

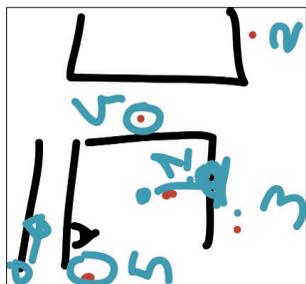
Newsdesk

Ogni mese tutte le novità dal mondo delle aziende e della comunità Open Source

Reportage

Inside CAT

Sono uno degli organizzatori del **CAT** (Cracca Al Tesoro, www.wardriving.it) e vorrei provare a raccontarvi cos'è questa manifestazione e cos'è successo a Milano il 12 marzo scorso. Ho visto nascere, svilupparsi e affermarsi negli anni questo progetto ludico-educativo che da un lato vuole far capire che esistono delle aree di sicurezza scoperte, e potenzialmente pericolose, e dall'altra dimostrare come non sia solo teoria o allarmismo creato ad arte dai produttori di software o hardware. L'idea è relativamente semplice: i partecipanti divisi in squadre, dispositivi portatili e connessioni wireless per trovare i bersagli, indizi criptici come nelle migliori cacce al tesoro, intelligenza, pazienza e utilizzo rigoroso di mezzi di trasporto a sola trazione umana. La cosa difficile, per gli organizzatori, è configurare di proposito gli apparati utilizzati per il gioco in modo non sicuro, inventarsi



I bersagli da bucare sono stati posizionati basandosi su questa mappa... ci stiamo ancora chiedendo come abbiano fatto a capirci qualcosa...



La foto di rito alla fine della manifestazione, con organizzatori e partecipanti al CAT di Milano – Foto di Matteo GP Flora

gli indizi, costruire una rete in grado di reggere agli attacchi di decine di persone contemporaneamente, trovare i luoghi fisici dove posizionare i bersagli. A Milano. In Corso Como. Il porta a porta fra i locali della zona non è stato facile. Abbiamo preso qualche porta in faccia ma tenacia e grandi sorrisi ci hanno aiutato.

Le ragioni

Non mi occupo di informatica, in realtà faccio altro nella vita, ma ho visto passare parecchi messaggi in lista in cui il resto degli organizzatori, "gli informatici", suggerivano, pensavano, correggevano strategie e ipotesi fino a che non hanno ottenuto un risultato soddisfacente. Alessio Pennasilico, Security Evangelist di Alba S.T., l'uomo sulla scala con il megafono, l'uomo delle regole e delle raccomandazioni ha infatti confessato: "È stato molto difficile per noi e per SonicWall configurare gli apparati

utilizzati per il gioco. Siamo abituati a configurare tutto al massimo grado di sicurezza. Il nostro lavoro è correggere i problemi che troviamo sulle reti e sui sistemi dei clienti. Creare una rete volutamente attaccabile, configurare i sistemi in modo errato è stato contro natura. Vedere, però, aumentare la consapevolezza sui rischi, vedere i partecipanti dimostrare quanto facilmente e velocemente un sistema insicuro possa essere violato, poter spiegare come evitare che succeda, per noi è stato importantissimo e sempre lo sarà. A Orvieto, dopo la prima edizione, abbiamo constatato che il nostro evento ha ridotto in maniera considerevole il numero di Access Point configurati male: una grande soddisfazione e un grande riconoscimento per i messaggi che abbiamo voluto lanciare. Se impegnare tutto il denaro e le energie che le nostre aziende investono in CAT significa avere reti più sicure, sistemi configurati meglio, meno

aziende a rischio, allora ne vale la pena. E non ci importa neppure che chiamino noi per mettersi al sicuro, l'importante è che lo facciano! Per ogni rete più sicura su Internet, infatti, saremo tutti meno vulnerabili ad attacchi DDoS, riceveremo meno spam, meno phishing, e i dati di meno persone saranno esposti a rischi. Per questo ci piace CAT: non è solo divertente e, per noi, stimolante: i risultati in termini di aumento della comprensione dei problemi legati alla sicurezza informatica sono immediati e tangibili". Per fortuna, aggiungo, e per fortuna anche i non addetti ai lavori e i divulgatori, giornalisti e blogger in testa, hanno capito che la sicurezza è un tema importante: sono soddisfazioni quando, se digiti "wardriving" su Google, trovi le prime tre pagine di risultati che parlano di CAT. Lo sa bene Cristiano Cafferata BDM & System Engineer SonicWALL Italia, l'uomo del "ferro" e del "don't panic" che ha "adottato" il CAT e, nonostante i bobotii ci si diverte un mondo. La mattina dell'11 marzo si è trovato davanti un disegno (vedi immagine in questa pagina) in cui erano segnati i luoghi dove posizionare i bersagli e la numerazione degli stessi. Chiaro, semplice e immediato. LOL. È lui che spiega come è stata creata e configurata la rete di macchine CAT, l'unica che le squadre erano autorizzate ad attaccare: "La struttura creata, che prevedeva cinque punti di accesso remoti distinti, ripresentava sul fronte wireless le casistiche classiche di 'mala configurazione',

volontariamente replicate durante il gioco: uso di chiavi WEP, uso di WPA corte e semplici da identificare (date di nascita, parole da vocabolario), nessuna *securizzazione* delle utenze una volta fatto accesso al Wi-Fi e molte altre. Il rischio corso dalle aziende è stato replicato sui primi tre livelli di accesso e infatti sono stati violati sia gli accessi radio che i server raggiungibili tramite tali linee. Al contrario gli ultimi due AP sono stati vincolati a feature aggiuntive, quali limitazione delle connessioni simultanee, limitazioni su MAC-ADDR e soprattutto filtri applicativi mirati a proteggere i server coinvolti, oltre a sistemi di autenticazione più forti e obbligo dell'uso di IPsec/SSL da client Wi-Fi a bersaglio server. Questo ha dimostrato come anche il Wi-Fi possa essere *securizzato* in modo semplice se si utilizzano i giusti sistemi. Grande soddisfazione ha dato sia l'elevato livello di resistenza dei sistemi wireless, anche sotto il carico di 12 squadre che incessantemente stressavano gli apparati, sia il dettaglio di reportistica che garantiva la visibilità chiara di 'chi provava a fare cosa!' Come sempre è stata una esperienza divertente e utile, sicuramente da replicare! Io non ho capito niente ma è per questo che due mesi fa ho preso

un worm e un tot di rimproveri dagli "informatici". Ho imparato la lezione? Spero di si...

Tornando alla gara...

Le squadre sono arrivate, come di consueto, da tutta Italia (isole comprese) chiamate dal tam tam sul Web, dalla curiosità e dalla voglia di fare del proprio meglio. Un numero di partecipanti mai raggiunto prima, come ripete a tutti il papà del CAT, Paolo Giardini, soprannominato "il notaio" per l'attenzione agli aspetti formali, per la calma e pacatezza: "Abbiamo battuto il record di squadre iscritte all'evento, ben 22. L'anno scorso sempre a Milano erano 'solo' undici mentre a Orvieto, in luglio, erano 17. Sarà difficile fare di meglio! Abbiamo avuto iscritti da tutto il nord Italia e anche, per la prima volta, dalla Sardegna. Siamo già in corsa per preparare al meglio la prossima edizione. Abbiamo individuato alcuni aspetti migliorabili e stiamo lavorando per coinvolgere ancora di più i 'non giocatori', il pubblico che sempre numeroso interviene per curiosità o per imparare qualcosa seguendo le squadre durante il gioco". Alle 14,30 dopo il brief e le raccomandazioni del caso le squadre si sono disperse nella zona di corso Como a Milano. Collegate costantemente con la control room tramite IRC, Twitter,

Facebook, livestreaming e cellulare per trasmettere messaggi, richieste d'aiuto e le chiavi che assegnavano loro i punti, le squadre quest'anno sono arrivate attrezzate con batterie e notebook di riserva. Si aggiravano per strada con il portatile in una mano e un'antenna o un cellulare nell'altra, senza curarsi del mondo esterno (non a caso abbiamo scelto una zona pedonale) dimostrando un entusiasmo, una passione e una voglia di capire come raggiungere l'obiettivo che raramente ho visto in ragazzi di quell'età. Su questo non posso far altro che sposare in pieno il pensiero di Raoul Chiesa, una delle persone che hanno visto nascere CAT in un caldo pomeriggio del 2009, nonché @ Mediaservice.net Srl / CLUSIT / UNICRI / ENISA PSG / OWASP Italian Charter: "quando CAT è nato, non avrei mai pensato a un simile successo. Ad oggi la 'Cracca Al Tesoro' è diventato un appuntamento fisso, che si ripete due volte all'anno, nell'edizione Security Summit (Marzo, Milano) e nell'edizione estiva umbra (Orvieto, Luglio). Quello che più mi ha colpito dell'ultima edizione milanese è stato il vedere squadre quasi completamente nuove, e provenienti anche da molto lontano. Secondo me questo è un chiaro segnale: i giovani

(e meno giovani!) hanno voglia di imparare, migliorare, costruire e, perchè no, una volta tanto, fare tutto questo in un contesto ludico, giocoso ma con ferree linee guida e 'regole di ingaggio'. Mi sento di dire che stiamo 'costruendo' i professionisti dell'Information Security di domani, in un'Italia che è, davvero, piena di talenti". Alle 19,30 dopo il conteggio dei punti tutti i partecipanti si sono ritrovati per fare domande, avere chiarimenti ed evidenziare difficoltà non preventivate. La targa del primo classificato è andata alla squadra degli **E-QUIPE** di Torino: veterani del CAT, non si sono persi un'edizione e in molti li ricordano correre su e giù per le strade di Orvieto nel caldo luglio umbro. La dimostrazione evidente che chi persevera alla fine arriva alla meta! Al secondo e al terzo posto due squadre che hanno fatto parecchia strada per giocare con noi: sono rispettivamente i **JUMPIN JESTER** che hanno raggiunto Milano dalla Sardegna e i **CRACKERS SALATI** di Trento che sono arrivati terzi con un distacco davvero minino dai secondi. Tutti gli altri li rivedremo sicuramente alla prossima edizione di CAT. Più preparati, più attrezzati e anche più agguerriti. E voi? Ci vediamo a Orvieto! **LXP**

Stefania Coltro

GIOCATI UN SUDOKU, TE LO OFFRE:

SETTIMANA
SUDOKU

A SOLO
€1,00

TUTTI I VENERDÌ IN EDICOLA

LA REGOLA E' UNA SOLA

Per giocare a SUDOKU si deve riempire la griglia in modo che ogni riga, ogni colonna e ogni riquadro contengano le cifre da 1 a 9 una sola volta. Per esempio, una riga è formata da 9 quadretti. In ciascuno dei quali va scritta una cifra scelta tra 1,2,3,4,5,6,7,8,9. Nella riga ciascuna cifra deve comparire una sola volta. Ci sono 9 righe e in ciascuna vale sempre la stessa regola: Sempre la stessa regola vale anche per le colonne. Ci sono 9 colonne, da riempire con le stesse cifre da 1 a 9, senza che si ripetano. Infine ci sono i riquadri 3x3, per un totale di 9 quadretti. In ciascun riquadro ogni cifra a 1 a 9 deve comparire una sola volta. Il gioco consiste nel riempire di cifre tutte le 81 caselle, rispettando contemporaneamente le regole per le righe, le colonne e i riquadri.

		3	5	2				6
	9	8						3
		5	8	4				9
	7		2	3	1		8	
			4	8	6			
	4		9	7	5		3	
3				9	2	5		
9						1	4	
6				5	4	3		

Difficoltà semplice

