Od dłuższego czasu noszę się z napisaniem serii artykułów na temat Vulnerability Management'u. Przy tym zamierzam opisać dwa rozwiązania, którymi zajmuję się na co dzień.

Na początek warto powiedzieć kilka słów o producencie. Rapid7 jest firmą składającą się z doświadczonych inżynierów, których umiejętności pozwalają na tworzenie prostych, a zarazem innowacyjnych rozwiązań dla największych wyzwań związanych z bezpieczeństwem IT. Ich rozwiązania dotyczące zbierania, analizowania informacji związanych z zagrożeniami w środowisku pozwalają na wykrywanie naruszeń zasad bezpieczeństwa oraz podejmowanie działania w czasie rzeczywistym. Produkty firmy Rapid7 przyspieszają analizę danych, co skutkuje zmniejszeniem ilości czasu potrzebnego na zatrzymanie niepożądanych działań oraz oczyszczenie zainfekowanego środowiska. Dodatkowym wynikiem analizy przy pomocy oprogramowania Rapid7 są niezwykle szczegółowe dane, które z powodzeniem można wykorzystać do doskonalenia procesów bezpieczeństwa. Rapid7 w przeciwieństwie do tradycyjnej oceny podatności oraz tradycyjnego podejścia do zarządzania incydentami daje możliwość gromadzenia pełnych danych zarówno na temat atakującego, jak i samego ataku oraz możliwość przeprowadzenia analizy zebranych danych. Rapid7 oferuje niezrównane możliwości obrony przed atakami stanowiącymi największe zagrożenie. Firma ta posiada zdolność do pomocy klientowi nie tylko w zakresie dostarczenia innowacyjnych rozwiązań technologicznych ale również w rozwijaniu polityk bezpieczeństwa obowiązujących w organizacji. Produkty Rapid7 są idealnymi narzędziami, które pomogą dostosować mechanizmy bezpieczeństwa organizacji. Firmie Rapid7 zaufało już ponad 3500 organizacji z 78 krajów, w tym aż 30 procent znajdujących się na liście Fortune 1000.

Pomimo, iż wstęp dość mocno przypomina biuletyn handlowy, mogę powiedzieć, że piszę to z czystym sumieniem, ponieważ firma ta odkąd pracuje z ich produktami mnie nie zawiodła.

W czasach coraz częściej pojawiających się podatności o charakterze krytycznym takich jak ostatnim czasy opublikowane błędy w protokole SSL pozwalające na złamanie szyfrowanie i doprowadzenie do wycieku danych najważniejszy jest czas w jakim podatności zostaną wykryte i naprawione. Regularne aktualizacje zarówno baz podatności jak i samego oprogramowania jakie firma Rapid7 opracowuje dla swoich klientów, powodują, iż już w dniu publikacji informacji o istnieniu podatności oprogramowanie dostarczone przez Rapid7 jest w stanie zidentyfikować zagrożenie. Dodatkowym co otrzymuje

użytkownik, to dołączona do każdej informacji o zidentyfikowanej podatności jest kilkupunktowa informacja opracowana przez inżynierów Rapid7 zawierająca porady jakie kroki należy podjąć aby wyeliminować zagrożenie. Przy każdej wykrytej podatności, oprogramowanie skanujące poinformuje użytkownika czy na chwilę obecną jest dostępne złośliwe oprogramowanie wykorzystujące daną podatność, linki do referencji opisujących wykryty incydent oraz oszacowany przez oprogramowanie poziom ryzyka. Informacje te niezwykle ułatwiają oszacowanie realnego ryzyka dla infrastruktury.

Obecnie na rynku jest dostępnych wiele rozwiązań typu opensource oraz kilka rozwiązań komercyjnych. Niestety żadne z nich nie jest wystarczająco rozwinięte oraz wspierane przez wykwalifikowany zespół inżynierów. Porównując owe rozwiązania do rozwiązań stworzonych przez Rapid7 można zauważyć spore różnice w czasie aktualizacji co znacznie wpływa na poziom wiarygodności oraz skuteczności rozwiązań nie pochodzących od firmy Rapid7. Dużym minusem produktów innych niż Rapid7 jest fakt, iż żaden w 100% nie jest w stanie potwierdzić istnienia wykrytej podatności. Ponadto dowodem na wyższość rozwiązań z rodziny Rapid7 pod kątem identyfikacji i potwierdzenia jest fakt, iż nawet twórcy rozwiązań konkurencyjnych odwołują się do produktów Rapid7, które służą do potwierdzenia istnienia danej luki. Rapid7 jako jedyny wiodący producent oprogramowania identyfikującego podatności oferuje swoim klientom dokonania skanowania w dwóch różnych obszarach. Pierwszym obszarem jest standardowe skanowanie z zewnątrz danego hosta, czyli bez logowania się do systemu. Podczas standardowego skanowania zostaną ujawnione wszelakie podatności związane z zewnętrzną warstwą systemu taką jak na przykład firewall. Jednakże należy pamiętać, że zagrożenia występują nie tylko z zewnątrz sieci ale i wewnątrz. W takich przypadkach jedynie Rapid7 proponuje rozwiązanie integrujące się z prawie każdym systemem uwierzytelniania. Podczas procesu identyfikacji podatności przeprowadzonego z uwierzytelniane użytkownik uzyskuje symulacje działań potencjalnego intruza, który działa na uprawnieniach użytkownika organizacji. Takie podejście do identyfikacji podatności nie tylko od strony zewnętrznej ale i od wewnątrz środowiska cechuje się wysoka skutecznością w wczesnym wykrywaniu i zapobieganiu zagrożeniom.

Oprogramowaniem odpowiedzialnym za identyfikacje podatności dostępnym w szerokiej ofercie oprogramowania Rapid7 jest Nexpose, który jest oprogramowaniem skanującym mającym na celu zbadanie jakie usługi są udostępnione oraz jakie porty są otwarte na danym hoście (w przypadku skanowania z zewnątrz) lub zalogowanie się jako użytkownik do hosta i określenie podatności na podstawie informacji systemowych pozyskanych w miarę tego na ile pozwala uprawnienia na jakich została utworzona sesja. Nexpose dodatkowo do informacji o rodzaju i lokalizacji podatności dodaje linki do referencji wykrytych zagrożeń oraz w kilku prostych krokach opisuje jak zabezpieczyć się przed występowaniem tego typu zagrożeń.

Proces weryfikacji wykrytych podatności odbywa się za pomocą oprogramowania Metasploit. Podczas weryfikacji wykrytych błędów zostaje wykorzystana najaktualniejsza oraz największa na świecie baza exploitów, czyli oprogramowania pozwalającego na wykorzystanie istniejących podatności. Wymieniać jego opcje można dosyć długo, ale do najważniejszych i zarazem najciekawszych należą:

- Phishing Campaign, która pozwoli użytkownikowi na przygotowanie zaawansowanej kampanii phishingowej podczas której zostaną wysłane nie tylko maile z fałszywymi panelami logowania, ale również osoby, które wykonały instrukcje z maili mogą zostać przekierowane na dowolną stronę. Taka stroną, może być na przykład e-learning na temat bezpieczeństwa.
- Vulnerability Validation czyli potwierdzenie tego co zostało wykryte przez Nexpose. Za pomocą tej opcji zweryfikowane zostanie to ile faktycznych podatności jest na danym hoście i umożliwi wyeliminowanie błędy typu false positive.
- Web App Test opcja pozwalająca testować aplikacje webowe, nie tylko te najpopularniejsze.

- Quick PenTest opcja, która w kilku prostych krokach pozwala przygotować i wykonać pełny test sieci, każdy task można dowolnie skonfigurować i użyć wybranych przez siebie exploitów z bazy metasploita.

W 2013 roku firma Rapid7 po raz czwarty z rzędu otrzymała najwyższą ocenę w rankingu przeprowadzonym przez **Gartner.com** w kategorii Vulnerability Assessment co pokazuje, iż ilość włożonej pracy oraz zaangażowania nie tylko nie maleje, ale i rośnie co pozwala na to by firma utrzymała wysoką pozycje w rankingach a co za tym idzie wysoką jakość usług oferowanych swoim klientom.
Rozwiązania stworzone przez Rapid7 można uruchomić na dowolnej platformie systemowej. Dla oprogramowania Nexpose są to:

- Ubuntu Linux 12.04 LTS (ZALECANY)
- Ubuntu Linux 14.04 LTS
- Ubuntu Linux 10.04 LTS
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1+
- Red Hat Enterprise Linux Server 6.5 lub późniejszy
- Red Hat Enterprise Linux Server 5.10 lub późniejszy
- Wirtualne maszyny na VMware ESXi 5.x, VMware vCenter Server 5.x

Nexpose wspiera jedynie wersje systemu 64 bit.

Wymagania sprzętowe dla Nexpose:

- 2 GHz+ processor (zalecany procesor Dual-core)
- 8 GB RAM (zalecane 16 GB)
- 80 GB+ dostępnej przestrzeni dyskowej (10 GB dla Community Edition)
- 10 GB+ dostępnej przestrzeni dyskowej dla Silników Skanujących
- karta sieciowa 100 Mbps (zalecana 1 Gbps NIC)

Systemy wspierane przez oprogramowanie Metasploit:
• Windows Vista, Windows 7, Windows 8.x, Server 2003, Server 2008 oraz Server 2012 (zalecane 64 bit)
• Red Hat Enterprise Linux 5.x, 6.x (x86 orazx86_64)
• Ubuntu Linux 10.04, 12.04, 14.04 (x86 oraz x86_64)

Wymagania sprzętowe dla oprogramowania Metasploit:

- 2 GHz+ processor
- 2 GB RAM (zalecane 4 GB)
- 1 GB wolnaprzestrzeń dyskowa (zalecane 50 GB)

karta sieciowa 10/100 Mbps
Zarówno Nexpose jak i Metasploit bez problemu można zwirtualizować. Podstawowymi wymaganiami są adekwatna ilość wolnej przestrzeni dyskowej, która posłuży do przechowywania zebranych informacji na temat podatności oraz w przypadku oprogramowania Nexpose adekwatnej ilości pamięci RAM która jest wykorzystywana podczas procesów identyfikacji zagrożenia.

W następnych częściach tej serii, postaram się pokazać konfiguracje oraz użycie zarówno Nexpose jak i Metasploit.