tenable network security

PVS passive vulnerability scanner™

Skanowanie sieci w sposób ciągły pozwala wykryć nieautoryzowane urządzenia, podatności i niezaufane połączenia, z weryfikacją na poziomie transmisji pakietów włącznie.

Przegląd istotnych cech produktu

Tenable Passive Vulnerability Scanner™ (PVS™) to opatentowana technologia badania oraz analizy podatności, która pozwala na ciągłe, nieinwazyjne analizowanie sieci. PVS monitoruje protokoły IPv4, IPv6 oraz sieci mieszane na niskim poziomie, dzięki czemu jest w stanie określić ich topologię oraz wykryć aktywne serwisy i ich podatności. PVS może być wykorzystywany jako samodzielne narzędzie do efektywnego badania segmentów lub małych sieci lub jako integralna część rozwiązania Tenable SecurityCenter Continuous View™. PVS w czasie rzeczywistym wykrywa i śledzi użytkowników, aplikacje, infrastrukturę w chmurze, zaufane połączenia oraz podatności. Ponadto automatycznie wykrywa użytkowników, infrastrukturę oraz podatności systemów operacyjnych, urządzeń sieciowych, maszyn wirtualnych, baz danych, tabletów, telefonów, serwerów webowych, aplikacji w chmurze i infrastruktury o znaczeniu krytycznym.

Korzyści z używania PVS

Najważniejszymi korzyściami ze skanowania ruchu w sieci za pomocą PVS jest identyfikacja wszystkich urządzeń i aplikacji, rozpoznanie ich podatności i wykrycie urządzeń mobilnych:

- Zawsze wiadomo jakie urządzenia, aplikacje, serwisy i połączenia są lub były aktywne w sieci
- Ochrona systemów wrażliwych, czyli takich, które nie mogą być skanowane aktywnie
- Efektywne skanowanie bez konieczności logowania się do systemów wrażliwych,
  a co za tym idzie bez ryzyka spowodowania przerw w świadczeniu usług
- Automatyczne wykrywanie zagrożeń stwarzanych przez podatności w znanych zasobach, nowych systemach lub systemach niezaufanych
- Badanie zgodności zarówno z politykami wewnętrznymi, jak i z kluczowymi wymogami prawa poprzez weryfikację poprawności konfiguracji systemów
- Wykrywanie nadużyć i określanie wewnętrznych zagrożeń, które nie są wykrywalne na urządzeniach strzegących obrzeża sieci
- Skoncentrowanie na odpowiedziach na incydenty dzięki wzbudzaniu alarmów w wypadku wykrycia rzeczywistych zagrożeń
- Przyśpieszenie usuwania zagrożeń i eliminacja "martwych obszarów" pomiędzy skanami aktywnymi
- Wypełnienie luk w zaplanowanym aktywnym skanowaniu dzięki ciągłej analizie pasywnej

Tenable Passive Vulnerability Scanner pozwala na monitorowanie sieci w czasie rzeczywistym i jest przeznaczony do ciągłego skanowania i oceny poziomu bezpieczeństwa w organizacji w sposób nieinwazyjny. PVS badając wszystkie urządzenia śledzi ruch sieciowy na niskim poziomie, co gwarantuje wykrycie podatności serwerów i urządzeń.

PVS łatwo integruje się z siecią i wykrywa pasywnie aktywne urządzenia, w tym urządzenia wirtualne i znajdujące się w chmurze, urządzenia BYOD/mobilne, a nawet złamane (jailbroken) urządzenia z systemem iOS. PVS jest dostosowany do przyszłego zapotrzebowania na monitorowanie systemów wirtualnych, serwisów w chmurze i zwiększającej się liczby urządzeń.

Kluczowe funkcjonalności

Monitorowanie i wykrywanie podatności w czasie rzeczywistym

Tenable PVS w sposób ciągły monitoruje ruch sieciowy w celu uzyskania następujących informacji związanych z bezpieczeństwem:

- Śledzenie wszystkich podatności na aplikacjach klienckich i serwerowych
- Wykrywanie zmodyfikowanych lub skompromitowanych aplikacji
- Wykrywanie i zapamiętywanie nowych urządzeń w sieci
- Wykrywanie sytuacji wykonywania nieautoryzowanych skanów sieci przez maszyny znajdujące się wewnątrz niej
- Wychwytywanie interaktywnych oraz zaszyfrowanych sesji sieciowych
- Inwentaryzacja otwartych portów sieciowych w systemach oraz detekcja ruchu pomiędzy nimi
- Pasywne wykrywanie systemu operacyjnego dla każdego aktywnego w sieci urządzenia
- Wykrywanie podatności w systemach wraz z określeniem, które protokoły i aplikacje były wykorzystane
- Rangowanie urządzeń według odnalezionych podatności systemów operacyjnych i aplikacji oraz generowanych przez nie połączeń
- Wsparcie dla sieci o przepustowości 10Gbps

PVS łączy się z siecią poprzez hub, span port, łącze ERSPAN albo network tap i w sposób ciągły monitoruje potoki danych, generując ostrzeżenia w czasie rzeczywistym i sporządzając wszechstronne raporty dla działów bezpieczeństwa, IT i kadry zarządzającej.

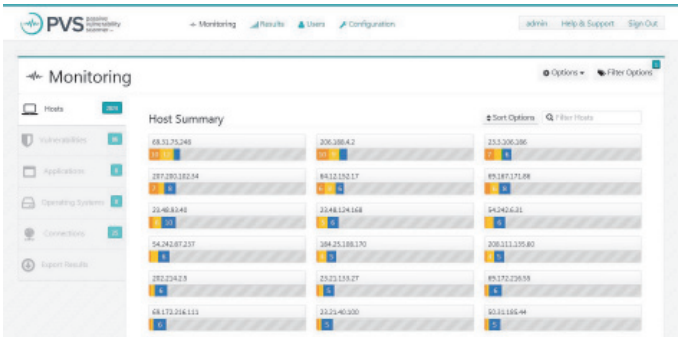
Monitorowanie sieci, WWW i FTP

PVS oferuje kompleksowe monitorowanie połączeń do sieci WWW lub FTP poprzez bezpośrednią analizę transferu pakietów. Pasywnie monitorując każde przesłanie danych poprzez HTTP lub FTP, PVS może określić i przedstawić informację o każdym urządzeniu w sieci, w tym:

- Wszystkie podatności i aplikacje zarówno po stronie klienta, jak i po stronie serwera WWW
- Listę wszystkich agentów WWW wykorzystanych na każdym urządzeniu
- Pasywne wyliczenie wszystkich plików udostępnianych przez FTP
- Zapisanie w czasie rzeczywistym logów wszystkich operacji GET, POST i pobranych plików
- Zapisanie w czasie rzeczywistym logów wszystkich plików przesyłanych przez GET, PUT lub protokołem FTP
- Zapisanie w czasie rzeczywistym logów zapytań do serwera DNS

Informacje takie są potrzebna do analizy aktywności wewnątrz sieci, aktywności pracowników, wykrywania infekcji złośliwym oprogramowaniem oraz zagrożeń zaawansowanych. Dzienniki detekcji mogą być wysłane do Tenable Log Correlation Engine™ w celu dalszej analizy, zbadania korelacji i archiwizacji.

Skanowanie bez konieczności instalacji agenta i dostęp bez instalacji klienta na urządzeniach końcowych



PVS oferuje zaawansowaną analizę protokołów SMB. Jeśli PVS jest wykorzystywany w sieci, w której funkcjonuje usługa Active Directory, to jest wówczas w stanie automatycznie uczyć się:

- Nazwy każdego urządzenia i każdej grupy roboczej
- Listy plików udostępnionych w dowolnym folderze
- Loginów i plików pobranych z sieci w czasie rzeczywistym

Możliwość pozyskania takiej informacji w czasie rzeczywistym pozwala na ocenę zaistniałej sytuacji i ma potężne znaczenie przy zbieraniu materiału dowodowego. W dużych sieciach pasywne określenie wszystkiego, co jest udostępniane w folderach, pozwala na o wiele łatwiejszą identyfikację ekspozycji potencjalnie wrażliwych danych. Stosowanie SecurityCenter Continuous View wraz z zintegrowanymi modulami PVS i Log Correlation Engine umożliwia analizę aktywności pracowników i złośliwego oprogramowania poprzez sprawdzenie informacji o udostępnionych przez sieć plikach.

Monitorowanie i zapisywanie logów baz danych SQL

PVS może przeglądać ruch sieciowy w celu identyfikacji baz danych SQL i ich podatności z jednoczesnym zapisywaniem logów tych działań w czasie rzeczywistym. Tak zapisywane logi zapytań SQL mogą być wysyłane do analizy do Log Correlation Engine, w celu archiwizacji oraz detekcji zagrożeń takich jak SQL injection ze strony serwerów WWW. Pełna obsługa środków kontrolowania wszystkich zdarzeń SQL może być osiągnięta zarówno poprzez połączenie danych z PVS z konfiguracją bazy danych SQL dla Nessus® i danymi audytu podatności, jak i poprzez logi zapisywane z serwera bazy danych SQL przez agenta Log Correlation Engine.

Pasywne wykrycie topologii i analiza identyfikacji serwisów

Analiza danych dla poszczególnych podatności klientów lub serwerów odbywa się poprzez rekonstruowanie zachowania po obydwu stronach połączenia sieciowego. Protokoły, takie jak HTTP, SMTP i FTP, mają specyficzne ciągi znaków, które pozwalają zidentyfikować wersję serwisu. PVS wyznacza wersje i kojarzy je ze specyficznymi wtyczkami i testami podatności.

Zgodność PCI DSS

Standard PCI DSS wymaga dokładnej i wszechstronnej identyfikacji wszystkich systemów zaangażowanych w transmisję, przetwarzanie oraz przechowanie danych kart kredytowych. Systemy te wspólnie stanowią “cardholder data environment” (CDE), które musi być corocznie weryfikowane na zgodność z wymogami PCI DSS. Organizacje powinny dodatkowo zapewniać dokumentowanie wypełnionych procedur w celu zwiększenia spójności danych CDE. PVS nie tylko monitoruje znane przepływy danych przez CDE, ale również identyfikuje działania nieudokumentowane, w szczególności informacje o niezaufanych płatnościach kartą.

Opcje wdrażania

The Tenable Passive Vulnerability Scanner jest dostępny w dwóch wersjach:standard (1 Gb/sek) i podwyższony (10 Gb/sek). Na każdym z tych poziomów PVS jest dostępny również jako samodzielny skaner i jako część SecurityCenter Continuous View. SecurityCenter Continuous View jest rozwiązaniem do zarządzania ryzykami bezpieczeństwa, w unikatowy sposób łączącym zdarzenia dot. bezpieczeństwa z aktywnym i pasywnym skanowaniem podatności.

tenable® network security

Więcej szczegółów na stronach tenable.com oraz openbiz.pl