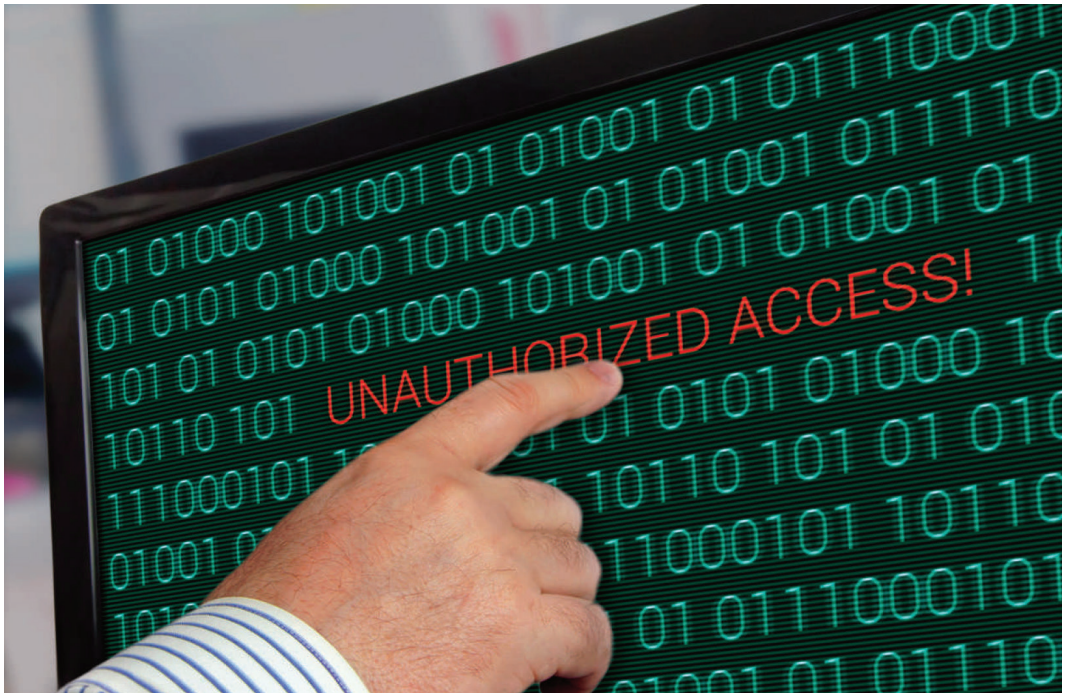
Core Impact

Testy penetracyjne, walidacja podatności i ryzyka

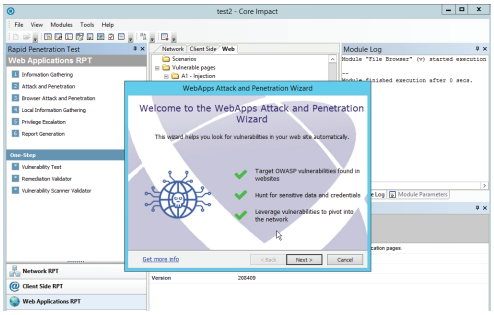


Core Impact jest narzędziem wspomagającym działy bezpieczeństwa w procesie weryfikacji i oceny skuteczności zastosowanych systemów zabezpieczeń. Umożliwia prowadzenie wielowymiarowych, profesjonalnych testów penetracyjnych, pozwalając bezpiecznie odtworzyć próby przełamania systemów ochrony. Dzięki integracji ze skanerami podatności weryfikuje, które z wykrytych podatności stanowią realne zagrożenie dla krytycznych zasobów organizacji. Tym samym działy bezpieczeństwa, kierownictwo firmy i osoby odpowiedzialne za politykę compliance uzyskują informacje, które pozwalają ustalić priorytety działań dla poszczególnych zespołów i zminimalizować ryzyko wymiernych strat.

Core Impact wskazuje m.in.:

- Które systemy są szczególnie narażone na atak, jeśli dojdzie do kompromitacji systemów ochrony brzegu sieci?
- Jakie luki w systemie operacyjnym i usługach stanowią rzeczywiste zagrożenia dla sieci?
- Czy i jak można podwyższyć uprawnienia w skompromitowanych systemach?
- Jakie informacje mogą stać się dostępne, zmienione lub skradzione?
- Jakie systemy są podatne na ataki typu „denial of service”?
- Które relacje zaufania między urządzeniami mogą zostać wykorzystane do lokalnych ataków na inne systemy?

Passus SA | Goraszewska 19, 02-910 Warszawa | tel. (+48) 695 444 803 | e-mail: passus@passus.com | www.passus.com



Intuicyjne wizardy ułatwiają przeprowadzenie testów exploitacyjnych na znalezione podatności według OWASP

Wielowymiarowe odtwarzanie złożonych zagrożeń

Core Impact to jedyne rozwiązanie, które umożliwia prowadzenie regularnych i powtarzalnych testów penetracyjnych z wykorztstaniem stale aktualizowanej bazy expoitów. Wykorzystując luki oraz najsłabiej zabezpieczone zasoby wskazuje możliwe wektory ataków na krytyczne urządzenia, aplikacje oraz dane organizacji.

Analiza „co jeśli" - (What-If Attack Analysis)

Wykazanie i udokumentowanie stopnia ryzyka poprzez odtworzenie sposobu, w jaki napastnik naraziłby na szwank systemy podatne na zagrożenia, wchodził z nimi w interakcję i do jakich danych uzyskałby dostęp.

Profesjonalnie przygotowane exploity

Core Impact zapewnia stale aktualizowaną aktualną bibliotekę exploitów, które można bezpiecznie stosować w środowisku produkcyjnym. Standardowo co miesiąc przygotowywanych jest co najmniej 10 nowych exploitów oraz innych aktualizacji dokładnie zweryfikowanych przez specjalistów i programistów CoreImpact.

Testy równoległe

Core Ipmact umożliwia równoczesne prowadzenie testów obejmujących różne obszary infrastruktury IT wielu zespołom. Zastosowane w programie rozwiązania pozwalają wygenerować jeden spójny obraz wszystkich wykrytych zagrożeń.

Raportowanie

Elastyczny system raportowy obejmuje:

- Zestawienie zweryfikowanych i potwierdzonych podatności co ułatwia zaplanowanie działań naprawczych.
- Metryki, które ilustrują skuteczność poszczególnych poziomów ochrony.
- Wyniki badań zgodności wprowadzonych zabezpieczeń z przepisami rządowymi i branżowymi.
- Walidację możliwych do przeprowadzenia działań naprawczych.

Testy penetracyjne sieci

- Gromadzenie informacji i budowa profilu sieci
- Przeprowadzenie ataków z wykorzystaniem zidentyfikowanych, krytycznych luk w systemach operacyjnych, urządzeniach, usługach i aplikacjach.
- Cykliczne próby uzyskania dostępu do danych i manipulowania nimi.
- Wstrzymanie i ponowienie ataku w celu weryfikacji parametrów SLA.
- Wykorzystanie skompromitowanych systemów do ataku na inne zasoby sieciowe z wykorzystaniem m.in. VPN, proxy oraz tunelowania.
- Weryfikacja przydatności poszczególnych zabezpieczeń w procesie rozpoznawania i blokowania ataków.
- Podszywanie się pod punkty dostępowe w celu uzyskania dostępu do urządzeń korzystających z WiFi.

Testy typu Client Side obejmujące użytkowników i urządzenia końcowe

- Wykorzystanie robotów, wyszukiwarek itp. do uzyskania przydatnych informacji o celu ataku.
- Przechwytywanie komunikacji (sniffing) między użytkownikami, a systemami docelowymi.
- Automatyczne oznaczenie użytkowników podatnych na ataki pihishingu na potrzeby ponownych testów.
- Gotowe szablony lub możliwość tworzenia wiadomości e-mail dla kampanii phishingowych.
- Expolity typu client-side do testowania zabezpieczeń urządzeń końcowych i oceny możliwości ich wykorzystania do ataków na zasoby informatyczne organizacji.
- Badanie świadomości użytkowników z wykorzystaniem różnych technik.

Ataki z wykorzystaniem kradzieży uwierzytelnień

- Próby przełamania zabezpieczeń Windows NTML w celu uzyskania haseł dostępu.
- Odczytywanie tożsamości: nazw użytkowników, haseł, ticketów/kluczy Kerberosa i kluczy SSH.
- Wykorzystanie tożsamości pozyskanych w ramach testów wielowectorowych.
- Wykorzystanie tożsamości Kerberosa do przeprowadzania ataków.
- Automatyczne lub ręczne (za pomocą kreatora szybkiego testu penetracyjnego), przejmowanie kontroli nad systemami korzystającymi ze słabych uwierzytelnień.
- Uzyskanie stałego dostępu do skompromitowanych systemów z wykorzystaniem kradzieży tożsamości.

Testy penetracji aplikacji internetowych

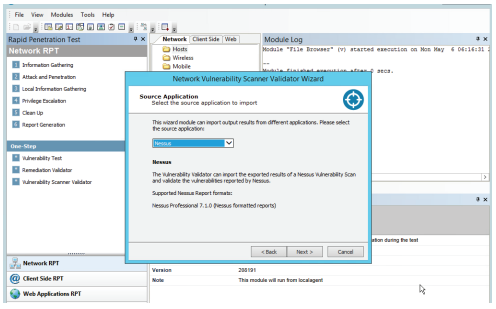
- Identyfikacja słabych punktów aplikacji internetowych, serwerów i związanych z nimi bazach danych bez żadnych błędów pierwszego rodzaju (ang. false-positive).
- Test wszystkich luk w aplikacjach internetowych wymienionych w OWASP Top Ten 2017.
- Dynamiczne generowanie exploitów, które mogą skompromitować aplikacje tworzone na indywidualne zamówienie.
- Importowanie i sprawdzanie poprawności wyników pracy skanerów podatności w celu określenia priorytetów dla działań naprawczych.
- Wykorzystanie najsłabiej zabezpieczonych zasobów do ataku na serwery webowe i rozwiązania back-end.
- Testowanie usług sieciowych aplikacji internetowych i mobilnych.

Testy penetracyjne urządzeń przenośnych

- Zidentyfikowanie krytycznych zagrożeń, których źródłem są urządzenia mobilne.
- Weryfikacja zabezpieczeń nowych urządzeń mobilnych i powiązanych z nimi usług sieciowych przed udzieleniem im dostępu.
- Test dostępności do listy połączeń, SMS, danych GPS i bazy kontaktów.
- Dedykowany agent dla urządzeń z systemem Android.

Ataki z wykorzystaniem kamer

- Identyfikacja hostów będących kamerą i testowanie ich podatności na ataki.
- Udokumentowanie podatności kamery na atak – możliwość rejestracji stopklatki z nagrania lub printscreenu z dostępu do interfejsu administracyjnego kamery.
- Prowadzenie testów manualnie lub z wykorzystaniem kreatora RPT.



Walidacja skanu podatności ze skanera Nessus.

Walidacja wyników podatności dostarczanych przez skanery:

Acunetix® Web Security Scanner
Portswigger BurpSuite Professional
Trustwave AppScan®
HP WebInspect
IBM Security AppScan®
Rapid7 AppSpider
Qualys Scanner
Beyond Security AVDS
GFI LANguardTM
IBM Enterprise Scanner® +
IBM Internet Scanner®
McAfee® Manager
Tenable Nessus®
Tenable.SC®
Tenable.IO®
Rapid7 Nexpose
Patchlink VMS
NMap
Qualys QualysGuard®
Skaner bezpieczeństwa sieci Retina
SAINTscanner®
TripWire IP360®
SAINTscanner®

Core Impact wskazuje, które z alarmów wygenerowanych przez skaner podatności wymagają uwagi. Wykazuje te, które mogą być wykorzystane poprzez exploity, ułatwiając nadawanie priorytetów zadaniom.

Grupa Passus specjalizuje się w projektowaniu i wdrażaniu wysoko specjalizowanych rozwiązań informatycznych z zakresu monitorowania i poprawy wydajności sieci i aplikacji oraz bezpieczeństwa IT zarówno w architekturze on-premise jak i środowiskach hybrydowych, chmurze prywatnej i publicznej. W skład Grupy wchodzą firmy Passus S.A., Wisenet sp. z o.o. oraz Chaos Gears sp. z o.o.

Oferta Grupy obejmuje:

- rozwiązania do monitorowania i rozwiązywania problemów z wydajnością sieci oraz aplikacji;
- rozwiązania z zakresu bezpieczeństwa IT w szczególności wykrywanie podatności, zabezpieczenie sieci, aplikacji oraz danych, systemy monitorowania i zarządzania incydentami bezpieczeństwa (SIEM/SOC/SOAR);
- projektowanie rozwiązań chmurowych, migracja aplikacji i danych do chmury oraz wsparcie w zarządzaniu i optymalizacja środowiskiem cloud;

Nasi Inżynierowie zrealizowali największe w Polsce projekty z zakresu Application and Network Performance Management oraz SIEM. **Ponad 20 lat współpracy z firmami oraz instytucjami z Polski i z zagranicy zaowocowało znajomością uwarunkowań biznesowych i technicznych tych organizacji.** Do grona Klientów w Polsce należą tak wymagający partnerzy, jak m.in. Ministerstwo Obrony Narodowej, T-Mobile, Narodowy Bank Polski, Grupa Enea, Centrum Onkologii w Gliwicach, Komisja Nadzoru Finansowego, Orange, PGE, Ikea, PKO BP, PZU, Volkswagen Polska, Politechnika Rzeszowska, Orlen, Grupa PKP SA, Wojskowy Instytut Medyczny.

Spółka zapewnia kompleksową obsługę, począwszy od analizy potrzeb, przez planowanie, usługi wdrożeniowe, rozwiązania na zamówienie, szkolenia pracowników, aż po opiekę serwisową oraz posprzedażną.

Grupa Passus jest partnerem firm Riverbed (Riverbed Premier Partner), Symantec (Gold Partner), IBM, Amazon Web Services, Fidelis Cybersecurity, Core Security, NetScout, New Relic, Cisco oraz Tenable. Passus posiada także własny zespół Research and Development. Na bazie zebranych doświadczeń zespół ten przygotował własne rozwiązania – zaawansowany sniffer sieciowy Passus Ambience oraz Passus FlowControl - system do monitorowania sieci w oparciu o protokół NetFlow.

Grupa zatrudnia blisko 60 wykwalifikowanych pracowników – inżynierów, programistów i specjalistów. **Potwierdzeniem kompetencji zespołu, obok wielu udanych wdrożeń, jest blisko 40 indywidualnych certyfikatów m.in.:** poświadczenie bezpieczeństwa osobowego do klauzuli „Tajne" oraz „NATO Secret", CISA, CISSP, Riverbed Certified Solutions Professional, Cisco Associate oraz Professional w zakresie R&S, Security oraz Wireless, Core Impact Certified Professional, Audytor wiodący ISO 27001, Riverbed NPM/AMP Qualified Trainer, IBM Certified Deployment Professional Security QRadar SIEM, ArcSight Certificate AS Data Platform Technical, Certified Ethical Hacker, Offensive Security Certified Professional. W 2017 roku firma spełniła wymagania stawiane przez Agencję Bezpieczeństwa Wewnętrznego i uzyskała świadectwa bezpieczeństwa przemysłowego, które potwierdzają zdolność spółki do realizacji usług w instytucjach i gałęziach przemysłowych związanych z dostępem do informacji niejawnych - krajowych jak i NATO oraz Unii Europejskiej.

Firma Passus SA powstała w wyniku wydzielenia Działu Sieci i Bezpieczeństwa IT z Passus sp. z o.o., działającej w branży IT od 1992 roku. Od lipca 2018 roku spółka notowana jest na rynku NewConnect.