Ettercap, analisi e sniffing nella rete

Gianfranco Costamagna

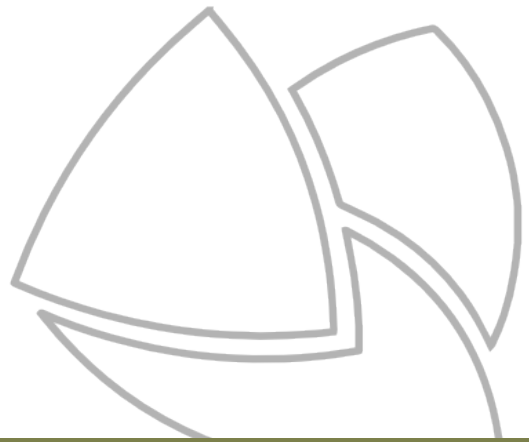
LinuxDay 2014

October 25, 2014

Chi siamo

Abinsula un'azienda specializzata in sistemi Embedded, Sicurezza Informatica e sviluppo di applicazioni Mobile con un organico di circa 30 sviluppatori software.

- Gianfranco Costamagna
  - Debian Maintainer
  - Ettercap Maintainer e Upstream Developer
- Ilario Pittau
  - Embedded Linux Developer
  - Factotum



Introduzione - Livello 2

- Il livello 2 comprende la comunicazione point-to-point, ovvero il livello MAC.
- Per raggiungere un certo ip nella rete, ho bisogno di avere il suo indirizzo MAC.
- Come lo posso ottenere?
  - Lookup nella mia ARP table.
  - ARP Request in broadcast nella rete.

Introduzione - Sicurezza a Livello 2

- La rete a livello 2 viene di norma (erroneamente) considerata “trusted”, un mezzo nel quale si deve avere accesso fisico per un’eventuale intrusione, ma ci sono alcuni casi in cui questo non vale, ad esempio:
  - Reti condivise
  - Reti wi-fi

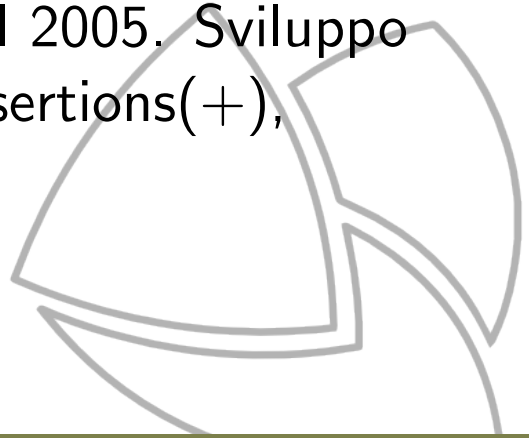
Ettercap

Ettercap una suite Open Source per attacchi MITM:

- Sniffing live delle connessioni
- Filtro dei contenuti "on the fly"
- Dissection attivo e passivo di molti protocolli
- Feature per analisi di reti e host
- Moltissimi altri trick

Storia

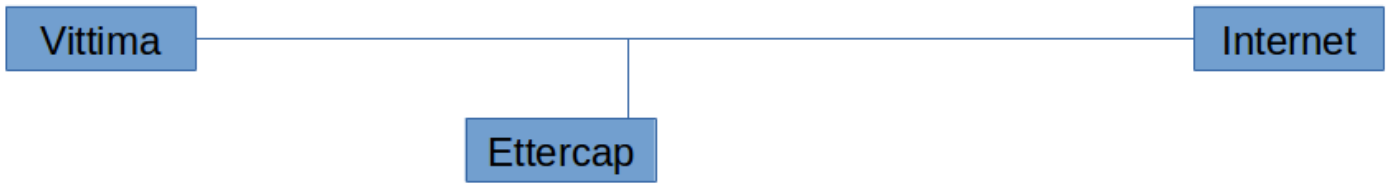
Creato da ALoR e NaGA nel 2001 e abbandonato nel 2005. Sviluppo ripreso nel 2011 Ad oggi 488 files changed, 46021 insertions(+), 18254 deletions(-)



Configurazione e Host-Scan

Ci sono due modalità di funzionamento:

- Unified Mode
  - Basta una singola interfaccia
  - Ideale per wifi o reti aziendali



- Bridged Mode
  - Usa due interfacce
  - Richiede accesso fisico al canale
  - Estremamente efficace

Configurazione e Host-Scan

Configurazione:

- Scelta dell'interfaccia
- Scelta della modalità di funzionamento

Host Scan:

- Mostra tutti gli host presenti nella rete: IP e MAC
- Permette di aggiungerli ai target per eseguire l'attacco MITM

MITM e Sniffing

ARP Poisoning:

- Il MAC Address dell'attaccante viene associato all'IP di un altro Host (spesso il default gateway)
- Tutti i dati verso il default gateway vengono rediretti verso l'attaccante

Una volta eseguito l'attacco ettercap permette di:

- Sniffare il contenuto delle connessioni
- Modificare il contenuto prima del forward
- Lanciare DOS attack

MITM e Sniffing

ICMP Redirect:

- Modifica la tabella di routing dell'host sotto attacco
- Permette di redirigere il traffico verso l'attaccante

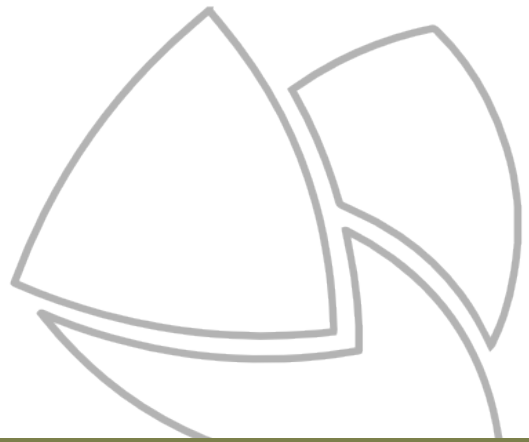
Port Stealing (inventato dai creatori di ettercap):

- Attraverso un pacchetto inviato allo switch viene rubata la porta di un altro host
- Lo switch inoltrerà tutti i dati di ritorno all'attaccante

MITM e Sniffing

DHCP Spoofing:

- L'attaccante si finge DHCP Server rispondendo alle DHCP Request
- Permette di redirigere il traffico con un fake default gateway
- Override del DNS server
- Come si fa con ettercap?



MITM e Sniffing

Sniffing:

- Permette di sniffare protocolli in chiaro e mostrare le informazioni principali. (es telnet, http...)
- Permette di sniffare protocolli cifrati. (es ssh, https...)
- In automatico attraverso regex mostra username e password trovate durante lo sniffing (share/etter.fields)

MITM e Sniffing

Sniffing SSL:

- Viene fornito all'attaccato un certificato non valido (browser avviserà l'utente)
- Il 70% degli utenti ignora il warning del browser e continua la navigazione insicura.
- Ettercap in automatico decifra col certificato fasullo e cifra con il certificato autentico del server.
- Supportato anche se attraverso un proxy

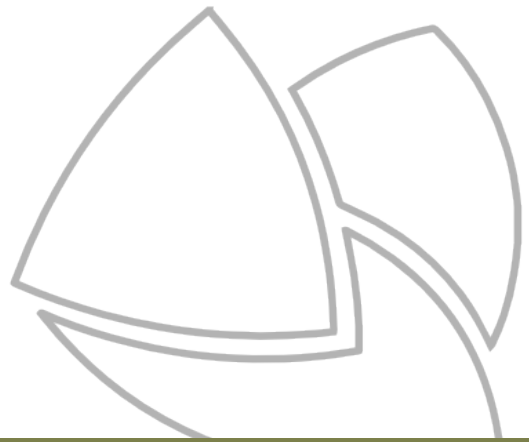
I filtri

I filtri sono utili quando si vuole modificare il traffico durante il transito nella rete.

- Filtri in base all'IP source e destination
- Filtri in base al MAC
- Utili per analizzare determinate connessioni
- Utili per attacchi mirati, ricerca di stringhe e sostituzione (injection)

Esempi:

- Cambio contenuto pacchetto
- Forzo il downgrade di un protocollo



Plugins

Ettercap supporta plugin esterni:

- arp_cop, autoadd, chk_poison, dns_spoof, dos_attack, find_ettercap, find_ip, finger, isolate, fraggle, mdns, pptp, remote browser, smurf_attack, sslstrip...

Plugins

Ad esempio, tramite DNS Fun, si può creare un file dns con I record dei quali si vuole cambiare ip che sarà dato in risposta alle query dns. Quando il vero server DNS risponderà oramai la vittima avrà già fatto la richiesta e scarterà la risposta duplicata

DNS Fun

microsoft.com A 107.170.40.56
*.microsoft.com A 107.170.40.56
www.microsoft.com PTR 107.170.40.56

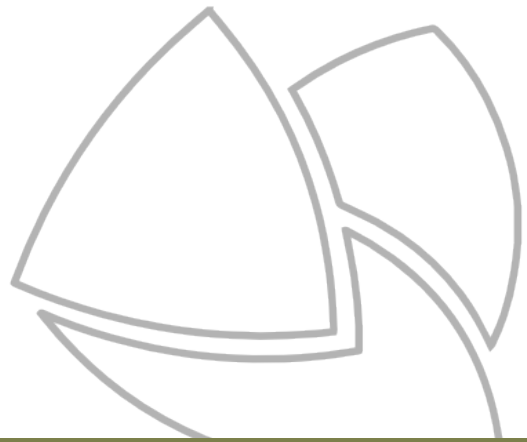
www.alor.org A 127.0.0.1
www.naga.org A 127.0.0.1
www.naga.org AAAA 2001:db8::2

Plugins

SSLstrip:
Nato come script python che durante il transito dei bytes nella rete toglieva la “s” forzando l’utilizzo del protocollo http, e quindi disabilitando di fatto la cifratura. Problemi di utilizzo, ettercap richiedeva l’ip_forwarding, sslstrip no, quindi difficile utilizzo dei due tool insieme.
Soluzione? Riscritto come plugin di ettercap, ora si può tenere traccia dei siti visitati direttamente dentro il codice di ettercap, trovando le password nello stesso modo di prima.

Come ci si pu proteggere?

- Usando ettercap (arp_cop/find_ettercap)!
- Arp watchers
- Arp statiche (funzionano veramente? Dipende dal kernel!)
  - Problemi con load balancers
- Sostituzioni GWs?
- Misure anti spoofing a livello 2 (switch ad esempio).



Domande

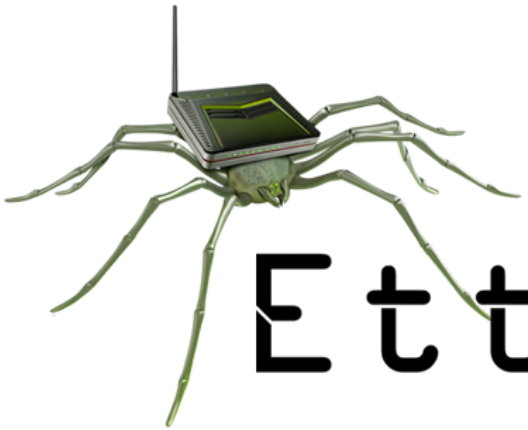
Gianfranco Costamagna

- gianfranco.costamagna@abinsula.com

Ilario Pittau

- ilario.pittau@abinsula.com

Grazie...



Ettercap