

Introducere

Inamicul este ignoranța

„Studiază-ți dușmanul, fiindcă el îți va descoperi mai întâi greșelile“.

Antistene, filozof atenian, 440 î.Hr.

De la începutul lumii am căutat cunoștințele și experiența vârstnicilor; îndrumările lor ne-au ferit de nenumăratele boli și nenorociri aruncate asupra noastră. Dar astăzi, în lumea subterană ezoterică și în continuă mișcare a securității calculatoarelor, puțini mai sunt înțelepții care rătăcesc pe coridoarele marilor corporații. Soldații digitali ai contemporaneității nu au la dispoziție nici măcar o hartă rutieră a securității, cu atât mai puțin un cadru confirmat pentru combaterea acestor inamici enigmatici și vicleni.

Pentru a ne îmbunătăți securitatea și a lupta împotriva inamicului, trebuie să-l cunoaștem, să ne împrietenim cu el și să învățăm de la el. Hackerii sunt mult prea abili și deciziși pentru a fi ignorați. Prin însăși natura lor, hackerii continuă să se reinventeze pe ei înșiși și tehnicile lor, devenind deseori fantome în peisajul cibernetice, practic imposibil de urmărit. Ca un virus, ei se multiplică și se adaptează pentru a supraviețui, ceea ce-i face extrem de dificil de studiat.

Lumea de astăzi este un câmp de bătălie digital dominat de haos. La fiecare pas, tehnologia și calculatoarele preiau controlul asupra lumii noastre de zi cu zi, oferind un mod de viață simplificat și eficient, ascunzând în tot acest timp secretul întunecat care le amenință însăși existența. Cablurile care conțin miliardele de electroni din Internet sunt păstrătoarele unui uriaș secret, unul pe care de abia am început să-l dezvăluim și să-l expunem lumii întregi: lumea hackerului cu intenții rele. Citind cărți precum volumul de față, dar și urmărindu-i pe acești hackeri și învățând de la ei, puteți începe să le înțelegeți atacurile, modul lor de lucru, cum procedează și care le sunt motivele. Nimic altceva nu-i poate ajuta mai mult pe profesioniștii securității să ducă acest război.

Jos cu ochelarii de cal!

Un hacker vă poate găsi calculatorul pe Internet în 30 de minute. În fiecare secundă a fiecărei zile, hackeri cu intenții rele patrulează în peisajul digital, căutând o pradă slabă și ușoară. Mediul este plin de ținte, deoarece puțini înțeleg conceptul de securitate și chiar și mai puțini pot lua măsuri pentru atenuarea riscurilor. Știați că în fiecare an sunt date publicității 819 puncte vulnerabile? Pe câte dintre ele le cunoașteți?

Prea puține lucruri sunt cunoscute despre această întunecată lume subterană și, până de curând, puțini au avut posibilitatea de a-și prezenta tacticile într-un forum public, ca acesta. Mijloacele tradiționale de luptă impun existența unui inamic pe care îl poți vedea și pipăi, unul care respectă regulile angajamentului și pe acelea ale rațiunii, calități absolut necunoscute în ciber-anarhia de astăzi. În calitate de profesioniști în domeniul securității, suntem chemați pentru a evalua aria de întindere a unui atac, pentru a ajuta firmele să-și

revină în urma unei compromiteri de sistem și pentru a furniza măsuri concrete de întărire a sistemelor de calcul. Dar, fără o cunoaștere a inamicului, cum ne putem apăra?

Capitolele următoare nu sunt povești de ficțiune concepute de studenți la teatru sau la filme de groază. Sunt tehnici autentice și relatări despre câmpul de bătălie digital în care am intrat cu toții. Inamicul se află în spatele ușii și este invizibil pentru toți, cu excepția câtorva experți în domeniu. În paginile de față se găsesc sfaturile acestor experți. Sunteți pe cale să înțelegeți rațiunea și motivația inamicului, iar de aici îi veți cunoaște motivele, tehnicile și, cel mai important, veți învăța să-l învingeți.

Despre această carte

Lumea digitală fuge ca vântul și ca gândul. În fiecare oră apar noi instrumente, tehnici și metodologii ale hackerilor, iar activitatea de colectare, diseminare și traducere a acestora în limba vorbită este o formidabilă provocare. Noi am făcut tot ce era omeneste posibil pentru a vă prezenta cele mai recente noutăți în materie de tehnici și tehnologii.

Ușor de parcurs, cu o grafică sugestivă și cu factori de risc

Am folosit pentru această carte un format atractiv:

▼ Fiecare tehnică de atac este evidențiată cu o pictogramă specială, amplasată în marginea paginii, astfel:

Această este o ilustrație de atac

Facilitează identificarea instrumentelor și metodologiilor specifice de testare a pătrunderilor.

■ Fiecare atac este contracarat cu soluții, relevante și testate practic, care dispun, de asemenea, de propria lor ilustrație:

Această este o ilustrație pentru contramăsuri

Rezolvați problemele pe care le-am scos în evidență, dacă doriți!

■ Am utilizat cu larghețe indicii vizuale de genul

NOTĂ

SUGESTIE

AVERTISMENT

pentru a evidenția acele mici detalii sâcâitoare atât de frecvent omise.

■ De asemenea, am folosit multe exemple de listinguri de program, capturi de ecran și diagrame, acordând o atenție specială datelor introduse de utilizator, scrise cu albine în exemplele de programe.

▲ Fiecare atac este însoțit de un calcul actualizat al factorului de risc, derivat din trei componente, bazate pe experiența combinată a autorilor:

<i>Popularitate</i>	<i>Frecvența de utilizare a atacului împotriva unor ținte reale; 1 indică un atac extrem de rar, 10 simbolizează un atac foarte frecvent utilizat</i>
<i>Simplitate</i>	<i>Nivelul de cunoștințe necesar pentru executarea atacului, 1 indicând un programator de securitate cu multă experiență, iar 10 arată că nivelul de experiență necesar este extrem de redus sau inexistent</i>
<i>Impact</i>	<i>Pagubele potențiale produse de executarea cu succes a atacului; 1 indică dezvăluirea unor informații banale despre țintă, iar 10 este echivalent cu o compromitere a contului de superutilizator sau ceva similar</i>
<i>Factor de risc</i>	<i>Media celor trei valori, care determină factorul de risc de ansamblu</i>

Tuturor

Noi ne-am angajat să furnizăm informații de securitate oportune, exacte și efectiv utile despre tehnicile și instrumentele utilizate de hackeri, iar în același timp v-am dat puterea să vă apărați chiar împotriva acestor hackeri. Sperăm să găsiți elemente de valoare în volumul de față, dincolo de ponturile și trucurile amuzante. Noi sperăm să descoperiți valoarea intimă, intrinsecă, a securizării zestrei dumneavoastră informațională în această lume de bandiți la drumul mare. Să vă fie de folos!