Newsdesk

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

Manifestazione

Cracca al Tesoro

Nella suggestiva cornice del centro storico della città di Orvieto si è svolta, in un afoso sabato di luglio, una caccia al tesoro sui generis o, per meglio dire, una **Cracca Al Tesoro**. Invece che gioielli e monete d'oro, il tanto agognato tesoro era un *geekissimo* router wireless ADSL/UMTS; gli indizi, invece di essere nascosti in lugubri anfratti, erano celati dietro a ipertecnologici Access Point; al posto di pirati rozzi e ubriaconi, i protagonisti erano affermati professionisti, ricercatori universitari, studenti o semplici appassionati ma con in comune una stessa univoca caratteristica: la curiosità. Ma cos'è dunque questo "Cracca al Tesoro". Lo chiediamo ad **Alessio "Mayhem" Pennasilico**, che coordina il team che terrà sotto controllo la rete e le macchine della gara.

LXP: Alessio, come si gioca e quali sono le regole di Cracca al Tesoro?

AP: Vengono forniti un paio di indizi iniziali che condurranno le squadre a diversi Access Point sparsi sul territorio del centro storico di Orvieto. Ogni squadra è libera di scegliere un indizio o un altro. Ogni Access Point nasconde dietro due macchine differenti; abbiamo macchine Linux, AIX, UNIX, SCO, Cisco, Windows di vario tipo e così via. Il compito delle squadre è bucare l'Access Point e poi tentare di ottenere dei privilegi di accesso su una o su ambedue le macchine trovando e interpretando un indizio che permetterà loro di accedere alla stazione successiva. Per rendere la gara più interessante, è anche ammesso dal regolamento che i giocatori possano eventualmente risolvere i buchi di sicurezza rendendo il lavoro molto più difficoltoso alle squadre che dovessero successivamente tentare un attacco allo stesso sistema. La soluzione dei vari enigmi comporterà l'assegnazione di punti che saranno significativi nel caso nessuna squadra dovesse raggiungere il tesoro.

LXP: Che consiste in...

AP: Ancora non si sa o meglio si sa qual è il premio finale, un router wireless ADSL/UMTS, quindi un giocattolo molto geek che piace molto. In che cosa consiste però l'oggetto che dà diritto a ricevere il premio finale è qualcosa che scopriremo nel corso del pomeriggio.

Ma come è nata l'idea di un gioco così originale? Ci spiega la genesi dell'evento **Paolo Giardini**, il suo ideatore e organizzatore.

LXP: Ciao Paolo. Come vi è venuta l'idea di organizzare una simile manifestazione nella città di Orvieto?

PG: Una concomitanza di situazioni. Un paio di mesi fa ero a Orvieto a discutere di un progetto con i ragazzi del LUG locale ed era anche presente **Emanuele Gentili** di Backtrack che stava qui organizzando un incontro nazionale degli sviluppatori della distribuzione e desiderava agganciare a questo una vetrina capace di catalizzare l'attenzione del pubblico sulla giornata. Allora ho tirato fuori dal cassetto l'idea di una particolare caccia al tesoro. È successo che l'idea è piaciuta moltissimo e oggi ne raccogliamo i frutti.

I partecipanti

Ed effettivamente, se di raccolto si tratta, è stato molto prolifico. Nonostante il caldo di una estate che ha deciso di arrivare con tutta la sua forza, nonostante la location un po' fuori dagli schemi usuali e l'argomento fortemente tecnico, la risposta è stata superiore a ogni ottimistica aspettativa. Al via 17 squadre con nomi che, nello spirito goliardico che contraddistingue gli informatici, spaziavano da nick inerenti all'argomento tecnologico come "AdHoc", "Aircrack-gun", "RegEx", "PDCA" a nomi fantasiosi e spiritosi quali "Bevo per craccare", "Baby l'Orsetto" tanto per citarne alcuni. Sessanta e più hacker, arrivati un po' da tutta Italia armati con antenne direttive, Yaghi e cantenna fatte in casa con i barattoli di caffè o con l'immancabile tubo del liquore Bayles. C'è anche chi, in vero spirito hacker, reinterpretando la regola per cui le squadre potevano spostarsi solo a piedi o comunque con mezzi di locomozione umana, è arrivato con una carriola da muratore. Su di essa erano montati una batteria da camper, un inverter, un'antenna direttiva a 2.4 GHz per l'analisi delle reti e una a 5 GHz per il collegamento a Internet tramite un provider WADSL. Sulla carriola poi, un ripiano dove appoggiare il portatile con i più aggiornati ed evoluti software per il cracking di reti e sistemi. Non hanno vinto ma si sono meritati una menzione speciale da parte della giuria. Con Mayhem arroccato su una scala a libretto, in piena piazza del Popolo, i concorrenti hanno ascoltato i primi indizi, celati all'interno di un suo scombussolato discorso e sono partiti alla ricerca dei primi Access Point da violare. Di fronte, nel palazzo omonimo,

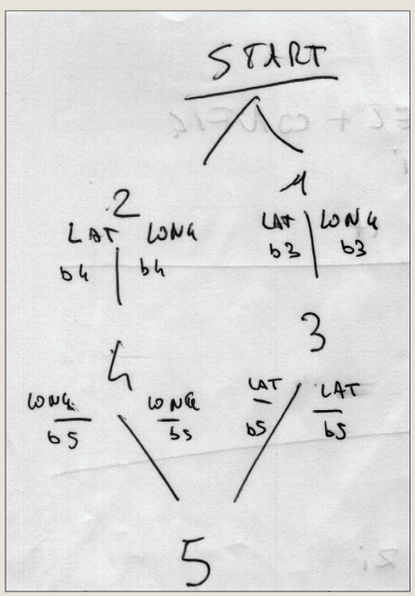
sede dell'evento, era stata istituita anche la *situation room*, la stanza dove i white hat monitoravano la rete e le macchine della gara, a cui erano state assegnate nomi di celebri gatti, da black cat a silvestro passando per ginxi, tom, felix e fritz.

La gara

Già dopo una ventina di minuti dall'inizio della gara, il team di controllo rilevava che alcune squadre, sulla base degli indizi iniziali, avevano già trovato i primi Access Point e stavano iniziando a lanciare attacchi agli stessi. Attacchi di breve durata in quanto gli Access Point, protetti dall'obsoleta cifratura WEP, hanno opposto flebile resistenza ai vari aircrack & co. Difatti, di lì a poco, iniziano ad arrivare nella situation room le chiavi WEP degli Access Point bucati da parte dei capitani delle squadre. Da qui all'attacco delle macchine a valle, il passo è stato breve ma non altrettanto facile. Armati di portscanning, nessus e altro, i nostri nuovi pirati hanno iniziato subito ad attaccare il server FTP e la porta SSH aperte sulla prima macchina e finalmente dopo un po' l'attacco dato i suoi frutti regalando l'accesso a un account FTP con user CAT2009 e password CAT2009. Ma l'accesso totale ancora è la da venire in quanto questo utente non ha i permessi di lettura per il file che contiene l'indizio per il successivo AP. Ma un ulteriore bug trovato nella versione dell'FTP presente sulla macchina permette di ottenere l'agognata informazione e di proseguire nella gara. Da questo momento in poi è tutto un susseguirsi di bug di Apache, di password "deboli" crackate, di server VNC senza password, di Cisco IOS con buchi di sistema e cosi via. Non sono mancati anche dei momenti di tensione durante l'evento che hanno messo a dura prova il team nella situation room. In un caso, una squadra, avendo ottenuto accesso di root a una macchina, ha pensato di cambiarne la password in modo

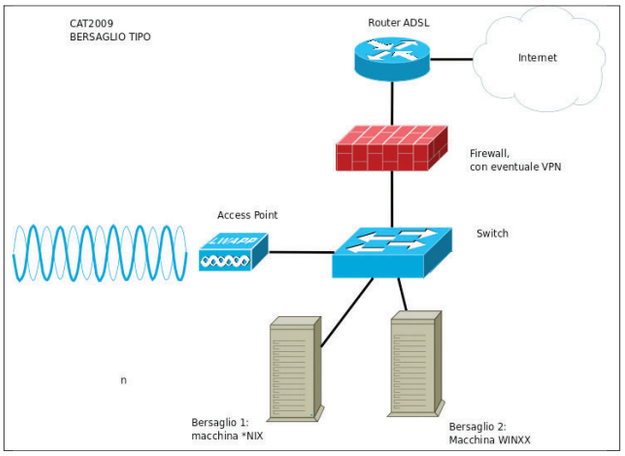
La rete di CAT2009 e la soluzione degli enigmi

Per capire meglio il funzionamento della caccia, vi mostriamo la mappa **originale** di CAT2009. Vedete infatti in questo box un abbozzo di struttura con la partenza, e i primi due AP da raggiungere grazie alle due indicazioni date da Mahyem durante il briefing iniziale. Le indicazioni, nascoste nel suo discorso erano "Olmo" e "Santa Maria della stella", ossia i nomi dei due quartieri dove erano situati i primi due AP. Il bersaglio numero 1, raggiungibile seguendo l'indicazione del quartiere "Olmo", era presso la sede di uno degli sponsor dell'evento ed era composto da un Access Point D-Link DAP 1160 con cifratura WEP. Dietro vi era una macchina Windows 2000 Server che aveva una vulnerabilità nel servizio RPC bypassabile via Metasploit. Inoltre, la macchina aveva un VNC server con password 1234. L'indizio da recuperare era nel file cat2009.txt sul desktop dell'administrator, indicante la latitudine bersaglio 3. La longitudine era invece in /home/test/cat2009.txt su un PC Linux DamnVulnerableLinux, a valle dello stesso AP, con attive vulnerabilità su vari servizi. Il bersaglio 2, raggiungibile grazie all'indicazione "Santa Maria della stella", era presso il centro studi città di Orvieto e si trattava di un AP Hamlet HNWS 254 con cifratura WEP. A valle, su una macchina Windows XP Pro con un server VNC installato senza password e con disco condiviso, vi era un indizio nascosto nei commenti del file hosts, indicante la latitudine del bersaglio n.4. La longitudine dello stesso bersaglio si trovava nel file cat2009 della home dell'utente "Paolo" su un'altra macchina a valle dello stesso AP. Questa era un IBM RISC 6000 con AIX 4. L'accesso a questo utente era possibile tramite tecniche di ingegneria sociale. La password era il nome del gatto di Paolo Giardini, nome reperibile sul suo blog. Il bersaglio n.3 era posto presso la caserma Piave: un AP D-Link DAP 1160 con cifratura WEP. Dietro di esso, un primo PC con Windows 95, disco condiviso, vulnerabilità relativa alla password delle condivisioni 'Share Level Password' e indizio sul file cat2009.txt sul desktop, indicante la longitudine del bersaglio 5. Questa volta lo stesso indizio, ossia la longitudine, era presente anche nell'altra macchina a valle di questo AP che era una Linux Badstore, con varie vulnerabilità (xss, sql injection,directory listing) e l'indizio era recuperabile, via Apache, sulla directory listabile /images in cat2009.txt. Per la latitudine dell'ultimo bersaglio bisognava trovare il bersaglio n.4 nascosto all'interno dell'ufficio del turismo nel piazzale Cahen composto da un AP D-Link DAP 1160 con una macchina Red Hat 7.2 con un utente "cat2009" e password "bucami", con vari servizi ssh, rcpbind, x11 con vari bug. La latitudine era nel file /home/cat2009/cat2009.txt. Inoltre, a valle dell'AP n.4 vi era anche un router Cisco 2600 con password utente standard "cisco" e password di enable uguale al nome del router (router2). La latitudine dell'ultimo bersaglio era nascosto nei commenti della configurazione delle interfacce. Infine, il *Santo Graal*, il bersaglio n.5 era posto nel palazzo sede dell'evento, ed era composto da un D-Link DAP 1160 con cifratura WPA2 e, a valle, un PC SCO Openserver 5 e una con Windows 7. Dato che quest'ultimo bersaglio non è stato "sconfitto", gli organizzatori non hanno voluto rendere note le loro vulnerabilità.



Significato dei nomi delle squadre

Diamo un senso ai nomi di alcune delle squadre:
- **AdHoc**: Collegamento di due dispositivi wireless senza presenza di Access Point.
- **Aircrack-gun**: Aircrack è un software di cracking per le reti wireless.
- **PDCA**: È un processo, spesso usato nei sistemi ISO-9001 per migliorare la qualità di un prodotto o di un processo produttivo. Sono le iniziali di "Plan-Do-Check-Act" ossia "programma-esegui-verifica-applica azioni migliorative".
- **RegEx**: Espressioni regolari. Stringa di codice che definisce la struttura per riconoscere, all'interno di documenti, determinati pattern testuali per estrazione, modifica ed elaborazione degli stessi.



da rendere alle altre squadre più complicato ottenere i privilegi di amministrazione. Ovviamente questo avrebbe impedito però anche l'accesso come root al team di controllo della gara che ha quindi ripristinato la password originale e da li è nato un battibecco via talk con il team che tentava di spiegare alla squadra i motivi per cui aveva reimpostato la password e la squadra che invece aveva deciso, per ripicca, di floodare il terminale di talk. In un altro caso, più grave, una squadra, una volta recuperato l'indizio nascosto, in questo caso le coordinate GPS del successivo bersaglio, hanno pensato bene di modificare l'informazione per ridirigere le successive squadre verso un paesino in Russia. Questa cosa ha comportato una lunga discussione all'interno del team per tentare di capire se era conforme alle regole dell'evento e alla fine è valsa la linea che la modica dell'indizio era un segno di "cattivo" cracking e quindi la squadra si è vista penalizzare di 10 punti per questo comportamento scorretto. Alla fine però nessuna delle squadre è riuscita a portare a termine, in tempo utile, l'arduo compito di craccare l'ultimo AP con cifratura WPA2 e quindi è stata la squadra dei **Disarm3d** ad aggiudicarsi l'ambito premio ai punti. Per rendersi conto che i moderni pirati non sono dei disadattati fuori dal mondo ma abili professionisti, basta guardare ai vincitori di questo contest. Sotto infatti al nick Disarm3d si cela in realtà il gruppo di reti e sicurezza dell'Università Roma Tre coadiuvati da un membro del gruppo reti e sicurezza dell'Università La Sapienza, sempre di Roma. Quindi non proprio gli ultimi venuti. Abbiamo chiesto loro quali sono state le difficoltà maggiori.

LXP: Quale è stato l'Access Point che vi ha fatto più penare?
Disarm3d: Il secondo perché era rotto :-D

LXP: Qual è stato invece quello più banale da bucare tra i quattro che avete violato?
Disarm3d: Mah, sono stati tutti abbastanza facili da violare. Il quarto è stato velocissimo da bucare ma solo perché eravamo i primi a violarlo ed eravamo i soli a lavorarci sopra quindi rispondeva meglio ai nostri attacchi mentre nei primi eravamo in tanti e quindi gli AP non rispondevano al meglio.

LXP: Che macchine avete violato?
Disarm3d: Un sistema CISCO, un Windows con XP o Vista e poi un ultimo sistema, una Web appliance, ma non abbiamo avuto tempo di fare fingerprint in quanto lo abbiamo violato senza sapere che SO fosse.
Dopo aver gustato l'ottimo buffet preparato dall'organizzazione non ci resta che tirare le somme di un evento che ha sicuramente raggiunto il suo scopo, ossia quello di far incontrare professionisti e appassionati del settore e metterli in amichevole competizione l'uno con l'altro al fine, non tanto di eleggere il migliore, quanto di permettere una crescita culturale dei partecipanti e una comprensione del problema della sicurezza informatica nel campo delle reti wireless anche ai non addetti ai lavori. Non c'è bisogno di dire che tutti noi aspettiamo con ansia il prossimo CAT2010.

Emiliano Bruni

Plone

Redomino Plone Tour

Giunto a metà del suo percorso, il **Redomino Plone Tour** può già tirare le somme: più di 200 presenze, quattro tappe svolte con successo, molto entusiasmo per le tre tappe rimanenti! Il Tour proseguirà infatti a ottobre, con una tappa a Torino martedì 6 e una a Marghera, in provincia di Venezia, martedì 20, ospitata dal CNA Veneto (Confederazione dell'Artigianato e della Piccola e Media Impresa); il tour terminerà con l'ultima tappa a Milano, mercoledì 11 novembre. La partecipazione è completamente gratuita, iscrizioni e maggiori informazioni all'indirizzo **http://redomino.com/it/promozioni/tour**. Per chi non conoscesse ancora questa iniziativa, ricordiamo che il Redomino Plone Tour è un ciclo di incontri gratuiti che ha come obiettivo presentare e diffondere la conoscenza su una tecnologia open flessibile, potente e user-friendly: il CMS **Plone**. Si tratta di un sistema per la gestione dei contenuti libero e a sorgente aperta, distribuito sotto licenza GPL e basato sul server per applicazioni Web Zope e sul linguaggio di programmazione Python. È uno strumento che consente di creare, aggiornare e gestire i contenuti di siti Web e intranet in modo semplice e intuitivo, indipendentemente dalle proprie conoscenze informatiche; inoltre presta particolare attenzione all'usabilità e all'accessibilità, rispettando la US Section 508, le linee guida del W3C in materia di accessibilità e le disposizioni in materia di Privacy (D.P.S.).