Większość ludzi uważa, że hakerzy mają niezwykłe umiejętności i wiedzę, które pozwalają im włamać się do systemów komputerowych i znaleźć cenne informacje. Termin hacker przywołuje obrazy młodego informatyka, który wypisuje kilka poleceń na ekranie komputera - i puf! Komputer wypluwa hasła, numery kont lub inne poufne dane. W rzeczywistości dobry haker lub specjalista od zabezpieczeń, działający jako etyczny haker, musi po prostu zrozumieć, jak działa system komputerowy i wiedzieć, jakie narzędzia zastosować, aby znaleźć słabość bezpieczeństwa. Ten tekst nauczy Cię tych samych technik i narzędzi oprogramowania, których używa wielu hakerów do zbierania wartościowych danych i atakowania systemów komputerowych. Sfera hakerów i ich działanie jest nieznana większości specjalistów od komputerów i bezpieczeństwa. Hakerzy korzystają ze specjalistycznych narzędzi komputerowych w celu uzyskania dostępu do informacji. Ucząc się tych samych umiejętności i wykorzystując narzędzia wykorzystywane przez hakerów, będziesz w stanie bronić swoich sieci komputerowych i systemów przed złośliwymi atakami. Celem tej pierwszej części jest zapoznanie Cię ze światem hakera i zdefiniowanie terminologii używanej w omawianiu bezpieczeństwa komputerowego. Aby być w stanie bronić się przed złośliwymi hakerami, specjaliści od bezpieczeństwa muszą najpierw zrozumieć, w jaki sposób stosować etyczne techniki hakowania. W tekście tym szczegółowo opisano narzędzia i techniki stosowane przez hakerów, dzięki czemu można ich używać do identyfikowania potencjalnych zagrożeń w systemach. Poprowadzi Cię przez proces hakowania jako dobrego faceta. Większość etycznych hakerów prowadzi interesy hakerskie na rzecz zysku, w skrócie działalność zwaną testowaniem penetracyjnym lub testowaniem pióra. Testowanie pióra jest zwykle przeprowadzane przez specjalistę od zabezpieczeń w celu zidentyfikowania zagrożeń bezpieczeństwa i słabych punktów systemów i sieci. Celem identyfikacji zagrożeń i luk w zabezpieczeniach jest wprowadzenie środka zaradczego i ograniczenie ryzyka w pewnym stopniu. Etyczni hakerzy zajmują się hakerstwem i jako tacy muszą zachowywać się profesjonalnie. Ponadto przed użyciem oprogramowania i technik hakerskich należy dokładnie zapoznać się z prawem stanu, kraju lub prawa międzynarodowego. Przestrzeganie prawa jest koniecznością dla etycznego hakera. Etyczny hacker działa jako specjalista od zabezpieczeń podczas wykonywania testów pióra i musi zawsze działać w sposób profesjonalny.

Definiowanie etycznego hakowania

Następna sekcja wyjaśni cel hakowania etycznego i dokładnie to, co robią etyczni hakerzy. Jak wspomniano wcześniej, etyczni hakerzy muszą zawsze działać w sposób profesjonalny, aby odróżnić się od złośliwych hakerów. Uzyskanie zaufania klienta i podjęcie wszelkich środków ostrożności, aby nie uszkodzić ich systemów podczas testu pióra, ma kluczowe znaczenie dla bycia profesjonalistą. Innym kluczowym elementem etycznego hakowania jest uzyskanie pozwolenia właściciela danych przed uzyskaniem dostępu do systemu komputerowego. Jest to jeden ze sposobów, w jakie hakerzy etyczni mogą przezwyciężyć stereotyp hakerów i zdobyć zaufanie klientów. Cele, które hakerzy etyczni próbują osiągnąć w swoich próbach włamania, zostaną wyjaśnione również w tej sekcji.

Zrozumienie celu hakowania etycznego

Kiedy mówię ludziom, że jestem etycznym hackerem, zwykle słyszę chichotu i komentarze typu "To jest oksymoron". Wiele osób pyta: "Czy hakowanie może być etyczne?" Tak! To najlepiej opisuje, co robię jako ochroniarz. Używam tych samych narzędzi i technik, co złośliwi hakerzy, aby znaleźć słabość zabezpieczeń w sieciach komputerowych i systemach. Następnie stosuję niezbędną poprawkę lub poprawki, aby uniemożliwić złośliwemu hakerowi uzyskanie dostępu do danych. Jest to niekończący się cykl, ponieważ ciągle odkrywane są nowe słabości w systemach komputerowych, a dostawcy oprogramowania tworzą łaty, aby zmniejszyć ryzyko ataku. Etyczni hakerzy to zazwyczaj specjaliści od zabezpieczeń lub testerzy penetracji sieci, którzy wykorzystują swoje umiejętności hakerskie i zestawy narzędzi do celów obronnych i ochronnych. Etyczni hakerzy, którzy są specjalistami od zabezpieczeń,

testują bezpieczeństwo swoich sieci i systemów w poszukiwaniu luk w zabezpieczeniach przy użyciu tych samych narzędzi, których haker może użyć do naruszenia sieci. Każdy profesjonalista komputerowy może nauczyć się umiejętności hakerskich w zakresie etyki. Termin "cracker" opisuje hakera używającego umiejętności hakerskich i zestawu narzędzi do destrukcyjnych lub złośliwych celów, takich jak rozpowszechnianie wirusów lub wykonywanie ataków DoS (Denial-ofservice) w celu złamania zabezpieczeń lub zniszczenia systemów i sieci. Nie szukają już zabawy, hakerzy ci czasami płacą za zniszczenie reputacji firmy lub kradną lub ujawniają informacje o karcie kredytowej, jednocześnie spowalniając procesy biznesowe i naruszając integralność organizacji.

Inną nazwą **crackera** jest **złośliwy haker**.

Hakerów można podzielić na trzy grupy:

* Białe kapelusze : Dobrzy faceci, etyczni hakerzy

* Czarne kapelusze : źli faceci, złośliwi hakerzy

* Szare kapelusze : Dobry lub zły hacker; zależy od sytuacji

Etyczni hakerzy zwykle podpadają pod kategorię białych kapeluszy, ale czasami są tacy jak szare kapelusze, którzy stali się specjalistami od bezpieczeństwa i teraz wykorzystują swoje umiejętności w sposób etyczny.

Białe kapelusze

Białe kapelusze to dobrzy ludzie, etyczni hakerzy, którzy wykorzystują swoje umiejętności hakerskie w celach obronnych. Hakerzy białego kapelusza są zwykle specjalistami od zabezpieczeń z wiedzą o hakowaniu i zestawem narzędzi hakerów, którzy wykorzystują tę wiedzę, aby zlokalizować słabości i wdrożyć środki zaradcze. Hakerzy z białym kapeluszem to najlepsi kandydaci do egzaminu. Białe czapki to te, które włamują się za zgodą właściciela danych. Uzyskanie pozwolenia przed rozpoczęciem wszelkiej aktywności hakerskiej jest bardzo ważne. To właśnie sprawia, że ochroniarzem jest biały kapelusz, a nie złośliwy haker, któremu nie można ufać.

Czarne kapelusze

Czarne kapelusze to źli ludzie: złośliwi hakerzy lub crackerzy, którzy wykorzystują swoje umiejętności w nielegalnych lub złośliwych celach. Łamią lub w inny sposób naruszają integralność systemów zdalnych, ze złośliwymi zamiarami. Uzyskawszy nieautoryzowany dostęp, hakerzy w czarnych kapeluszach niszczą ważne dane, odmawiają legalnej obsługi użytkowników i powodują problemy z ich celami. Hackerów i crackerów w czarnych kapeluszch można łatwo odróżnić od białych hakerów, ponieważ ich działania są złośliwe. Jest to tradycyjna definicja hakera i to, co większość ludzi uważa za hakera.

Szare kapelusze

Szare kapelusze to hakerzy, którzy mogą pracować ofensywnie lub defensywnie, w zależności od sytuacji. To jest granica między hackerem a crackerem. Hackerzy szarego kapelusza mogą być zainteresowani hackowaniem narzędzi i technologii i nie są złośliwymi czarnymi kapeluszami. Szare kapelusze są samozwańczymi hakerami etycznymi, którzy interesują się narzędziami hakerskimi, głównie z punktu widzenia ciekawości. Mogą chcieć uwypuklić problemy związane z bezpieczeństwem w systemie lub edukować ofiary, aby odpowiednio zabezpieczyć swoje systemy. Ci hakerzy wyświadczają swoją "ofiarom" przysługę. Na przykład, jeśli wykryje się słabość w usłudze oferowanej przez bank inwestycyjny, haker robi bankowi przysługę, dając mu szansę na naprawienie luki. Z bardziej

kontrowersyjnego punktu widzenia niektórzy uważają, że samo włamanie się jest nieetyczne, jak złamanie i wejście. Ale przekonanie, że "etyczne" hakowanie wyklucza zniszczenie, przynajmniej łagodzi zachowania ludzi, którzy uważają się za "łagodnych" hakerów. Zgodnie z tym poglądem może to być jedna z najwyższych form "hackerskiej" uprzejmości, aby włamać się do systemu, a następnie wyjaśnić operatorowi systemu dokładnie, jak to się stało i jak można podłączyć dziurę; haker działa jako niezapłacony i niezamierzony zespół tygrysów (grupa, która przeprowadza audyty bezpieczeństwa na wynajem). Takie podejście przyciągnęło wielu etycznych hakerów w kłopotach prawnych. Upewnij się, że znasz prawo i swoje zobowiązania prawne, gdy angażujesz się w etyczne działania hakerskie. Wielu samozwańczych hakerów etycznych próbuje wejść na pole bezpieczeństwa jako konsultanci. Większość firm nie patrzy korzystnie na kogoś, kto pojawia się na ich progu z poufnymi danymi i oferuje "naprawę" dziur w zabezpieczeniach "za pewną cenę". Odpowiedzi obejmują zakres od "dziękuję za te informacje, naprawimy problem". wezwanie policji do aresztowania samozwańczego etycznego hakera. Różnica między białymi czapkami a szarymi kapeluszami jest tym słowem zezwolenia. Chociaż szare czapki mogą mieć dobre intencje, bez właściwego pozwolenia nie można ich już uznać za etyczne.

Teraz, gdy rozumiesz typy hakerów, spójrzmy, na to co robią hakerzy. To może wydawać się proste - włamują się do systemów komputerowych - ale czasami nie jest to takie proste raczej mgliste. Istnieje proces, który powinien być przestrzegany i informacje, które należy udokumentować. W następnej sekcji przyjrzymy się, co robią hakerzy i, co najważniejsze, etyczni hakerzy.

Co robią etyczni hakerzy?

Etyczni hakerzy są motywowani różnymi powodami, ale ich cel jest zwykle taki sam jak w przypadku crackerów: próbują ustalić, co intruz może zobaczyć w docelowej sieci lub systemie oraz co haker może zrobić z tymi informacjami. Ten proces testowania bezpieczeństwa systemu lub sieci nazywany jest testem penetracyjnym lub testem pen. Hakerzy włamują się do systemów komputerowych. W przeciwieństwie do powszechnego mitu, robienie tego zazwyczaj nie wiąże się z tajemniczym skokiem hackerskiego blasku, ale raczej uporczywością i zawziętym powtarzaniem garści dość dobrze znanych sztuczek, które wykorzystują wspólne słabości w bezpieczeństwie systemów docelowych. Test pióra to tylko wykonanie tych samych kroków przy użyciu tych samych narzędzi, których używa złośliwy haker, aby sprawdzić, jakie dane mogą zostać ujawnione za pomocą narzędzi i technik hakerskich. Wielu etycznych hakerów wykrywa złośliwą aktywność hakerów w ramach zespołu bezpieczeństwa organizacji, mającej za zadanie obronę przed złośliwymi działaniami hakerskimi. Zatrudniony etycznie haker pyta organizację, co ma być chronione, od kogo i jakie zasoby firma chce wydać, aby uzyskać ochronę. Plan badań penetracyjnych można następnie zbudować wokół danych, które wymagają ochrony i potencjalnych zagrożeń. Udokumentowanie wyników różnych testów ma kluczowe znaczenie dla uzyskania końcowego produktu testu pióra: raportu z testu pióra. Robienie zrzutów ekranu z potencjalnie cennymi informacjami lub zapisywanie plików dziennika ma kluczowe znaczenie dla przedstawienia wyników klientowi w raporcie z testu pióra. Raport z testu pióra jest kompilacją wszystkich potencjalnych zagrożeń w komputerze lub systemie.

Cele atakujących jakie próbują osiągnąć

Utrzymywane przez etycznego hakera lub złośliwego hakera wszystkie ataki są próbą złamania zabezpieczeń systemu komputerowego. Bezpieczeństwo składa się z czterech podstawowych elementów:

* Poufność

* Autentyczność

* Integralność

* Dostępność

Celem hakera jest wykorzystanie luk w systemie lub sieci w celu znalezienia słabości jednego lub więcej spośród czterech elementów bezpieczeństwa. Na przykład podczas wykonywania ataku DoS (Denial-of-Service) haker atakuje elementy dostępności systemów i sieci. Chociaż atak DoS może przybierać różne formy, głównym celem jest wykorzystanie zasobów systemowych lub przepustowości. Napływ komunikatów przychodzących do systemu docelowego zmusza go do wyłączenia, odmawiając w ten sposób obsługi legalnym użytkownikom systemu. Chociaż media skupiają się na celu ataków DoS, w rzeczywistości takie ataki mają wiele ofiar - ostateczny cel i systemy, które kontroluje intruz. Kradzież informacji, na przykład kradzież haseł lub innych danych podczas podróży w zaufanych sieciach, stanowi atak na poufność, ponieważ pozwala osobie innej niż zamierzony odbiorca uzyskać dostęp do danych. Ta kradzież nie jest ograniczona do danych na serwerach sieciowych. Laptopy, dyski i taśmy kopii zapasowych są zagrożone. Te urządzenia należące do firmy są obciążone poufnymi informacjami i mogą przekazać hakerom informacje o środkach bezpieczeństwa stosowanych w organizacji. Ataki typu "bit-flipping" są uznawane za ataki integralności, ponieważ dane mogły zostać naruszone podczas przesyłania lub odpoczynku w systemach komputerowych; w związku z tym administratorzy systemu nie są w stanie sprawdzić, czy dane są zgodne z zamierzeniem nadawcy. Lekki atak to atak w szyfrze kryptograficznym: atakujący zmienia tekst szyfrowania w taki sposób, aby doprowadzić do przewidywalnej zmiany zwykłego tekstu, chociaż atakujący nie uczy się samego zwykłego tekstu. Ten rodzaj ataku nie jest skierowany przeciwko szyfrowi, ale przeciwko wiadomości lub serii wiadomości. W skrajnym przypadku może to stać się atakiem DoS przeciwko wszystkim wiadomościom na określonym kanale za pomocą tego szyfru. Atak jest szczególnie niebezpieczny, gdy atakujący zna format wiadomości. W przypadku ataku bitowego na podpis cyfrowy, osoba atakująca może zmienić obietnicę z informacją "Zawdzięczam ci 10,00 $" w jednym stwierdzeniu na : "Jestem ci winien 10 000 $". Podszywanie się pod adres MAC jest atakiem uwierzytelniającym, ponieważ umożliwia nieautoryzowane logowanie urządzenia do łączenia się z siecią, gdy jest włączone filtrowanie Media Access Control (MAC), na przykład w sieci bezprzewodowej. Podszywając się pod adres MAC legalnej stacji bezprzewodowej, intruz może przyjąć tożsamość tej stacji i korzystać z sieci.

Zestaw umiejętności etycznego hakera

Etyczni hakerzy, którzy wyprzedzają złośliwych hakerów, muszą być ekspertami systemów komputerowych, którzy posiadają dużą wiedzę na temat programowania komputerów, sieci i systemów operacyjnych. Wymagana jest również dogłębna wiedza na temat wysoce ukierunkowanych platform (takich jak Windows, Unix i Linux). Cierpliwość, wytrwałość i ogromna wytrwałość są ważnymi cechami dla etycznych hakerów ze względu na długi czas i poziom koncentracji wymagany do spłacenia większości ataków. Praca w sieci, programowanie w Internecie i umiejętności baz danych są przydatne przy przeprowadzaniu etycznych testów hakerskich i testów podatności na ataki. Większość etycznych hakerów jest dobrze wyszkolona dzięki szerokiej wiedzy na temat komputerów i sieci. W niektórych przypadkach etyczny haker będzie działał jako część "zespołu tygrysów", który został zatrudniony do testowania sieci i systemów komputerowych i znajdowania luk. W takim przypadku każdy członek zespołu będzie miał odrębne specjalności, a etyczny haker może potrzebować bardziej wyspecjalizowanych umiejętności w jednym obszarze systemów komputerowych i sieci. Większość etycznych hakerów posiada wiedzę na temat obszarów bezpieczeństwa i pokrewnych zagadnień, ale niekoniecznie posiada silną kontrolę nad środkami zaradczymi, które mogą zapobiegać atakom.

Terminologia etycznego hakowania

Umiejętność zrozumienia i zdefiniowania terminologii jest ważną częścią pracy. Ta terminologia mówi o tym, jak komunikować się w dziedzinie bezpieczeństwa, jak działają jako etyczni hakerzy. Ten "język" hakowania jest niezbędny jako podstawa dalszych pojęć z późniejszych części. W tej sekcji omówimy kilka terminów, które należałoby poznać:

Zagrożenie Środowisko lub sytuacja, która może prowadzić do potencjalnego naruszenia bezpieczeństwa. Etyczni hakerzy szukają i ustalają priorytety zagrożeń podczas przeprowadzania analizy bezpieczeństwa. Szkodliwi hakerzy i ich użycie oprogramowania i technik hakerskich same w sobie stanowią zagrożenie dla bezpieczeństwa informacji w organizacji.

Exploit Oprogramowanie lub technologia wykorzystująca błąd, usterkę lub lukę w zabezpieczeniach, prowadząca do nieautoryzowanego dostępu, eskalacji uprawnień lub odmowy usługi w systemie komputerowym. Złośliwi hakerzy szukają exploitów w systemach komputerowych, aby otworzyć drzwi do pierwszego ataku. Większość exploitów to małe ciągi kodu komputerowego, które po uruchomieniu w systemie narażają na atak. Doświadczeni hakerzy tworzą własne exploity, ale nie jest konieczne posiadanie umiejętności programowania, aby być etycznym hakerem, ponieważ wiele programów hakerskich ma gotowe exploity, które można uruchomić przeciwko systemowi komputerowemu lub sieci. Exploit to zdefiniowany sposób na złamanie zabezpieczeń systemu informatycznego poprzez lukę w zabezpieczeniach.

Luka w zabezpieczeniach Istnienie luki w oprogramowaniu, projektu logiki lub błędu implementacji, które może doprowadzić do nieoczekiwanego i niepożądanego zdarzenia, powodującego nieprawidłowe lub szkodliwe instrukcje dla systemu. Kod exploita jest zapisywany w celu wykrycia luki i spowodowania błędu w systemie w celu pobrania cennych danych.

Cel oceny (TOE) System, program lub sieć, która jest przedmiotem analizy bezpieczeństwa lub ataku. Etyczni hakerzy zazwyczaj dotyczą wysokiej jakości TOE, systemów zawierających poufne informacje, takie jak numery kont, hasła, numery ubezpieczenia społecznego lub inne poufne dane. Celem etycznego hakera jest przetestowanie narzędzi hakerskich przeciwko wysokiej jakości TOE w celu określenia luk w zabezpieczeniach i ich łatania w celu ochrony przed exploitami i narażeniem wrażliwych danych.

Atak. Atak ma miejsce, gdy system zostanie zaatakowany w oparciu o lukę. Wiele ataków jest utrwalanych za pośrednictwem exploita. Etyczni hakerzy używają narzędzi do znajdowania systemów, które mogą być podatne na exploity z powodu systemu operacyjnego, konfiguracji sieci lub aplikacji zainstalowanych w systemach, a także w celu zapobiegania atakom.

Istnieją dwie podstawowe metody dostarczania exploitów do systemów komputerowych:

Zdalnie: Exploit jest wysyłany przez sieć i wykorzystuje luki w zabezpieczeniach bez wcześniejszego dostępu do systemu podatnego na ataki. Ataki hakerskie na korporacyjne systemy komputerowe lub sieci inicjowane ze świata zewnętrznego są uznawane za zdalne. Większość ludzi myśli o tego rodzaju ataku, gdy słyszy termin hacker, ale w rzeczywistości większość ataków znajduje się w następnej kategorii.

Lokalnie : Exploit jest dostarczany bezpośrednio do systemu komputerowego lub sieci, co wymaga wcześniejszego dostępu do podatnego na atak systemu w celu zwiększenia uprawnień. Polityki bezpieczeństwa informacji powinny być tworzone w taki sposób, aby dostęp do informacji mieli dostęp tylko ci, którzy mieliby dostęp do informacji i mieli najniższy poziom dostępu do pełnienia swojej funkcji. Pojęcia te są powszechnie nazywane "potrzebą poznania" i "najmniejszymi przywilejami", a gdy są właściwie stosowane, zapobiegną lokalnym exploitom. Większość prób włamań ma miejsce

wewnątrz organizacji i jest utrwalana przez pracowników, kontrahentów lub inne osoby na zaufanej pozycji. Aby osoba atakująca mogła rozpocząć atak, musi mieć wyższe przywileje niż to konieczne w oparciu o koncepcję "potrzeby poznania". Można to osiągnąć przez eskalację uprawnień lub słabe zabezpieczenia.

Fazy hakowania etycznego

Proces hackowania etycznego można podzielić na pięć różnych faz. Później w tym tekście hakowanie programów i narzędzi będzie podzielone na kategorie dla każdego z tych kroków. Etyczny haker podąża za procesami podobnymi do złośliwego hakera. Kroki mające na celu uzyskanie i utrzymanie dostępu do systemu komputerowego są podobne, niezależnie od intencji hakera.

Faza 1: Rozpoznanie pasywne i aktywne

Bierny rekonesans polega na zbieraniu informacji o potencjalnym celu bez wiedzy konkretnej osoby lub firmy. Pasywny rekonesans może być tak prosty, jak obserwowanie budynku, aby określić, kiedy pracownicy wchodzą do budynku i kiedy wychodzą. Jednak większość rekonesansu odbywa się siedząc przed komputerem. Gdy hakerzy szukają informacji na temat potencjalnego celu, zwykle przeprowadzają wyszukiwanie w Internecie na osobie lub firmie, aby uzyskać informacje. Jestem pewien, że wielu z was przeprowadziło takie samo przeszukanie pod własnym nazwiskiem lub potencjalnym pracodawcą, lub po prostu zebrali informacje na dany temat. Ten proces, gdy jest używany do zbierania informacji dotyczących TOE, jest ogólnie nazywany gromadzeniem informacji. Inżynieria społeczna i nurkowanie w śmietnikach są również uważane za pasywne metody gromadzenia informacji. Te dwie metody zostaną omówione bardziej szczegółowo w dalszej części. Sniffowanie sieci jest kolejnym sposobem biernego rozpoznania i może dostarczyć użytecznych informacji, takich jak zakresy adresów IP, konwencje nazewnictwa, ukryte serwery lub sieci oraz inne dostępne usługi w systemie lub sieci. Sniffowanie ruchu sieciowego jest podobne do monitorowania budynku: haker obserwuje przepływ danych, aby sprawdzić, kiedy mają miejsce określone transakcje i gdzie odbywa się ruch. Sniffowanie ruchu sieciowego jest powszechnym hakiem dla wielu etycznych hakerów. Po wykorzystaniu niektórych narzędzi hakerskich i wyświetleniu wszystkich danych przesyłanych w przejrzysty sposób przez sieci komunikacyjne są chętni do nauki i zobaczenia więcej. Narzędzia do sniffowania są proste i łatwe w użyciu, dostarczając wiele cennych informacji. Wiele razy obejmuje to nazwy użytkownika i hasła oraz inne poufne dane. Jest to zwykle bardzo atrakcyjne doświadczenie dla wielu administratorów sieci i specjalistów bezpieczeństwa i prowadzi do poważnych problemów związanych z bezpieczeństwem. Aktywny rekonesans polega na sondowaniu sieci w poszukiwaniu poszczególnych hostów, adresów IP i usług w sieci. Proces ten wiąże się z większym ryzykiem wykrycia niż bierny rekonesans i czasami jest nazywany *grzechotaniem klamkami*. Aktywny rekonesans może dać hakerowi informację o zastosowanych środkach bezpieczeństwa (czy drzwi wejściowe są zamknięte?), Ale proces ten zwiększa również szansę na złapanie lub przynajmniej podniesienie podejrzeń. Wiele narzędzi programowych wykonujących aktywny rekonesans można prześledzić z powrotem do komputera, na którym działają narzędzia, zwiększając w ten sposób szansę wykrycia hakera. Zarówno pasywny, jak i aktywny rekonesans może doprowadzić do odkrycia użytecznych informacji do wykorzystania w ataku. Na przykład zazwyczaj łatwo jest znaleźć typ serwera WWW i numer wersji systemu operacyjnego, z którego korzysta firma. Informacje te mogą umożliwić hakerowi znalezienie luki w tej wersji systemu operacyjnego i wykorzystać lukę w zabezpieczeniach w celu uzyskania większego dostępu.

Faza 2: Skanowanie

Skanowanie polega na pobraniu informacji odkrytych podczas zapoznania się z trasą i wykorzystaniu jej do zbadania sieci. Narzędzia, które haker może zastosować podczas fazy skanowania, obejmują

* Dialery

* Skanery Portów

* Skanery Internet Control Message Protocol (ICMP)

* Zakres Ping

* Odwzorowanie Sieci

* Zakres Simple Network Management Protocol (SNMP)

* Skanery podatności

Hakerzy szukają informacji, które pomogą im w ataku na cel, takie jak:

* Nazwy komputerów

* System operacyjny (OS)

* Zainstalowane oprogramowanie

* Adresy IP

* Konta użytkowników

Faza 3: Uzyskanie dostępu

Faza 3 ma miejsce, kiedy ma miejsce prawdziwe hakowanie. Luki ujawnione podczas fazy rozpoznania i skanowania są obecnie wykorzystywane do uzyskania dostępu do systemu docelowego. Atak hakerski może zostać dostarczony do systemu docelowego za pośrednictwem sieci lokalnej (LAN), przewodowej lub bezprzewodowej; lokalny dostęp do komputera, Internet, lub offline. Przykłady obejmują przepełnienie bufora w stosie, odmowę usługi i przejmowanie sesji. Tematy te zostaną omówione w dalszych rozdziałach. Uzyskanie dostępu jest znane w świecie hakerów jako posiadanie systemu, ponieważ gdy system został zhakowany, haker ma kontrolę i może używać tego systemu zgodnie z własnym życzeniem.

Faza 4: Utrzymanie dostępu

Gdy haker uzyska dostęp do systemu docelowego, chce zachować ten dostęp do przyszłej eksploatacji i ataków. Czasami hakerzy wzmacniają system przed hakerami lub pracownikami ochrony, zapewniając im wyłączny dostęp za pomocą backdoorów, rootkitów i trojanów. Po tym, jak haker zostanie właścicielem systemu, może użyć go jako bazy do przeprowadzenia dodatkowych ataków. W tym przypadku system będący jego własnością jest czasami nazywany systemem zombie.

Faza 5: Zakrywanie ścieżek

Gdy hakerzy uzyskają i utrzymają dostęp, zakrywają swoje ślady, aby uniknąć wykrycia przez personel bezpieczeństwa, aby nadal korzystać z posiadanego systemu, aby usunąć dowody włamania lub aby uniknąć działań prawnych. Hakerzy próbują usunąć wszystkie ślady ataku, takie jak pliki dziennika lub alarmy systemu wykrywania włamań (IDS). Przykłady działań w tej fazie ataku obejmują

* Steganografia

* Korzystanie z protokołu tunelowania

* Modyfikowanie plików dziennika

Identyfikacja typów technologii hakerskich

Istnieje wiele metod i narzędzi służących do lokalizowania luk w zabezpieczeniach, uruchamiania exploitów i narażania systemów. Po wykryciu luk w systemie, haker może wykorzystać tę lukę i zainstalować złośliwe oprogramowanie. Trojany, backdoory i rootkity to wszelkie formy złośliwego oprogramowania . Złośliwe oprogramowanie jest instalowane w zhakowanym systemie po wykorzystaniu luki w zabezpieczeniach. Przepełnienie bufora i iniekcja SQL to dwie inne metody uzyskiwania dostępu do systemów komputerowych. Przepełnienie bufora i iniekcja SQL są używane głównie przeciwko serwerom aplikacji, które zawierają bazy danych informacji. Większość narzędzi hakerskich wykorzystuje słabości w jednym z czterech następujących obszarów:

* Systemy operacyjne Wielu administratorów systemu instaluje systemy operacyjne z ustawieniami domyślnymi, co powoduje, że potencjalne luki w zabezpieczeniach pozostają niezałatwione.

* Aplikacje .Aplikacje zwykle nie są dokładnie testowane pod kątem luk w zabezpieczeniach, gdy programiści piszą kod, co może pozostawić wiele wad programistycznych, które może wykorzystać haker. Większość opracowań aplikacji jest "oparta na funkcjach", co oznacza, że programiści są w nieodległym terminie, aby w najkrótszym czasie stworzyć najbardziej niezawodną aplikację.

* Kod Shrink-Wrap Wiele gotowych programów posiada dodatkowe funkcje, których zwykły użytkownik nie zna, a te funkcje mogą być wykorzystane do wykorzystania systemu. Makra w programie Microsoft Word mogą na przykład pozwolić hakerowi na wykonywanie programów z poziomu aplikacji.

* Błędne konfiguracje Systemy mogą być również źle skonfigurowane lub pozostawione przy najniższych wspólnych ustawieniach bezpieczeństwa w celu zwiększenia łatwości użytkowania dla użytkownika; może to spowodować podatność na atak i atak.

Identyfikacja rodzajów etycznych metod

Etyczni hakerzy stosują wiele różnych metod w celu naruszenia bezpieczeństwa organizacji podczas symulowanego ataku lub testu penetracji. Większość etycznych hakerów ma specjalność w jednej lub kilku następujących metodach ataku. Podczas wstępnej dyskusji z klientem, jednym z pytań, które należy zadać, jest to, czy istnieją pewne szczególne obszary zainteresowania, takie jak sieci bezprzewodowe lub inżynieria społeczna. Dzięki temu haker etyczny może dostosować test do potrzeb klienta. W przeciwnym razie audyty bezpieczeństwa powinny obejmować próby dostępu do danych z wszystkich poniższych metod. Oto najczęstsze punkty wejścia do ataku:

Zdalna sieć .Zdalny hack sieciowy próbuje symulować intruza przeprowadzającego atak przez Internet. Etyczny haker próbuje złamać lub znaleźć lukę w zabezpieczeniach zewnętrznych sieci, takich jak luki w zabezpieczeniach zapory ogniowej, proxy lub routera. Internet jest uważany za najczęstszy pojazd hakerski, podczas gdy w rzeczywistości większość organizacji wzmocniła swoje mechanizmy obronne w stopniu wystarczającym, aby zapobiec włamaniom z sieci publicznej.

Zdalna sieć telefoniczna Zdalny hak sieciowy próbuje symulować intruza uruchomiającego atak na pule modemów klienta. War dialing numeru jest procesem powtarzalnego wybierania numeru w celu znalezienia otwartego systemu i jest przykładem takiego ataku. Wiele organizacji zastąpiło połączenia dial-in z dedykowanymi połączeniami internetowymi, więc ta metoda jest mniej istotna niż kiedyś.

Sieć lokalna Hack sieci lokalnej (LAN) symuluje osobę fizyczną uzyskującą dodatkowy nieautoryzowany dostęp za pośrednictwem sieci lokalnej. Etyczny haker musi uzyskać bezpośredni dostęp do lokalnej sieci, aby uruchomić ten rodzaj ataku. Bezprzewodowe sieci LAN (WLAN) należą do tej kategorii i

dodały całkowicie nową drogę ataku, gdy fale radiowe przemieszczają się przez struktury budynków. Ponieważ sygnał WLAN można zidentyfikować i przechwycić poza budynkiem, hakerzy nie muszą już uzyskiwać fizycznego dostępu do budynku i sieci w celu przeprowadzenia ataku w sieci LAN. Ponadto ogromny rozwój sieci WLAN sprawił, że stało się to coraz częstszym źródłem ataków i potencjalnego ryzyka dla wielu organizacji.

Skradziony sprzęt Skradziony sprzęt symuluje kradzież zasobów krytycznych informacji takich jak laptop należący do pracownika. Informacje takie jak nazwy użytkowników, hasła, ustawienia zabezpieczeń i typy szyfrowania można uzyskać, kradnąc laptopa. Zazwyczaj jest to często pomijany obszar przez wiele organizacji. Gdy haker uzyska dostęp do laptopa autoryzowanego w domenie bezpieczeństwa, można zebrać wiele informacji, takich jak konfiguracja zabezpieczeń. Laptopy często znikają i nie są raportowane wystarczająco szybko, aby umożliwić administratorowi bezpieczeństwa zablokowanie tego urządzenia poza siecią.

Inżynieria społeczna Atak socjotechniczny sprawdza bezpieczeństwo i integralność pracowników organizacji, wykorzystując telefon lub bezpośrednią komunikację w celu zebrania informacji do wykorzystania w ataku. Ataki socjotechniczne mogą służyć do pozyskiwania nazw użytkowników, haseł lub innych środków bezpieczeństwa organizacyjnego. Scenariusze socjotechniczne zazwyczaj składają się z hakera, który dzwoni do działu pomocy i rozmawia z pracownikiem działu pomocy technicznej o wydaniu poufnych informacji o bezpieczeństwie.

Wejście fizyczne Atak fizycznego wejścia próbuje zaatakować fizyczne pomieszczenia organizacji. Etyczny haker, który uzyskuje dostęp fizyczny, może wysyłać wirusy, trojany, rootkity lub sprzętowe rejestratory kluczy (fizyczne urządzenia używane do rejestrowania naciśnięć klawiszy) bezpośrednio w systemach w sieci docelowej. Ponadto, poufne dokumenty, które nie są przechowywane w bezpiecznym miejscu, mogą być gromadzone przez hakera. Wreszcie fizyczny dostęp do budynku pozwoliłby hakerowi na umieszczenie nieuczciwych urządzeń, takich jak bezprzewodowy punkt dostępowy w sieci. Urządzenia te mogłyby następnie zostać wykorzystane przez hakera do uzyskania dostępu do sieci LAN ze zdalnej lokalizacji.

Zrozumienie typów testowania

Podczas przeprowadzania testu bezpieczeństwa lub testu penetracji etyczny haker wykorzystuje jeden lub więcej typów testów w systemie. Każdy typ symuluje atakującego o różnych poziomach wiedzy na temat organizacji docelowej. Są to następujące typy:

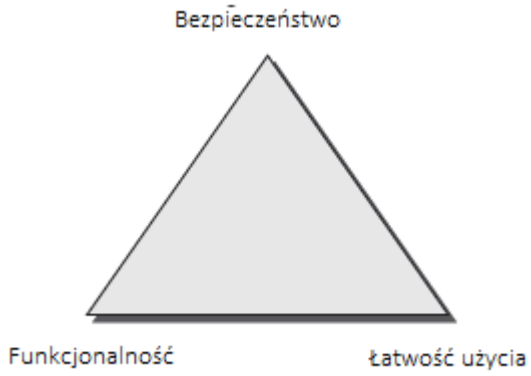
Black Box. Black Box polega na przeprowadzaniu oceny bezpieczeństwa i testowaniu bez wcześniejszej wiedzy o infrastrukturze sieci lub testowanym systemie. Testowanie symuluje atak złośliwego hakera poza obszarem ochrony organizacji. Testowanie Black-Box może trwać najdłużej i wymagać najwięcej wysiłku, ponieważ zespół testujący nie otrzymuje żadnych informacji. Dlatego też zbieranie informacji, rozpoznanie i skanowanie zajmie dużo czasu. Zaletą tego typu testów jest to, że najbardziej przypomina symulacje i wyniki prawdziwego złośliwego atakującego. Wady to przede wszystkim ilość czasu i związane z tym dodatkowe koszty ponoszone przez zespół testujący.

White Box Testowanie White-box polega na przeprowadzeniu oceny bezpieczeństwa i testowania przy pełnej znajomości infrastruktury sieciowej, takiej jak administrator sieci. Testowanie jest znacznie szybsze niż w przypadku pozostałych dwóch metod, ponieważ etyczny haker może przejść do fazy ataku, omijając wszystkie fazy zbierania informacji, rozpoznania i skanowania. Wiele audytów bezpieczeństwa składa się z testów w trybie "white-box", aby uniknąć dodatkowego czasu i kosztów testowania czarnej skrzynki.

Testowanie Gray Box Testowanie to polega na wewnętrznym przeprowadzaniu oceny bezpieczeństwa i testowania. Testowanie bada zakres dostępu osób wewnętrznych w sieci. Celem tego testu jest symulacja najbardziej rozpowszechnionej formy ataku, inicjowanej z sieci. Chodzi o to, aby sprawdzić lub sprawdzić poziom dostępu pracowników lub kontrahentów i sprawdzić, czy można przenieść te uprawnienia na wyższy poziom. Oprócz różnych typów technologii, z których może skorzystać haker, istnieją różne rodzaje ataków. Ataki można podzielić na pasywne lub aktywne. Ataki pasywne i aktywne są wykorzystywane zarówno w infrastrukturze bezpieczeństwa sieci, jak i na hostach. Aktywne ataki zmieniają system lub sieć, którą atakują, podczas gdy ataki pasywne próbują uzyskać informacje z systemu. Aktywne ataki wpływają na dostępność, integralność i autentyczność danych; ataki pasywne są naruszeniem poufności. Oprócz kategorii aktywnych i pasywnych ataki są klasyfikowane jako ataki lub ataki z zewnątrz. Atak pochodzący z obszaru ochrony organizacji jest atakiem wewnętrznym i zazwyczaj jest spowodowany przez "osobę z wewnątrz", która uzyskuje dostęp do większej ilości zasobów niż się spodziewano. Zewnętrzny atak pochodzi ze źródła znajdującego się poza granicami bezpieczeństwa, takiego jak Internet lub połączenie dostępu zdalnego.

Trójkąt bezpieczeństwa, funkcjonalności i łatwości użytkowania

Jako specjaliście ds. bezpieczeństwa trudno jest znaleźć równowagę między dodawaniem barier bezpieczeństwa, aby zapobiec atakowi i pozostawieniu systemu funkcjonalnego dla użytkowników. Trójkąt bezpieczeństwa, funkcjonalności i łatwości użytkowania jest odzwierciedleniem równowagi między bezpieczeństwem i funkcjonalnością a łatwością użytkowania systemu dla użytkowników



Ogólnie rzecz biorąc, wraz ze wzrostem bezpieczeństwa, funkcjonalnośći łatwość użytkowania systemu zmniejsza się dla użytkowników. W idealnym świecie specjaliści od bezpieczeństwa chcieliby mieć najwyższy poziom bezpieczeństwa na wszystkich systemach, jednak czasami nie jest to możliwe. Powstaje zbyt wiele barier bezpieczeństwa trudnych dla użytkowników korzystanie z systemu i utrudniających funkcjonalność systemu

<u>Użyteczność a bezpieczeństwo</u>

Załóżmy, że aby uzyskać wstęp do biura w pracy, musisz najpierw przejść przez punkt kontrolny przy wejściu na parking, aby zweryfikować numer tablicy rejestracyjnej, a następnie pokazać odznakę po wejściu do budynku, a następnie użyć kodu dostępu aby uzyskać dostęp do windy, a na koniec użyj klucza do odblokowania drzwi do biura. Możesz czuć, że kontrole bezpieczeństwa są zbyt surowe! Każda z tych kontroli może spowodować, że zostaniesz zatrzymany, a w konsekwencji przegapisz ważne spotkanie - na przykład, jeśli Twój samochód był w warsztacie i miałeś wynajęty samochód, lub zapomniałeś klucza lub plakietki dostępu do budynku, windy, lub drzwi do biura. Jest to przykład

napięcia między użytecznością a bezpieczeństwem. W wielu przypadkach, jeśli kontrole bezpieczeństwa są zbyt surowe, ludzie całkowicie je ominą. Na przykład ludzie mogą podpierać drzwi, aby mogli wrócić do budynku. Kiedy przeprowadzam audyt bezpieczeństwa fizycznego podczas testu penetracji, po prostu niosę pudełko w kierunku drzwi budynku, niezmiennie ludzie będą trzymać drzwi otwarte dla kogoś niosącego coś. Jest to po prostu ludzka natura i jest łatwym sposobem, aby haker pomijał środki bezpieczeństwa.

Narzędzia i badanie luk w zabezpieczeniach

Badanie narażenia na atak polega na wykrywaniu luk w zabezpieczeniach i projektowaniu,co może doprowadzić do ataku na system. Istnieje kilka witryn i narzędzi, które pomagają hakerom etycznym w utrzymywaniu aktualnej listy luk w zabezpieczeniach i możliwych exploitów przeciwko systemom lub sieciom. Niezwykle ważne jest, aby administratorzy systemu śledzili najnowsze wirusy, trojany i inne typowe exploity, aby odpowiednio chronić swoje systemy i sieć. Ponadto, zapoznając się z najnowszymi zagrożeniami, administrator może dowiedzieć się, jak wykryć, zapobiec i odzyskać po ataku. Badania podatności różnią się od hakerów etycznych, ponieważ badania te pasywnie szukają możliwych luk w zabezpieczeniach, podczas gdy hakerzy etyczni próbują zobaczyć, jakie informacje można zebrać. Jest podobny do intruza, który bada budynek i widzi okno na poziomie gruntu i myśli: "Cóż, może mógłbym użyć tego jako punktu wejścia." Etyczny haker przejdzie i spróbuje otworzyć okno, aby zobaczyć, czy jest odblokowane i zapewnić dostęp do budynku. Następnie rozejrzy się po pomieszczeniu, do którego wszedł przez budynek, by uzyskać cenne informacje. Każde wejście do systemu i dodatkowy poziom dostępu daje punkt oparcia dla dodatkowych exploitów lub ataków.

Raport etycznego hakowania

Wynikiem testu penetracji sieci lub audytu bezpieczeństwa jest hakerstwo etyczne lub raport z testu penetracji. Każda nazwa jest dopuszczalna i mogą być używane zamiennie. Ten raport zawiera szczegółowe informacje o wynikach działań hakerskich, rodzajach testów i zastosowanych metodach hakerskich. Wyniki są porównywane z oczekiwaniami wstępnie uzgodnionymi z klientem. Wszelkie zidentyfikowane luki są szczegółowe i sugerowane są środki zaradcze. Ten dokument jest zwykle dostarczany do organizacji w formacie papierowym, ze względów bezpieczeństwa. Szczegóły etycznego raportu hakerskiego muszą być poufne, ponieważ podkreślają zagrożenia bezpieczeństwa i podatności na zagrożenia w organizacji. Jeśli ten dokument wpadnie w niepowołane ręce, wyniki mogą być katastrofalne dla organizacji. Zasadniczo dałoby to komuś mapę drogową dla wszystkich słabości bezpieczeństwa organizacji.

Jak być etycznym

Haking etyczny jest zwykle przeprowadzany w uporządkowany i zorganizowany sposób, zwykle w ramach testu penetracyjnego lub audytu bezpieczeństwa. Głębokość i zakres systemów i aplikacji, które mają być testowane, zależy zwykle od potrzeb i problemów klienta. Wielu etycznych hakerów jest członkami zespołu tygrysów. Zespół tygrysa pracuje razem, aby przeprowadzić pełny test obejmujący wszystkie aspekty włamań sieciowych, fizycznych i systemowych. Etyczny haker musi przestrzegać pewnych zasad, aby zapewnić spełnienie wszystkich etycznych i moralnych zobowiązań. Etyczny haker musi wykonać następujące czynności:

* Uzyskać autoryzację od klienta i podpisaną umowę dającą testerowi uprawnienia do wykonania testu.

* Utrzymać i postępować zgodnie z umową o zachowaniu poufności (NDA) z klientem w przypadku poufnych informacji ujawnionych podczas testu.

* Zachować poufność podczas przeprowadzania testu. Zebrane informacje mogą zawierać poufne informacje. Żadna informacja o teście lub poufnych danych firmy nie powinna być nigdy ujawniana stronom trzecim.

* Wykonać test, ale nie przekraczając uzgodnionych limitów. Na przykład ataki DoS powinny być uruchamiane tylko w ramach testu, jeśli wcześniej zostały uzgodnione z klientem. Utrata przychodów, dobra wola i gorsze może spaść organizacji, której serwery lub aplikacje są niedostępne dla klientów w wyniku testów.

Poniższe kroki stanowią ramy do wykonania zabezpieczenia audyt organizacji i pomoże zapewnić, że test jest przeprowadzany w sposób zorganizowany, skuteczny i etyczny:

1. Porozmawiaj z klientem i omów potrzeby, które należy rozwiązać podczas testowania.

2. Przygotuj i podpisz dokumenty NDA u klienta.

3. Zorganizuj etyczny zespół hakerski i przygotuj harmonogram testów.

4. Przeprowadzić test.

5. Przeanalizuj wyniki testów i przygotuj raport.

6. Przedstaw raport ustaleń klientowi.

Przeprowadzanie testu penetracji

Wielu etycznych hakerów działających w roli specjalistów od bezpieczeństwa wykorzystuje swoje umiejętności do przeprowadzania ocen bezpieczeństwa lub testów penetracyjnych. Te testy i oceny mają trzy fazy, generalnie uporządkowane w następujący sposób:

Przygotowanie. Ta faza obejmuje formalne porozumienie między hackerem etycznym a organizacją. Ta umowa powinna zawierać pełny zakres testu, rodzaje ataków (wewnętrznych lub zewnętrznych), które należy zastosować, oraz typy testów: białe, czarne lub szare.

Przeprowadzenie oceny bezpieczeństwa. Na tym etapie przeprowadzane są testy, po których tester przygotowuje formalny raport dotyczący luk w zabezpieczeniach i innych ustaleń.

Wnioski. Wyniki zostały przedstawione organizacji na tym etapie wraz z zaleceniami dotyczącymi poprawy bezpieczeństwa.

Zauważ, że etyczny haker nie "naprawia" ani nie załatwia żadnych luk w zabezpieczeniach, które może znaleźć w ocenianym celu. Jest to powszechne błędne przekonanie o przeprowadzaniu audytów bezpieczeństwa lub testów penetracyjnych. Etyczny haker zwykle nie wykonuje żadnych łatek ani nie wdraża środków zaradczych. Ostatecznym celem lub dostarczeniem są w rzeczywistości wyniki testu i analiza związanego z nim ryzyka. Test jest tym, co prowadzi do ustaleń w raporcie końcowym i musi być dobrze udokumentowane. Wbrew powszechnemu przekonaniu, etyczni hakerzy wykonujący test penetracji muszą być bardzo zorganizowani i wydajni oraz muszą udokumentować każde odkrycie, wykonując zrzuty ekranu, kopiując wyniki narzędzia hakerskiego lub drukując ważne pliki dziennika. Etyczni hakerzy muszą być bardzo profesjonalni i przedstawiać dobrze udokumentowany raport, który należy traktować poważnie w swoim zawodzie.

Definiowanie haktywizmu

Haktywizm odnosi się do hakowania w sprawie. Ci hakerzy zwykle mają program społeczny lub polityczny. Ich intencją jest wysłanie wiadomości poprzez swoje działania hakerskie, jednocześnie uzyskując widoczność dla sprawy i dla siebie. Wielu z tych hakerów uczestniczy w takich działaniach, jak defragmentowanie stron internetowych, tworzenie wirusów i wdrażanie DoS lub innych destrukcyjnych ataków, aby uzyskać rozgłos dla swojej sprawy przyczyny. Haktywizm zwykle dotyczy agencji rządowych, grup politycznych i wszelkich innych podmiotów, które to grupy lub osoby postrzegane są jako "złe".

Utrzymanie się w mocy prawnej

Etyczny haker powinien znać kary nieautoryzowanego włamania się do systemu. Żadne etyczne działania hakerskie związane z testem penetracji sieci lub audytem bezpieczeństwa nie powinny się rozpocząć, dopóki podpisany dokument prawny potwierdzający, że haker etyczny wyraził zgodę na wykonywanie działań hakerskich, nie zostanie odebrany przez organizację docelową. Etyczni hakerzy muszą być rozsądni dzięki swoim umiejętnościom hakerskim i rozpoznawać konsekwencje nadużywania tych umiejętności.

Próba Hackowania

Witryna prowadzona przez maklerską firmę maklerską przechodzi atak hakerski. W wyniku ataku klienci firmy nie mogą przeprowadzać transakcji przez kilka godzin. W dniu ataku giełda jest niestabilna, a wielu klientów próbuje bezskutecznie kupować lub sprzedawać akcje. Klienci są bardzo nieszczęśliwi i obwiniają firmę za niepowodzenie w zapobieganiu, wykryciu i odzyskaniu sił po ataku. W tej sytuacji hakerzy są winni. Ale co z samą firmą maklerską? Klienci polegają na stronie internetowej firmy, aby dokonywać transakcji. Czy firma brokerska i jej dostawcy sieci są podatni na proces sądowy ze strony nieszczęśliwych klientów, którzy stracili pieniądze w wyniku zamknięcia? Czy firma brokerska ponosi jakąkolwiek odpowiedzialność, ponieważ nie była w stanie zapobiec zamknięciu systemu handlu opartego na stronie internetowej? Niektóre prawa omówione w tym rozdziale zajmą się kwestią odpowiedzialności po atakach hakerskich.

Przestępstwa komputerowe można ogólnie podzielić na dwie kategorie: przestępstwa popełniane przez komputer i przestępstwa, w których komputer jest celem. Najważniejsze prawa Stanów Zjednoczonych dotyczące przestępstw komputerowych opisano w poniższych sekcjach. Pamiętaj, że zamiar nie stawia hakera ponad prawem, nawet etyczny haker może być ścigany za łamanie tych praw.

Ustawa o wzmocnieniu bezpieczeństwa cybernetycznego i SPY ACT

Ustawa o wzmocnieniu bezpieczeństwa cybernetycznego z 2002 r. Nakazuje dożywocie dla hakerów, którzy "lekkomyślnie" zagrażają życiu innych. Szkodliwi hakerzy, którzy stwarzają zagrożenie dla życia poprzez atakowanie sieci komputerowych dla systemów transportowych, firm energetycznych lub innych usług publicznych lub mediów, mogą być ścigani zgodnie z tym prawem. Securely Protect Yourself Against Cyber Trespass Act (SPY ACT) z 2007 roku przy użyciu programów szpiegujących w systemach komputerowych zasadniczo zabrania:

* Zdalne sterowanie komputerem, gdy nie jesteś do tego upoważniony

* Używanie komputera do wysyłania niechcianych informacji do ludzi (powszechnie znanych jako spamowanie)

* Przekierowanie przeglądarki internetowej do innej witryny, która nie jest autoryzowana przez użytkownika

* Wyświetlanie reklam powodujących zamknięcie przeglądarki (okna podręczne)

* Zbieranie danych osobowych za pomocą rejestrowania naciśnięć klawiszy

* Zmiana domyślnej strony internetowej przeglądarki internetowej

* Użytkownicy wprowadzający w błąd, dlatego klikają łącze do strony internetowej lub powtarzają podobną stronę internetową w celu wprowadzenia użytkownika w błąd

SPY ACT jest ważny, ponieważ zaczyna rozpoznawać denerwujące pop-up'y i spam jako coś więcej niż zwykłe irytacje i prawdziwe próby hakowania. SPY ACT stanowi podstawę do ścigania hakerów wykorzystujących spam, pop-upy i linki w wiadomościach e-mail.

18 USC §1029 i 1030

Kodeks Stanów Zjednoczonych klasyfikuje i definiuje prawa Stanów Zjednoczonych według tytułów. Tytuł 18 zawiera szczegółowe informacje na temat "Zbrodni i procedury karnej". Sekcja 1029, "Oszustwo i powiązana działalność w związku z urządzeniami dostępowymi", stwierdza, że jeśli produkujesz, sprzedajesz lub używasz podrobionych urządzeń dostępu lub instrumentów telekomunikacyjnych w celu popełnienia oszustwa i uzyskania usług lub produkty o wartości powyżej 1000 USD, złamałeś prawo. Sekcja 1029 kryminalizuje niewłaściwe użycie haseł komputerowych i innych urządzeń dostępu, takich jak karty tokenów. Sekcja 1030, "Oszustwo i związana z nim działalność w związku z komputerami", zabrania dostępu do chronionych komputerów bez pozwolenia i powodując szkody. Ustawa ta kryminalizuje rozprzestrzenianie się wirusów i robaków oraz włamywanie się do systemów komputerowych przez osoby nieuprawnione.

Przepisy Stanów Zjednoczonych

Oprócz przepisów federalnych, wiele stanów ma swoje własne prawa związane z hakowaniem i audytowaniem sieci komputerowych i systemów. Wykonując testy penetracyjne, przejrzyj obowiązujące przepisy prawa stanowego, aby upewnić się, że pozostajesz po właściwej stronie prawa. W wielu przypadkach podpisana umowa testowa i NDA będą wystarczające, jeśli chodzi o cel i charakter testów. Instytut Bezpieczeństwa Narodowego ma stronę internetową zawierającą listę wszystkich przepisów państwowych mających zastosowanie do przestępstw komputerowych. Adres URL to http://nsi.org/Library/Compsec/computerlaw/statelaws.html

Federal Managers Financial Integrity Act

Ustawa Federal Managers Financial Integrity Act z 1982 r. (FMFIA) jest zasadniczo aktem odpowiedzialności, aby zapewnić, że osoby zarządzające rachunkami finansowymi robią to z najwyższą odpowiedzialnością i zapewniają ochronę aktywów. Opis ten można interpretować jako obejmujący wszelkie mierzalne zabezpieczenia w celu ochrony zasobów przed próbą włamania. Akt zasadniczo zapewnia,że :

* Fundusze, nieruchomości i inne aktywa są zabezpieczone przed marnotrawstwem, utratą, nieuprawnionym użyciem lub sprzeniewierzeniem.

* Koszty są zgodne z obowiązującymi przepisami.

FMFIA jest ważna dla etycznego hakowania, ponieważ nakłada na organizację odpowiedzialność za właściwe wykorzystanie funduszy i innych aktywów. W związku z tym prawo to wymaga od kierownictwa odpowiedzialności za bezpieczeństwo organizacji i zapewnienia odpowiednich zabezpieczeń przed atakami hakerskimi.

Ustawa o wolności informacji (FOIA)

Ustawa o wolności informacji (5 USC 552), lub FOIA, udostępnia wiele informacji i dokumentów o organizacjach publicznych. Większość zapisów i dokumentów rządowych można uzyskać za pośrednictwem FOIA. Każda informacja zebrana za pomocą tego aktu jest uczciwa, gdy przeprowadzasz rekonesans i zbierasz informacje o potencjalnym celu.

Federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA)

Federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) zasadniczo daje etycznym hakerom uprawnienia do wykonywania typów testów, które wykonują, i czyni je obowiązkowym wymogiem dla agencji rządowych. FISMA wymaga, aby każda federalna agencja opracowywała, dokumentowała i wdrażała program bezpieczeństwa informacji obejmujący całą agencję w celu zapewnienia bezpieczeństwa informacji dla systemów informacji i informacji, które wspierają operacje i aktywa agencji, w tym te dostarczane lub zarządzane przez inną agencję, wykonawcę lub inne źródło. Program bezpieczeństwa informacji musi obejmować:

* Okresowe oceny ryzyka i wielkości szkody, która może wynikać z nieuprawnionego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia systemów informacji i informacji, które wspierają operacje i aktywa agencji

* Zasady i procedury opierające się na ocenach ryzyka, opłacalnie zmniejszają ryzyko bezpieczeństwa informacji do akceptowalnego poziomu i zapewniają, że bezpieczeństwo informacji jest rozwiązywane w całym cyklu życia każdego systemu informacji agencji

* Plany podrzędne zapewniające odpowiednie bezpieczeństwo informacji w odniesieniu do sieci, obiektów, systemów informatycznych lub grup systemów informacyjnych, stosownie do przypadku

* Szkolenie w zakresie świadomości bezpieczeństwa mające na celu informowanie personelu (w tym wykonawców i innych użytkowników systemów informatycznych, które wspierają operacje i aktywa agencji) o zagrożeniach bezpieczeństwa informacji związanych z ich działaniami i ich obowiązkami w zakresie przestrzegania zasad i procedur agencji opracowanych w celu ograniczenia tych zagrożeń

* Okresowe testowanie i ocena skuteczności polityk, procedur i praktyk związanych z bezpieczeństwem informacji (w tym zarządzanie, kontrola operacyjna i techniczna każdego agencyjnego systemu informatycznego określonego w ich wykazie) z częstotliwością zależną od ryzyka, ale nie rzadziej niż raz w roku

* Proces planowania, wdrażania, oceny i dokumentowania działań zaradczych w celu wyeliminowania wszelkich braków w polityce bezpieczeństwa informacji, procedurach i praktykach agencji

* Procedury dotyczące wykrywania, zgłaszania i reagowania na incydenty związane z bezpieczeństwem (w tym łagodzenia ryzyka związanego z takimi incydentami przed dokonaniem istotnych szkód oraz powiadamiania i konsultowania się z federalnym centrum reagowania na incydenty bezpieczeństwa informacji oraz, w stosownych przypadkach, organami ścigania, odpowiednimi urzędami inspektora Ogólne i wszelkie inne agencje lub biura, zgodnie z prawem lub zgodnie z zaleceniami Prezydenta

* Plany i procedury zapewniające ciągłość operacji dla systemów informatycznych wspierających operacje i aktywa agencji

Gwarantuje to bezpieczeństwo pracy etycznym hakerom w białym kapeluszu, aby wykonywać nieustannie audyty bezpieczeństwa agencji rządowych i innych organizacji

Ustawa o ochronie prywatności z 1974 r

Ustawa o ochronie prywatności z 1974 r. (5 USC 552a) zapewnia nieujawnianie danych osobowych i gwarantuje, że agencje rządowe nie ujawniają informacji bez uprzedniej pisemnej zgody osoby, której dane informacje dotyczą.

US PATRIOT Act

Ta ustawa, z oficjalną nazwą Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, z 2001 r., Daje rządowi prawo do przechwytywania komunikacji głosowej w hakowaniu komputerowym i innych rodzajach dochodzeń. Ustawa Patriot Act została uchwalona przede wszystkim w celu radzenia sobie z działalnością terrorystyczną, ale może być również rozumiana jako mechanizm podsłuchowy do wykrywania i zapobiegania próbom włamania.

Ustawa o likwidacji papierkowej ustawy (GPEA)

Ustawa o likwidacji papierków rządowych (GPEA) z 1998 r. Wymaga od agencji federalnych zezwolenia na korzystanie z komunikacji elektronicznej podczas interakcji z agencją rządową. GPEA zachęca również do korzystania z podpisów elektronicznych. Kiedy cenne informacje rządowe są przechowywane w formie elektronicznej, zwiększa się cele i stawki dla hakerów.

Prawa cybernetyczne w innych krajach

W innych krajach obowiązują własne przepisy dotyczące ochrony informacji i ataków hakerskich. Podczas przeprowadzania testów penetracyjnych dla organizacji międzynarodowych konieczne jest sprawdzenie praw rządzącego państwa, aby upewnić się, że testy są legalne w danym kraju. Za pomocą Internetu i zdalnych ataków można bardzo szybko przekroczyć granice regionalne i międzynarodowe. Podczas wykonywania zewnętrznego ataku zdalnego dane mogą być przechowywane na serwerach w innym kraju i mogą obowiązywać przepisy tego kraju. Lepiej być bezpiecznym niż żałować, tak samo jak badania przed przeprowadzeniem testu penetracji dla podmiotu międzynarodowego. W niektórych krajach przepisy mogą być łagodniejsze niż w Stanach Zjednoczonych i fakt ten może działać na Twoją korzyść podczas gromadzenia informacji.

Podsumowanie

Etyczne hakowanie to coś więcej niż uruchamianie narzędzi hakerskich i uzyskiwanie nieautoryzowanego dostępu do systemów tylko po to, by zobaczyć, co jest dostępne. W przypadku hakerów etycznych hakowanie obejmuje wszystkie aspekty rozpoznania i zbierania informacji, ustrukturyzowane podejście i analizę po wszczęciu postepowania. Etyczni hakerzy wymagają dogłębnej znajomości systemów i narzędzi, a także dużej cierpliwości i powściągliwości, aby nie dopuścić do uszkodzenia systemów docelowych. Hackowanie może odbywać się w sposób etyczny, a w rzeczywistości jest zlecane przez rząd i sektor prywatny w celu zapewnienia bezpieczeństwa systemów.

Do Zapamiętania!

- Zrozumienie podstawowej terminologii hakerów. Upewnij się, że znasz i możesz zdefiniować terminy: zagrożenie, exploit, podatność, cel oceny i atak.

- Zrozumienie różnicy między etycznymi hakerami i crackerami. Etyczni hakerzy to specjaliści od bezpieczeństwa, którzy działają w obronie. Krakersy są złośliwymi hakerami, którzy decydują się zadać obrażenia w systemie docelowym.

- Poznanie klasy hakerów. Kluczowe znaczenie ma znajomość różnic między czarnymi kapeluszami, białymi i szarymi kapeluszami na egzaminie. Wiesz, kim są dobrzy ludzie i kim są źli ludzie w świecie hakowania.

- Poznanie fazy hackowania. Pasywne i aktywne rozpoznawanie, skanowanie, uzyskiwanie dostępu, utrzymywanie dostępu i pokonywanie ścieżek to pięć etapów hakowania. Zna kolejność faz i to, co dzieje się podczas każdej fazy

- Bądź świadomy rodzajów ataków. Rozumienie różnice między atakami aktywnymi i pasywnymi oraz atakami wewnętrznymi i zewnętrznymi. Zdolność do wykrywania to różnica pomiędzy atakami aktywnymi i pasywnymi. Lokalizacja atakującego to różnica między atakami wewnętrznymi i zewnętrznymi.

- Poznanie typu hackowania etycznego. Hakerzy mogą atakować sieć ze zdalnej sieci, zdalnej sieci dial-up lub sieci lokalnej, lub za pomocą socjotechniki, skradzionego sprzętu lub fizycznego dostępu.

- Zapoznanie z typami testów bezpieczeństwa. Etyczni hakerzy mogą testować sieć za pomocą black-box, white-box lub gray-box testing.

- Znajomość raportu etycznego hakowania. Raport etyczny hakowania zawiera informacje o wykonanych działaniach hakerskich, wykrytych lukach w sieci lub systemie oraz środki zaradcze, które należy wdrożyć.

- Poznanie konsekwencji prawnych związanych z hakowaniem. Ustawa o wzmocnieniu bezpieczeństwa cybernetycznego z 2002 r. Może być wykorzystana do ścigania etycznych hakerów, którzy lekkomyślnie zagrażają życiu innych.

- Bądź świadomy praw i kar mających zastosowanie do włamań do komputera. Tytuł 18 sekcji 1029 i 1030 amerykańskiego Kodeksu nakłada surowe kary za włamania, bez względu na intencje