CTF 2005: "Spaghetti Hacker" per una nottata...

di Luca Carettoni

22 giugno 2005

Ore 15: Notebook, alimentatore, manuali, caramelle alla caffeina...Ok, c'è tutto...possiamo partire!

Sono le 16; l'università inizia a svuotarsi poichè molti studenti lasciano il campus per tornare a casa al termine della settimana; noi invece entriamo, ma non è certo un peso arrivare ora in università per questo venerdì sera "diverso" dal solito. In laboratorio il clima è decisamente amichevole. Non ci conosciamo tutti bene, ma di certo condividiamo le stesse passioni: i computer, le nuove tecnologie, l'OpenSource e il piacere di "smanettare". Questa sera però lavorando insieme, fianco a fianco, sarà l'occasione buona per socializzare, per condividere conoscenza e per instaurare dei sinceri legami personali. Al di là della gara che ci attende, percepiamo tutti che è una sensazione bellissima sentirsi parte di un gruppo, una crew composta da persone così diverse sia dal lato umano che tecnico. E' un genere di sensazione che può essere percepita solamente da tutti quelli che hanno partecipato a qualche *lan-party*: in questi momenti ogni persona è veramente se stessa perchè davanti al proprio computer ricrea una sorta di dimensione personale e in effetti, lavorando per gran parte della giornata su questo strumento, non è difficile trasferire su di esso parte della propria vita. E' assolutamente interessante osservare gli altri disporre meticolosamente i propri gadget tecnologici, al fianco degli amati portatili, per sentirsi a casa propria.

Alcuni ridono divertiti mentre mostrano le loro facce ad una webcam, montata per l'occasione, per lo streaming online; altri iniziano discorsi su quale distribuzione linux sia meglio o se un notebook con un solo tasto è ancora "geek"; altri, indaffarati, completano gli ultimi preparativi: c'è da finire di scrivere alcuni exploit, da ricontrollare le regole del firewall e da ridefinire la strategia per la gara. Il tempo passa ed inesorabilmente la tensione cresce. Si avvicina l'ora del setup della macchina virtuale su cui "girano" i servizi da proteggere e da

attaccare.

Una volta ricevuta la chiave per decifrare l'immagine virtuale è ora di entrare nel pieno della gara. E' un crescendo di sensazioni, di emozioni e di operazioni da compiere. Questa fase di setup è fondamentale per la buona riuscita della competizione: da un lato un gruppo di persone deve iniziare ad analizzare il sistema, scoprirne i servizi da salvaguardare ed iniziare a fare auditing del codice sorgente, dove disponibile. Sono in queste due ore che un buon team riesce a capire a fondo il sistema su cui dovrà lavorare, riesce ad individuare le prime vulnerabilità, a creare i primi exploit e le prime patch per proteggersi. Tra web application in php e perl, tra binari senza codice sorgente e strani file di configurazione diventano indispensabili le competenze di ognuno ed è in questo momento che la forza del team inizia a farsi sentire. Osservare il "guru" della situazione ti permette di imparare, di scoprire nuove tecniche e di insegnarle a tua volta. Ascoltare urla di "regular expression" o comandi linux ti fa poi sentire come un vero "Spaghetti hacker": alcuni di noi, nel senso puro del termine, lo sono realmente e lo si percepisce osservando la passione con cui digitano i comandi in console ed osservano intere pagine di codice sorgente. L'imperativo di "metterci su le mani" è la cosa fondamentale e per noi tutti è un vero piacere.

Trascorsa questa fase di preparazione, inizia la gara vera e propria. Tutte le vulnerabilità scoperte devono ora essere usate contro i server avversari per rubare queste misteriose flag. Alcuni di noi, usando gli exploit realizzati, si occupano di rubare queste stringhe alfanumeriche così preziose per il risultato della gara, altri analizzano lunghe sequenze di log e cercano di fermare gli attacchi avversari mentre altri ancora continuano la ricerca di difetti all'interno dei programmi, che permettano di estrarre le flag o di acquisire determinati privilegi sulle altre macchine. Il tempo scorre velocissimo, senza sosta, nelle prime ore. Ci sono tante cose da fare e la soddisfazione di urlare "flag", dopo essere riusciti a rubare informazioni dagli avversari, supera la stanchezza e la fame. In questi momenti un trancio di pizza ed una coca possono essere consumati mentre si lavora, perchè non c'è tempo da perdere vedendo i risultati delle altre squadre salire sempre più. Trascorse però queste prime ore, delle otto totali, l'euforia cala ma la determinazione di ognuno di noi è costante; siamo concentrati sui monitor a patchare sistemi e ad effettuare code injection in un'applicazione ancora non protetta. Le vulnerabilità semplici sono già state scoperte e corrette da tutte le squadre, ora è il momento delle cose "leet": dell'uso inaspettato di file presenti nelle applicazioni, di variabili apparentemente innocue o di servizi

sembrati inizialmente poco interessanti. Nelle ultime ore della gara la stanchezza è tanta e le parti del sistema con problemi di sicurezza sempre meno. Ma non vogliamo staccare, dobbiamo fare tutto quello che possiamo, ognuno con le proprie forze, sino alla fine. Un messaggio sul canale IRC, da parte degli organizzatori, segnala la fine della gara. Da un lato una liberazione grossa, dall'altro la speranza di aver fatto bene.

Minuti lunghissimi di attesa, minuti usati per vantarsi degli exploit scritti o per commentare eventi della gara. Il risultato tanto sperato, quanto atteso, arriva per il secondo anno consecutivo. Per noi tutti è un'enorme soddisfazione: la dimostrazione di poter essere all'altezza delle tanto blasonate università americane e la consapevolezza di essere al top di quel mondo al confine tra ricerca universitaria e underground, fatto di passione per le tecnologie e di puro piacere nel conoscere e scoprire i sistemi.