TB pojemności dyskowej.

Jeśli mamy monitorować sieć szkieletową 10 Gbps wymagana pojemność zwiększy się dziesięciokrotnie, jednak w wielu przypadkach procentowe obciążenie takiej sieci nie przekracza 10-15%. Należy również wziąć pod uwagę, że przy całodobowym monitoringu do obliczenia niezbędnej pojemności powinniśmy przyjąć obciążenie średnie – a nie szczytowe. Nowoczesne systemy monitorujące obsługują pamięci dyskowe o pojemności nawet 5 PB (5000 TB), więc w praktyce ograniczenie czasu zapisu jest cena takiego urządzenia.

Po siódme – analiza zapisu.

System monitorowania nie jest wiele wart, jeśli nie sprawdza się wyników monitoringu. W przypadku monitorowania transmisji sieciowych mamy do czynienia z zapisem ogromnej ilości danych, których przeanalizowanie bez efektywnego oprogramowania jest po prostu niemożliwe. Niezbędne jest więc odpowiednie oprogramowanie, które będzie realizować filtrację zapisanych danych na możliwie najwyższym poziomie – z warstwami sesji, prezentacji i aplikacji modelu ISO/OSI włącznie.

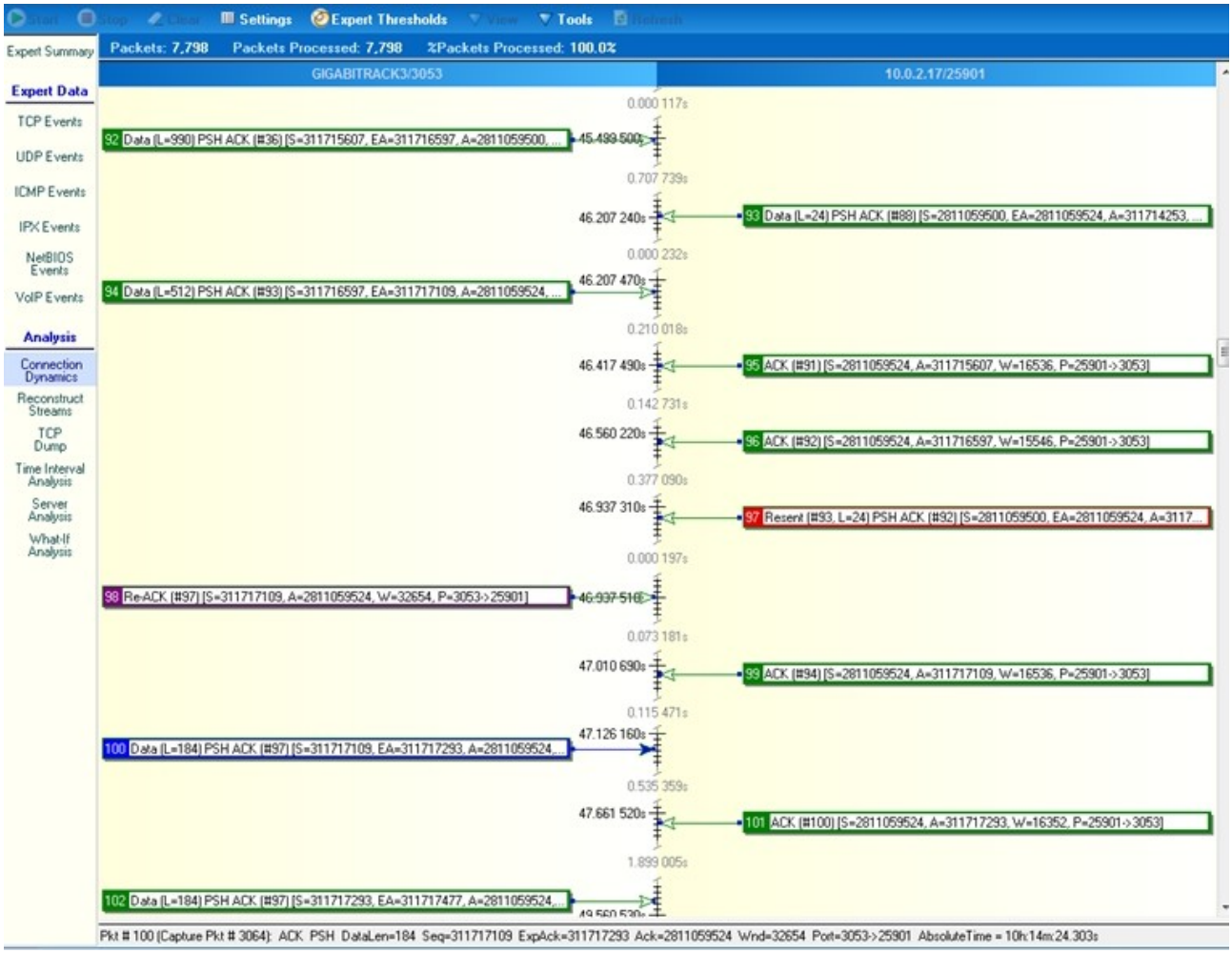
Zapis transmisji sieciowych umożliwia odtworzenie historii transmisji sieciowych, a w konsekwencji również sprawdzenie wydajności pracy programów użytkowych, opóźnień

odpowiedzi serwerów, procesu nawiązywania połączeń itp. Analiza tych danych umożliwia sprawdzenie rzeczywistego stanu sieci oraz pozwala na uzyskanie informacji o ewentualnych zakłóceniach, przyczynach opóźnień itp.

System monitoringu może udostępnić informacje zbiorcze (np. o pracy chmury obliczeniowej):

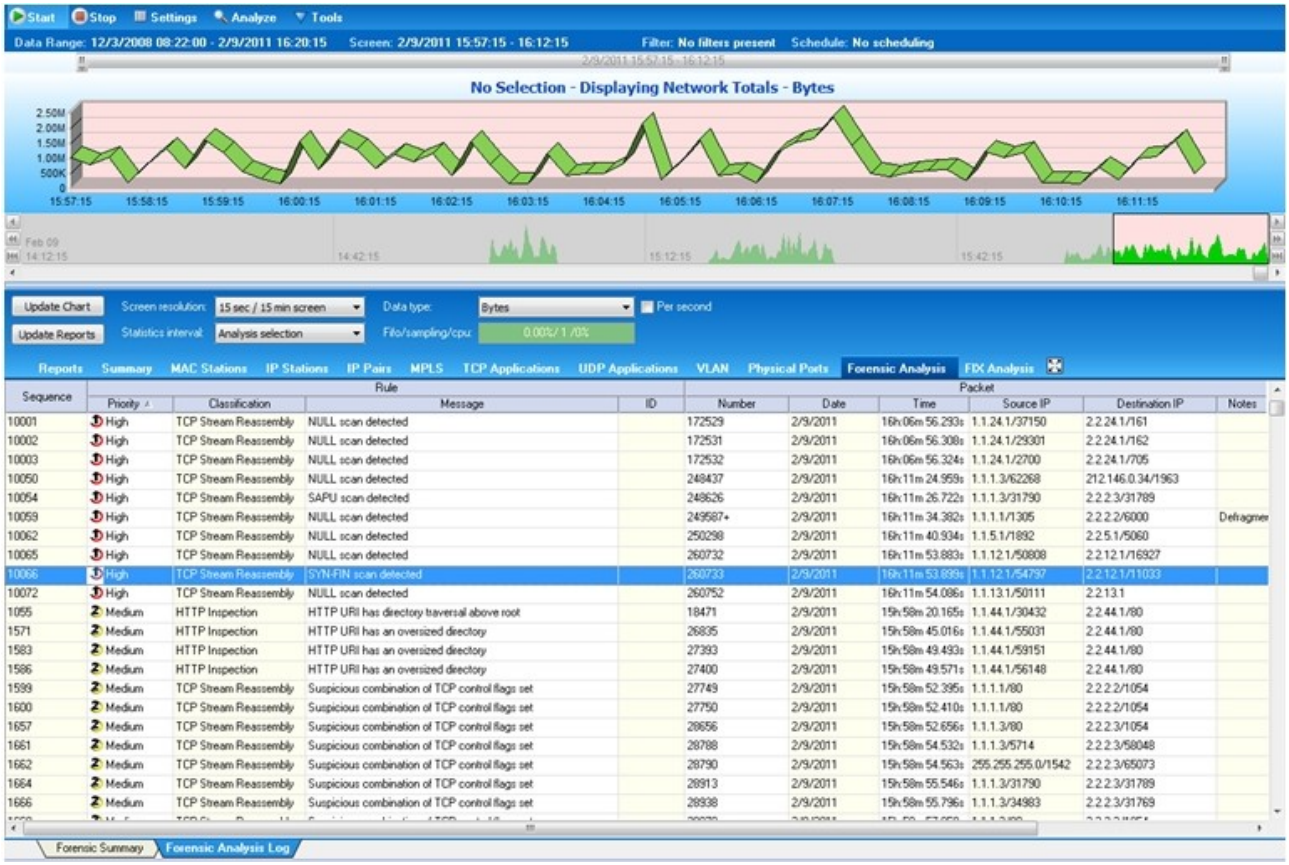
W razie potrzeby możemy przejść do bardziej szczegółowej analizy czasów odpowiedzi poszczególnych aplikacji:

Oprogramowanie analizujące dane umożliwia przechodzenie „od ogółu do szczegółu”. W przepadku stwierdzenia, że jakaś funkcja systemu nie osiąga wymaganych parametrów wydajnościowych możliwe jest szczegółowe prześledzenie dynamiki procesu nawiązywania połączenia oraz przebiegu transmisji danych.



Analiza zapisanych danych pozwala również na dokładne prześledzenie ewentualnych prób ataków sieciowych. Dane monitoringu zawierają informacje nie tylko o atakach zewnętrznych, lecz także o naruszeniach zasad bezpieczeństwa (celowych lub przypadkowych) dokonywanych przez użytkowników sieci lokalnej.

Program analizujący pozwala wykryć „dziwne" transmisje, próby uzyskania informacji o topologii sieci, zabezpieczeniach serwerów i strukturze oprogramowania itp. oraz wykrycie źródeł takiej aktywności.



Sequence	Rule				Packet					
	Priority	Classification	Message	ID	Number	Date	Time	Source IP	Destination IP	Notes
10001	High	TCP Stream Reassembly	NULL scan detected		172529	2/9/2011	16h:06m:56.293s	1.1.24.1/37150	2.2.24.1/161	
10002	High	TCP Stream Reassembly	NULL scan detected		172531	2/9/2011	16h:06m:56.308s	1.1.24.1/29301	2.2.24.1/162	
10003	High	TCP Stream Reassembly	NULL scan detected		172532	2/9/2011	16h:06m:56.324s	1.1.24.1/2700	2.2.24.1/705	
10050	High	TCP Stream Reassembly	NULL scan detected		248437	2/9/2011	16h:11m:24.959s	1.1.1.3/62268	212.146.0.34/1963	
10054	High	TCP Stream Reassembly	SAPU scan detected		248626	2/9/2011	16h:11m:26.722s	1.1.1.3/31790	2.2.2.3/31789	
10059	High	TCP Stream Reassembly	NULL scan detected		249587+	2/9/2011	16h:11m:34.382s	1.1.1.1/1305	2.2.2.2/6000	Defragmer
10062	High	TCP Stream Reassembly	NULL scan detected		250298	2/9/2011	16h:11m:40.934s	1.1.5.1/1892	2.2.5.1/5060	
10065	High	TCP Stream Reassembly	NULL scan detected		260732	2/9/2011	16h:11m:53.883s	1.1.12.1/50808	2.2.12.1/16927	
10066	High	TCP Stream Reassembly	SYN-FIN scan detected		260733	2/9/2011	16h:11m:53.899s	1.1.12.1/54797	2.2.12.1/11033	
10072	High	TCP Stream Reassembly	NULL scan detected		260752	2/9/2011	16h:11m:54.086s	1.1.13.1/50111	2.2.13.1	
1055	Medium	HTTP Inspection	HTTP URI has directory traversal above root		18471	2/9/2011	15h:58m:20.165s	1.1.44.1/30432	2.2.44.1/80	
1571	Medium	HTTP Inspection	HTTP URI has an oversized directory		26835	2/9/2011	15h:58m:45.016s	1.1.44.1/55031	2.2.44.1/80	
1583	Medium	HTTP Inspection	HTTP URI has an oversized directory		27393	2/9/2011	15h:58m:49.493s	1.1.44.1/59151	2.2.44.1/80	
1586	Medium	HTTP Inspection	HTTP URI has an oversized directory		27400	2/9/2011	15h:58m:49.571s	1.1.44.1/56148	2.2.44.1/80	
1599	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		27749	2/9/2011	15h:58m:52.395s	1.1.1.1/80	2.2.2.2/1054	
1600	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		27750	2/9/2011	15h:58m:52.410s	1.1.1.1/80	2.2.2.2/1054	
1657	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		28656	2/9/2011	15h:58m:52.656s	1.1.1.3/80	2.2.2.3/1054	
1661	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		28788	2/9/2011	15h:58m:54.532s	1.1.1.3/5714	2.2.2.3/58048	
1662	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		28790	2/9/2011	15h:58m:54.563s	255.255.255.0/1542	2.2.2.3/65073	
1664	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		28913	2/9/2011	15h:58m:55.546s	1.1.1.3/31790	2.2.2.3/31789	
1666	Medium	TCP Stream Reassembly	Suspicious combination of TCP control flags set		28938	2/9/2011	15h:58m:55.796s	1.1.1.3/34983	2.2.2.3/31769	

Podsumowanie:

Wymagania, które powinien spełniać profesjonalny system monitorowania pracy sieci komputerowej są wysokie. Konieczne są urządzenia (rozgałęźniki) do pobierania sygnału bezpośrednio z kabla sieciowego, specjalne karty sieciowe przystosowane jedynie do odbioru danych, wydajny system zapisu oraz oprogramowanie analizujące zapisane dane.

W większości przypadków wymaga to stosowania specjalizowanego sprzętu (appliance). Urządzenia te pełnią rolę próbników sieciowych z możliwością zapisu danych, do których dostęp jest możliwy z centralnej konsoli systemu. Dzięki temu możliwe jest monitorowanie nawet bardzo złożonej sieci oraz znajdywanie korelacji w przypadku skoordynowanych ataków.

Możliwość szczegółowego monitorowania sieci znacznie ułatwia również pracę centrów danych. Oto jedna z wielu opinii:

"Every time we initiate a particular site or application consolidation", explains Donnelly "we use the long-term views of traffic provided by GigaStor to establish performance baselines and validate application performance has not been impacted by the change."

Z przyjemnością udzielę PT Czytelnikom wszelkich dodatkowych informacji. Zapraszam również na naszą stronę poświęconą monitorowaniu sieci: www.aba.krakow.pl/NI