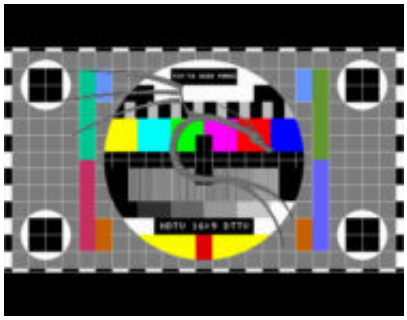
Telecamere e sicurezza: connubio possibile?

Author : Milo Caranti

Date : 4 Marzo 2019



Il tema della videosorveglianza è sicuramente caro al cittadino del terzo millennio. Il crescente utilizzo della rete internet nell'ambito delle telecomunicazioni, la diffusione della banda larga e i sempre più contenuti costi di implementazione hanno permesso l'affermazione delle telecamere IP, ormai onnipresenti nella vita e nelle abitazioni di ciascuno di noi.

La comodità di questi apparecchi è indiscutibile: con una semplice interrogazione al web server interno è possibile accedere in remoto all'apparecchio, visualizzare dal vivo le immagini e memorizzarle su dispositivi di archiviazione o piattaforme cloud spesso integrate.

Nel nostro Paese si contano all'incirca **2 milioni di telecamere**, una ogni 35 abitanti. In Europa è la Gran Bretagna a guidare la classifica con 4 milioni, un apparecchio ogni 14 abitanti.

Cifre sicuramente importanti e che offrono spunti di riflessione circa la concezione della privacy dell'odierna civiltà tecnologica. Eppure non reggono il confronto con la **Cina**, che entro la fine del 2020 conterà ben **626 milioni di telecamere** - una ogni due abitanti - a completamento di una manovra orwelliana e distopica di social rating e controllo delle masse, in cui chi attraversa fuori dalle strisce pedonali, oppure non rispetta la fila, vede comparire il proprio volto sui tanti schermi presenti in città, quasi fosse un ricercato in fuga.

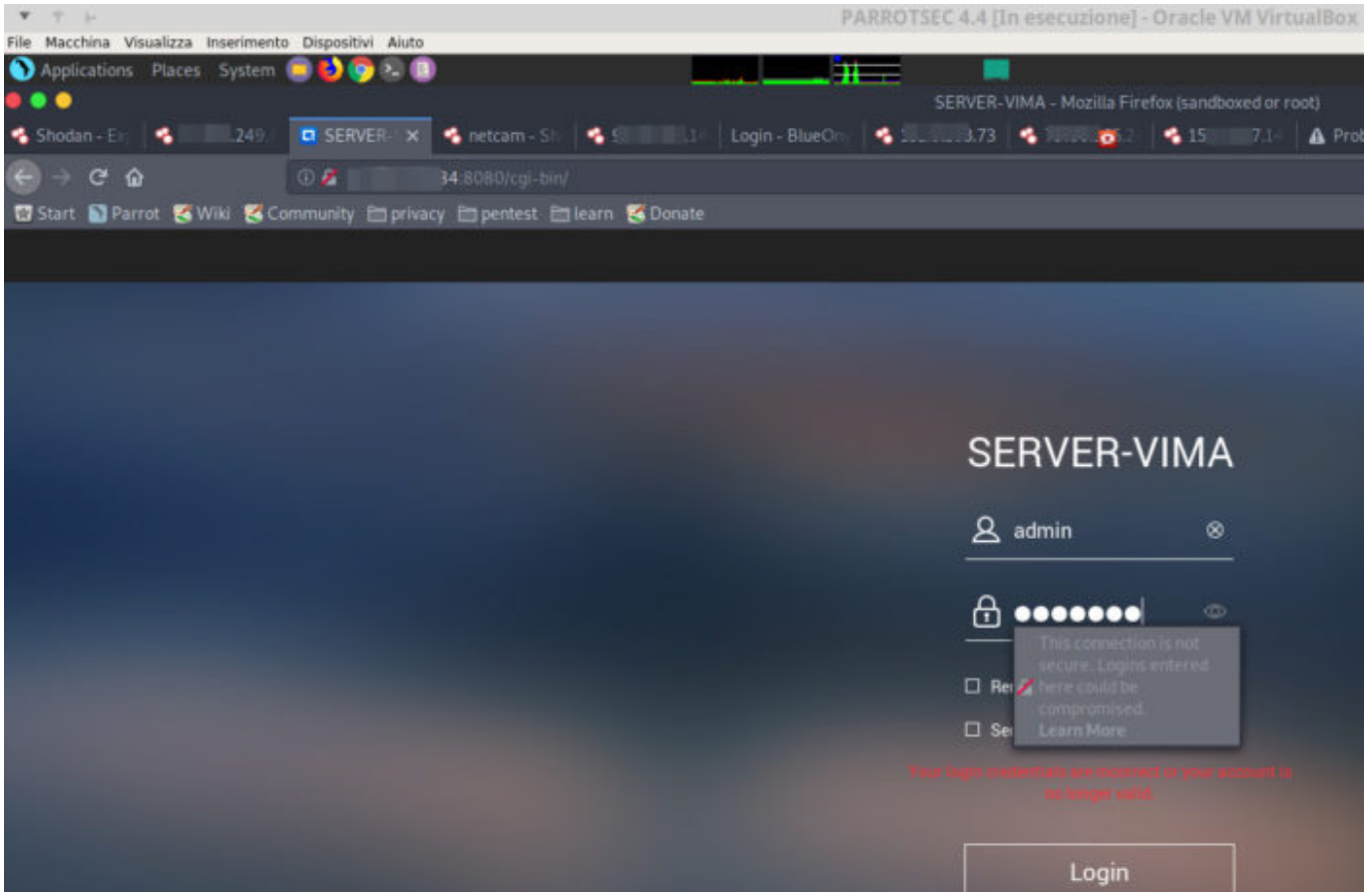
I più curiosi - e coloro che si occupano di sicurezza informatica - si saranno sicuramente trovati a riflettere, volgendo lo sguardo verso l'ennesima telecamera, riguardo l'effettiva sicurezza e discrezione che l'onnisciente apparecchio è in grado di garantire.

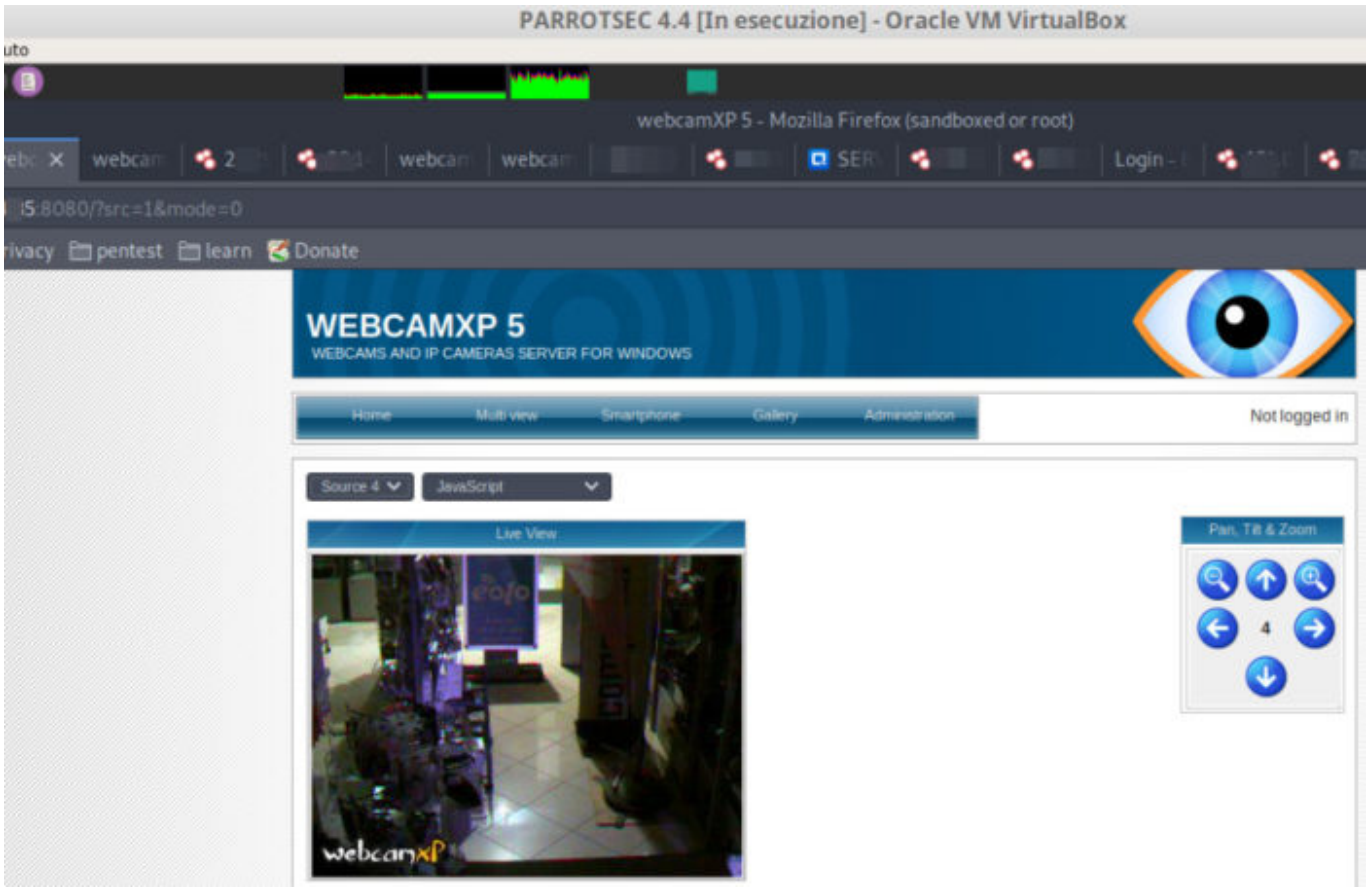
Per rendercene conto e avere un quadro più ampio della situazione, dobbiamo presentare *Shodan*, il motore di ricerca del mondo dell'internet delle cose. Inizialmente sviluppato da **John Matherly** per finalità di monitoring di prodotti tecnologici al fine di migliorare le strategie di marketing, è in grado di indicizzare i dispositivi connessi a Internet e, con opportune *query*, filtrare i risultati a seconda della versione del software installato (con relative indicazioni di potenziali vulnerabilità e bollettini CVE), del protocollo che si desidera interrogare, della presenza di credenziali di default o della completa assenza di autenticazione.

Previa registrazione al portale è possibile, seppur con diverse limitazioni circa il numero di risultati visualizzabili, restringere la ricerca per territorio, ottenere informazioni su porte e servizi aperti, versioni di sistemi operativi e così via.

Come è facile intuire, su Shodan troviamo anche **un numero enorme di telecamere mal configurate** ed esposte incautamente ad internet. Per i nostri scopi, ecco alcune semplici *query* che è possibile formulare alla ricerca dei più diffusi software per videosorveglianza:

```
Server: SQ-WEBCAM country:IT  webcamxp country:IT
```





Come si può vedere, la facilità con cui si accede alle pagine di login delle telecamere è sbalorditiva. In diversi casi l'accesso avviene direttamente al pannello delle impostazioni della telecamera, dunque il web server non è protetto da credenziali.

È bene puntualizzare che l'accesso a queste risorse, nonostante la totale assenza di procedure di autenticazione, può rappresentare comunque una violazione del Codice Penale:

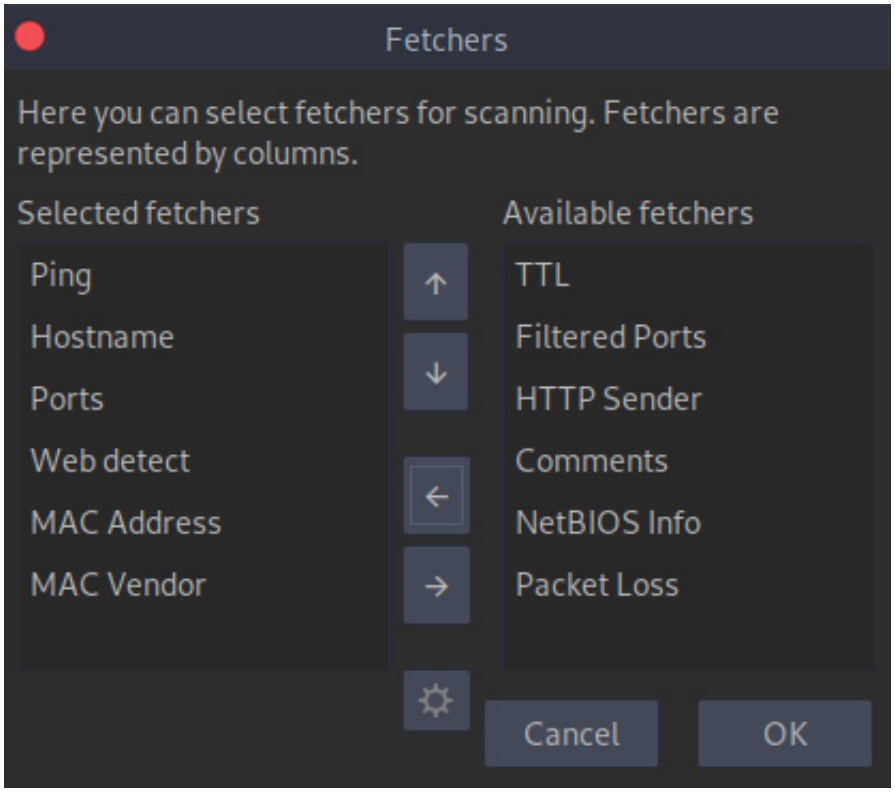
Art. 614 (**Violazione di domicilio**), art. 615-bis (**Interferenze illecite nella vita privata**), art. 615-ter (**Accesso abusivo ad un sistema informatico o telematico**), art. 615-quater (**Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**) art. 617-quater (**Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**), art. 635-bis (**Danneggiamento di informazioni, dati e programmi informatici**), art. 635-ter (**Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**), art. 635-quater (**Danneggiamento di sistemi informatici o telematici**), art. 635-quinquies (**Danneggiamento di sistemi informatici o telematici di pubblica utilità**).

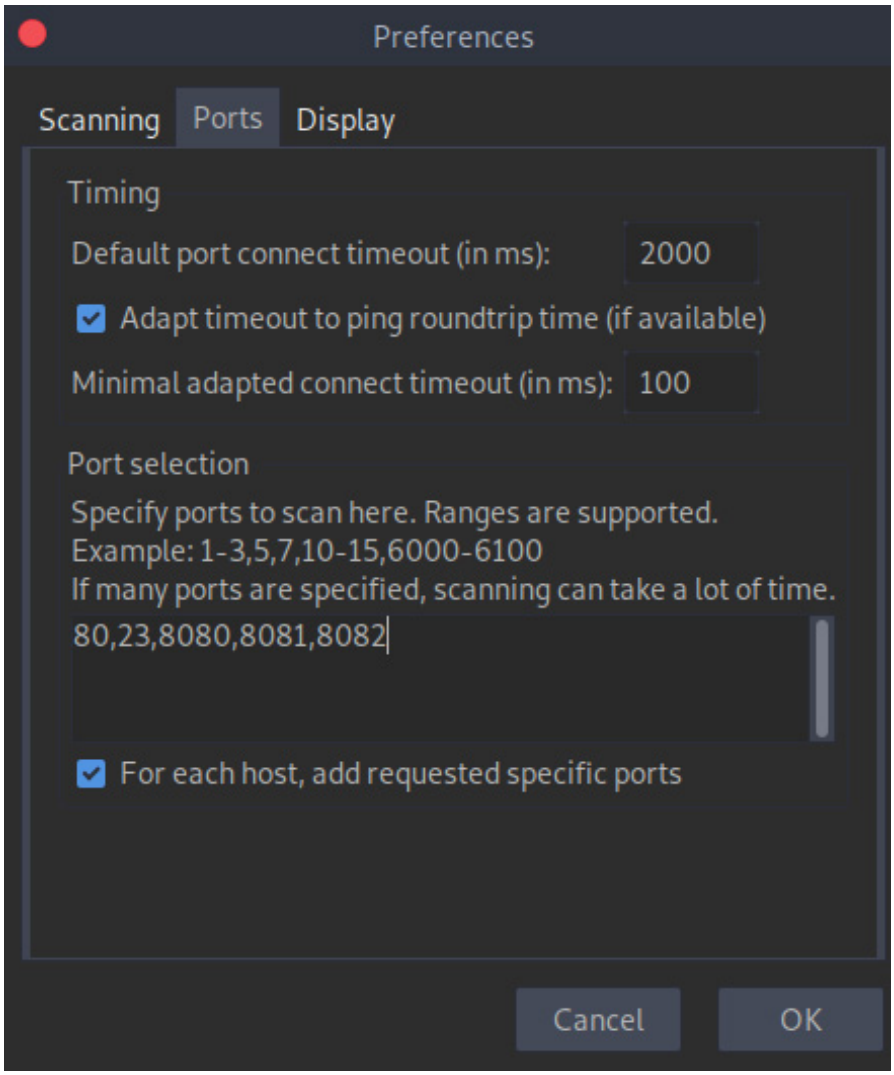
Dopo aver visto come cercare un dispositivo vulnerabile attraverso internet, sorge spontaneo chiedersi se sia possibile, per l'utente malintenzionato, individuare una telecamera di un dato luogo correttamente configurata ed eventualmente attaccarla al fine di ottenere un accesso abusivo. La risposta a questa domanda è sì, si può tentare.

Vestiamo dunque, per un attimo, i panni di un potenziale attaccante e prepariamo il terreno per definire il campo di azione.

Come prima cosa individuiamo la localizzazione del nostro indirizzo IP: un semplice *myip* digitato in un browser potrà illuminarci sulla nostra posizione. Dal momento che è ragionevole presumere - seppur entro certi limiti - che lo stesso ISP acquisti un blocco di indirizzi IP da assegnare ad una determinata zona geografica, possiamo tentare di individuare l'indirizzo IP pubblico delle telecamere che presentano un IP contiguo al nostro e che dovrebbero trovarsi, dunque, vicine alla nostra posizione. È bene sapere che la ricerca potrebbe non essere accurata, non potendo conoscere le policy interne con cui ciascun provider internet acquista e assegna gli indirizzi, ma è sicuramente un buon punto di partenza.

Procuriamoci poi una distribuzione Linux dedicata al *pentesting* e installiamo **AngryIP**, uno scanner di rete leggero e multipiattaforma, e impostiamo i parametri *Ports* e *Web detect* per avere più probabilità di successo (la visibilità degli indirizzi MAC e relativi vendor è opzionale). Specifichiamo poi le *well-known ports* più utilizzate in ascolto sul web server della telecamera. Naturalmente, se l'amministratore ha saggiamente impostato una porta non comune, il device non rientrerà nella nostra scansione:

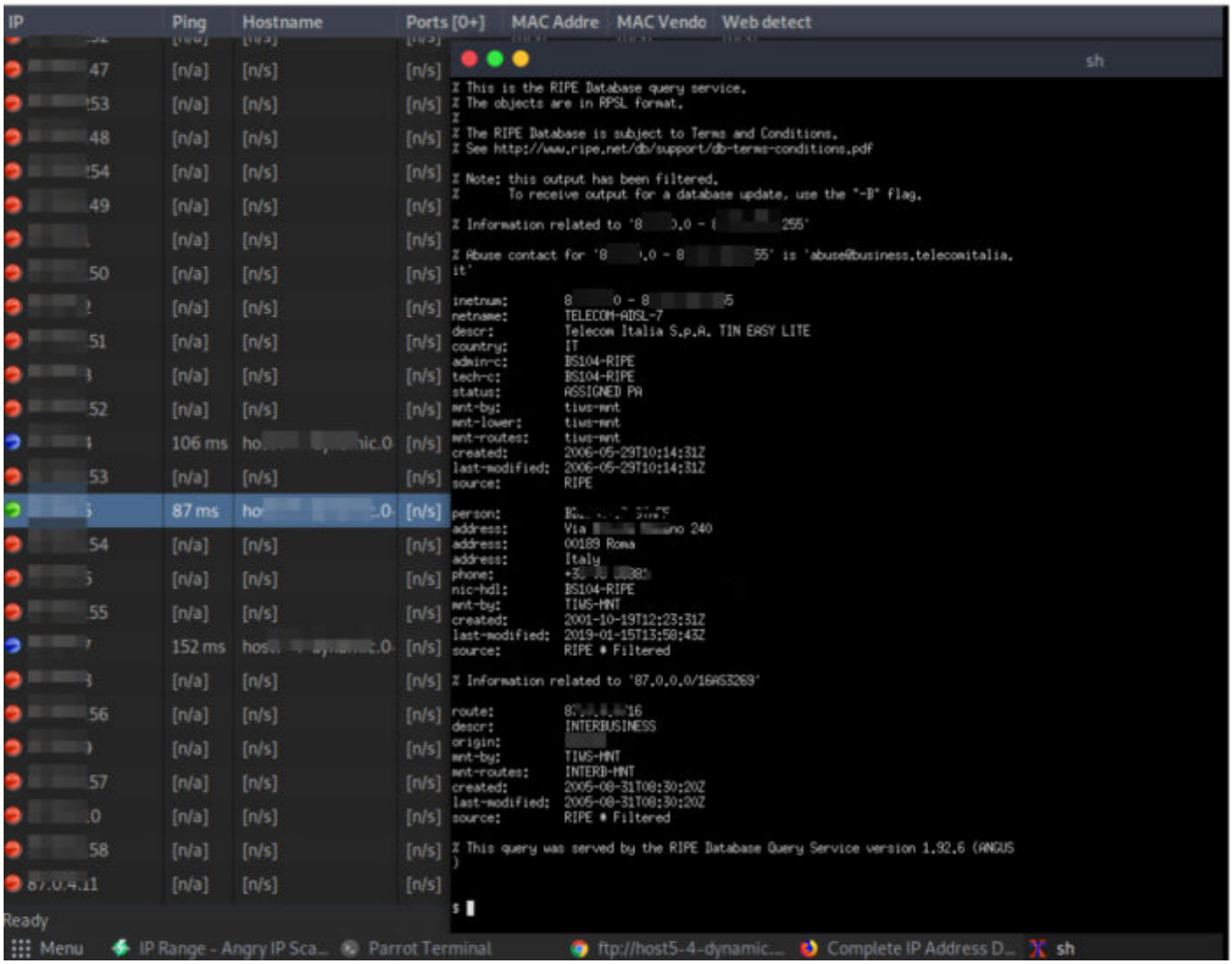




Stabiliamo a questo punto un range di indirizzi IP e avviamo la rilevazione. Per un primo test, suggerisco di impostare a /24 oppure a /20 la dimensione della sottorete IP, per arrivare a /16 nel caso non si trovassero device on-line; proseguire oltre risulterebbe poco pratico e allungherebbe significativamente i tempi di attesa. Ad ogni modo, è buona norma avvalersi di un calcolatore di indirizzi IP per meglio definire il numero di host che è possibile passare al vaglio. Per le distribuzioni debian-based, è possibile installarlo rapidamente con il comando:

```
sudo apt install ipcalc.
```

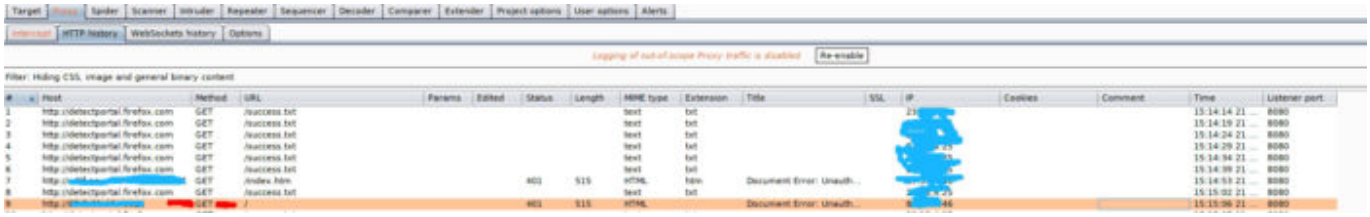
Per gli host trovati attivi, il programma consente poi di effettuare rapide ricerche *whois* oppure di aprire rapidamente con un browser la pagina web dell'interfaccia di login:



La classica combinazione *admin/admin* è d'obbligo per tentare un primo accesso: vale poi sicuramente la pena rintracciare su internet una lista di credenziali di default per marca/modello da provare rapidamente.

Qualora non avessimo successo, dovremo ricorrere a Hydra, strumento sviluppato da *The Hacker Choice* dedicato al cracking on-line utilizzabile su svariati protocolli.

Aiutandoci con un proxy interceptor (la scelta, in questo caso, ricade sempre su *Burp Suite*), identifichiamo il metodo HTTP impiegato dal server della telecamera e specifichiamolo come parametro per Hydra:



Infine, costruiamo il comando per lanciare un attacco di tipo dizionario al web form di accesso della telecamera:

```
hydra -s http-get 80 -l ?admin -P ?WORDLIST
 -e nsr -t 20 ?IPPUBBLICOCAMERA
```

dove:

-s rappresenta il numero di porta e il metodo usato;

-l è l'username da testare (in questo caso admin, ma possiamo indicare un file di username con lo switch *-L*);

-P è la lista di password da testare;

-e indica di provare password nulle, di usare l'username e il suo inverso come password;

-t rappresenta il numero di thread in parallelo.

CONCLUSIONI

L'installazione di una IP cam è, oggigiorno, un'operazione semplice e alla portata di tutti. Bisogna però tenere presente che - come per qualsiasi altro server esposto ad internet - vanno adottate tutte le cautele per minimizzare le probabilità di successo di un attacco.

Prescindendo da vulnerabilità di cui potrebbe soffrire la piattaforma cloud cui la telecamera potrebbe appoggiarsi per la trasmissione delle immagini, è buona norma assicurarsi di aver impostato una **combinazione username/password robusta**, da cambiare periodicamente, e una **porta di accesso alta** per evitare facili scansioni. Nel caso ci si appoggi a servizi DDNS, indicare anche qui nomi complessi e di difficile individuazione. In gioco c'è la nostra privacy e in questi casi essere paranoici paga, eccome. Dopotutto, "*la paranoia è solo un calcolo più attivo delle probabilità"* (Richard Krause).

BIBLIOGRAFIA

https://www.repubblica.it/esteri/2017/12/29/news/cina_il_grande_fratello_che_controlla_un_miliardo_e_mezzo_di_cittadini-185424301/.

https://www.ilsole24ore.com/art/tecnologie/2018-04-10/cina-quando-sorveglianza-e-globale-sotto-controllo-13-miliardi-persone-084939.shtml?uuid=AEuUQXVE&refresh_ce=1.

Articolo a cura di **Milo Caranti**