PORADNIKI

Metody Hackingu: Socjotechnika

WPROWADZENIE

Główną taktyką wykorzystywaną przez firmy i instytucje dla zapobieżenia atakom hackerów jest zwiększenie bezpieczeństwa dzięki zastosowaniu bezpieczeniejszych i bardziej złożonych programów w systemach komputerowych. Modernizacja komputerów i szyfowanie danych z górnej półki jest wspólnym rozwiązaniem problemu hackerskich włamań. W celu przeciwdziałaniu rosnącej ilości oprogramowania i sprzętu do ochrony przeciwko hackerom dla uzyskania nieautoryzowanego dostępu do systemów, hackerzy stosują metody omijania technicznych systemów. Zamiast ataków na system, uderzają w możliwą słabość : człowieka. Pomimo dzisiejszej ogromnej automatyzacji komputerów i sieci, nie ma jednego systemu komputerowego na świecie, który nie zależy od człowieka w tym czy innym punkcie. Zawsze są ludzie , którzy muszą zapewnić sieci informację i konserwację. Hacker który wykorzystuje socjotechnikę określa tych ludzi, i próbuje wycisnąć z nich informację za pomocą przebiegłych (w rzadszych i mniej udanych przedsięwzięciach, hacker może po prostu poprosić o informację bezpośrednio) Sojotechnika jest to próba uzyskania od legalnego użytkownika systemu komputerowego użytecznych informacji; najczęściej nazwy i hasła w celu uzyskania dostępu do systemu.

Dlaczego używamy socjotechniki?

Powody stosowania socjotechniki dla uzyskania dostępu są proste:po jej opanowanio=u, socjotechnika może być używana w systemie mimo platfoprmy i obecności sprzętu i oprogramowania. Socjotechnika ma wiele postaci, ale wszystkie są oparte na zasadzie maskowania się jak niehacker, który potrzebuje informacji lub zasługuje na uzyskanie dostępu do systemu. Oprócz obsługi dużych systemów bezpieczeństwa, inną taktyką jaką stosują profesjonalni pracownicy od bezpieczeństwa, jest 'bezpieczeństwo przez niezrozumiałość', która udostępnia szczątkowe informacje użytkownikom, przy założeniu ,że uprawnieni użytkownicy zostali przeszkoleni a hackerzy zniechęcą się do odgadywania różnych poleceń lub procedur. Bezpieczeństwo przez niezrozumiałość może być również zrealizowana przez ukrywanie pewnych plików lub systemów informatycznych lub proszenie o mylące logowanie. Ta metoda zabezpieczenia jest całkowicie podważona, gdy zaangażujemy inżynierię społeczną. Przy elemencie ludzkim, wszystkie informacje, które pozwalają na zabezpieczenie przez niezrozumiałość również mogą zostać ujawnione hackerowi.

Metody ataku

Mimo,że metody używane przez socjotechników opierają się na tych samych zasadach, przebrania hackerów mogą być bardzo różńe, w zależności od poziomu umiejętności hackera i rodzaj informacji po jakie sięga. Jedną z typowych metod stosowaną przez atakującego

jest udawanie nowego w systemi i że potrzebuje pomocy z uzyskaniem dostępu. Rola nowej osoby ("newbie" lub "neofity") jest łatwa dla potencjalnego hackera do osiagnięcia. Łatwo może udawać ,że nie wie zbyt wiele o systemie i dalej pobierać informacje. Ten podstęp jest powszechnie stosowany, gdy osoba atakująca nie jest w stanie dostateczni wybadać firmy lub znaleźć informacje, które pozwoliłyby jeej umieścić nogę w drzwiach. Prosta metoda tej techniki polega na tym ,że hacker dzwoni do sekretariatu firmy i udaje nowego pracownika czasowego, który ma problemy z dostępem do systemu. Sekretarka (lub inna uprawniona osoba) może skłaniać się i być dumna ,że może zaoferować pomoc nowej osobie w pracy. Użytkownik może po prostu podać nazwę i hasło konta gościa, lub nawet może przejść do szczegółó informacji na temat procedury logowania do różnych działów. Jeśli intruz jest jużna końcie gościa, może mieć dostęp do innych (ważniejszych) kont stamtąd. Może być też w stanie znaleźć wystarczająco informacji o firmie aby wykorzystać podobną taktykę : odwrócona socjotechnika. Inne postacie jakie mogą przybierać socjotechnicy to doradca komputerowy lub pomoc , dzięki czemu uzyskują informacje jak naprawić komputer. Ta technika opiera się na założeniu ,że jest cosnie tak z komputerem. Pojawiając sie jako pan od pomocy, użytkownik będzie mniej podejrzliwy i bardziej skłonny odpowiadać na dociekliwe pytania. Inną formą ataku na przejęcie jest samego systemu operatora. Potencjalny hacker będzie udawał,że istnieje błąd na wszystkich kontach, i,że musi zresetować konta. Aby to zrobić musi użyć starych haseł użytkowników. Jeśli pracownik jest na tyle naiwny będą ujawniać informacje myśląc ,że robią firmie przysługę. Chociaż istnieje wiele metod i technik, te powyższe przypadki stanowią większość zarejestrowanych przypadków inżynierii społecznej.Przebrania i sztuczki jakie hackerzy stosują do socjotechnik mają jednak swoje ograniczenia. Podczas ataku inżynierii społecznej hacker zakłada wsółdziałanie i liczy na szczęście przy udanym hackowaniu, Powyższe przykłady działają zwykle na pracowników którzy nie są świadomi różnych form socjotechniki, albo nie dbają o bezpieczeństwo firmy. Nawet jeśli pracownik nie jest świadom inżynierii społecznej, nie powinien mieć zaufania do hackera, który nie ma właściwej identyfikacji. Pracownik ,może również mieć świadomość ,że pracownicy czasowi zwykle mają kontak z menadżerami lub innymi osobami wewnątrz swopjego biura, i byłoby podejrzane aby prośba o pomoc przychodziła od nich. Problemy te są stałym zagrożeniem dla potencjalnego hackera, który wykorzystuje nowy rodzaj inżynierii społecznej nazwany odwróconą inżynierią społeczną.

Odwróćona inżynieria społeczna

Odwrócona inżynieria społeczna jest wyższą formą socjotechniki, która dotyczy różnych problemów jakie pochodzą z normalnej inżynierii społecznej. Ta forma może być opisana w ten sposób ,że to legalny użytkownik prosi hackera o informacje. W odwóconej inżynierii społecznej (RSE) to hacker jest uważany za człowieka z wyższego poziomu wobec użytkwonika, któy w rzeczywistości jest celem. Aby zastosować atak RSE, atakujący musi mieć wiedzę o

systemie i zazwyczaj musi również mieć dostęp do poprzednio przyznanego mu dostępu, zwykle poprzez normalną inżynierię społeczną.Szybki rzut oka na plusy i minusy SE i RSE:

- SE:Hacker ustala połączenia i jest zależny do użytkownika
- RSE: Użytkownik ustala połączenia i jest zależny od użytkownika

- SE: Użytkownik czuje ,że hacker jest mu zobowiązany
- RSE: Użytkownik czuje się dłużnikiem hackera

- SE:Pytania często pozostają nierozwiązane dla ofiary
- RSE:Wszystkie problemy zostaną rozwiązane , żadnych podejrzeń

- SE:Użytkownik ma kontrolę dostarczając informacji
- RSE: Hacker ma całkowitą kontrolę

- SE: Mało lub brak wymaganego przygotowania
- RSE: Dużo planowania i konieczny poprzedni dostęp

Typowy atak RSE składa się z trzech głównych części : sabotaż, rekalmy i pomocy. Po zdobyciu łatwego dostępu za pośrednictwem innych śrdodków, hacker sabotuje stację roboczą albo przez jej uszkodzenie albo przez sprawienie wrażenia ,że jest uszkodzona. Mnogość komunikatów o błędach, przełączanie parametrów/opcji lub symulowanie programów takich jak fałszywe podpowiedzi mogą wykonać tego typu sabotaż. Użytkownik systemu widzie nieprawidłowości, a potem próbuje szukać pomocy. Aby być tym jedynym do którego zadzowni użytkownik, atakujący musi si reklamować jak ten który jest w stanie wyeliminować problem. Reklamą może być rozprowadzanie fałszywych wizytówek w biurze lub nawet podając numer telefonu w samym komunikacie błędu. Prosty komunikat błędu może być następujący:

* * ERROR 03 – Restricted Access Denied * * -Brak dostępu do pliku przez użytkownika. Skonsultuj się z Panem Kowalskim pod numerem (11) 111 222 333 po informacje o uprawnieniach pliku

W tym przypadku użytkownik dzwoni do pana Kowalskeigo po pomoc, i ujawnia informacje o koncie bez podejrzeń co do pana Kowalskiego Inny rodzaj rekalmy może wykorzystywać socjotechnikę. Przykładem tego może być to ,że hacker dzwoni do swojego celu i informuje go ,że obsługa techniczna ma nowy numer telefonu, a potem hacker podaje swój własny numer. Trzecią (i łatwiejszą) częścią ataku RSE dla hacketrów jest pomoc przy tym problemie. Ponieważ hacker jest inicjatorem sabotażu, problem jest łatwy do skorygowania, a cel nie podejrzewa osoby pomagającej, ponieważ zna ona się na swojej pracy. Zadadniem hackera jest tylko zdobycie informacji o koncie celu podczas pomagania mu. Po uzyskaniu informacji, hacker rozwiązuje problem a potem ko,nczy rozmowę, chętnie używając swojej nowno nabytej wiedzy.

Dlaczego działa Inżynieria Społeczna

Użycie inżynierii społecznej i odwróconej inżynierii społecznej są poszechne ponieważ często pracują w dobrych warunkach i zajmują mniej czasu (a czasem mniej wiedzy) niż ataki typu brute force.Działają ponieważ wszyscy ludzie mają pewne cechy psychiczne, które mogą być wykorzystane. Dyzfuzja odpowiedzialności jest używana kiedy użytkownik czuje ,że nie jest wyłącznie odpowiedzialny za swoje działania, co pozwala im udzielać informacji dużo łatwiej. Użytkownik może również ujawniać informacje jeśli czuje ,że robi coś co pomoże im w przyszłości. Obowiązek moralny wchodzi do gry kiedy cel wierzy ,że pomaga firmie rozwiązać problem, i często się ciezy kiedy pomaga. Istnieją różne inne czynniki , które pozwalają socjotechnikom być skutecznym, takie jak poczucie winy i perswazja osobista.

Metody zabezpieczenia

Ponieważ inżynieria społeczna i odwrócona inżynieria społeczna stają się coraz bardziej rozpowszechnione, a firmy i menadżerowie próbują zatrzymać ataki przed kolejnymi sukcesami. Firmy zaangażowane w bezpieczeństwo zdają sobie sprawę, że ogromne ilości pieniędzy na modernizacje i zestawy zabezpieczeń są zmarnowane jeśli nie można zapobiec atakom SE i RSE. Prostą odpowiedzią na zapobieganie takim atakom jest edukacja. Użytkownicy muszą być poinformowani aby nigdy nie podawali informacji o koncie bez zgody kierownika. Użytkownicy powinni byćświadomi popularnych metod SE i zawsze powinni zgłaszać podejrzane zachowanie. Wyłapywanie ataków RSE jest dużo trudniejsze, ale użytkownicy powinni nadal byćświadomi komu ufać gdy wystąpi problem. Socjotechnik może zaatakować każdego pracownika prosząc go o udzielenie informacji, wszyscy pracownicy powinni być poinformowani o metodach ataku. Hackerzy wiedzą ,że na niskim szczeblu pracowniczym i wśród osób o niskim morale firmy są łatwym celem do uzyskiwania informacji bez większego wysiłku. Ci pracownicy muszą współpracować aby dbać o bezpieczeństwo komputera i przedsiębiorstwa jako całości.

Konkluzja

Wszystkie systemy komputerowe na świecie muszą opierać się na człowieku, który jako taki posiada wrażliwe charakterystyki. Niezależnie od tego jak bezpieczne są urządzenia od strony elektronicznej, wiedza wydobyta od użytkownika mogą sprawić ,że sieci komputerowe będa niesprawne, jeśli są używane w sposób nieuprawniony. Hackerzy starają się dowiedzieć jak manipulować użytkwonikami którzy dostarczają cennych informacji w sieci. Mogą nawet korzystać z odwrtonej inżynierii społecznej w celu uzyskania dodatkowego dostępu do systemu.