Vodafone Station
Uauthenticated full router backend access

Indice

1. Introduzione

Vodafone Italia BV ad Aprile '15 ha presentato il progetto Vodafone Wi-Fi Comunity[1] [2] in partnership con Fon, tale servizio permette ai clienti di rete fissa Vodafone di accedere senza costi aggiuntivi ad oltre 1 milione di hotspot condivisi su tutto il territorio italiano e grazie alla collaborazione con Fon il servizio sarà disponibile anche all'estero in oltre 15 milioni di hotspot presenti nei 15 paesi in cui è attivo il servizio. Gli utenti non Vodafone potranno accedere a tali hotspot acquistando un pass orario o giornaliero.

Vodafone Wi-Fi community è un sevizio offerto gratuitamente e viene automaticamente attivato su tutte le Vodafone Station 2 e Revolution dei clienti Vodafone Casa con abbonamento Fibra o ADSL.

Si è quindi deciso di analizzare questo progetto per verificare se la privacy del titolare della linea telefonica viene rispettata e se i suoi dati vengono protetti come precisato dalle FAQ di Vodafone Comunity.

> *I MIEI DATI SARANNO PROTETTI?*
> *Certo! La tua privacy e la sicurezza delle tue connessioni e dati sarà sempre garantita. La rete Wi-Fi per gli altri membri della community è separata dalla rete domestica Wi-Fi. Nessuno avrà quindi accesso alle tue navigazioni e ai tuoi dati sensibili.*

L'analisi ha purtroppo portato alla luce una importante vulnerabilità sulla procedura di autenticazione degli utenti, tale vulnerabilità permette ad un attaccante di risalire alla chiave Wireless della rete privata dell'abbonato, di visualizzare il numero telefonico dell'abbonato, le chiamate, i files condivisi e di effettuare chiamate telefoniche ai danni dell'abbonato.

Abbiamo poi analizzato il firmware della Vodafone Station Business, individuando un'altra vulnerabilità.

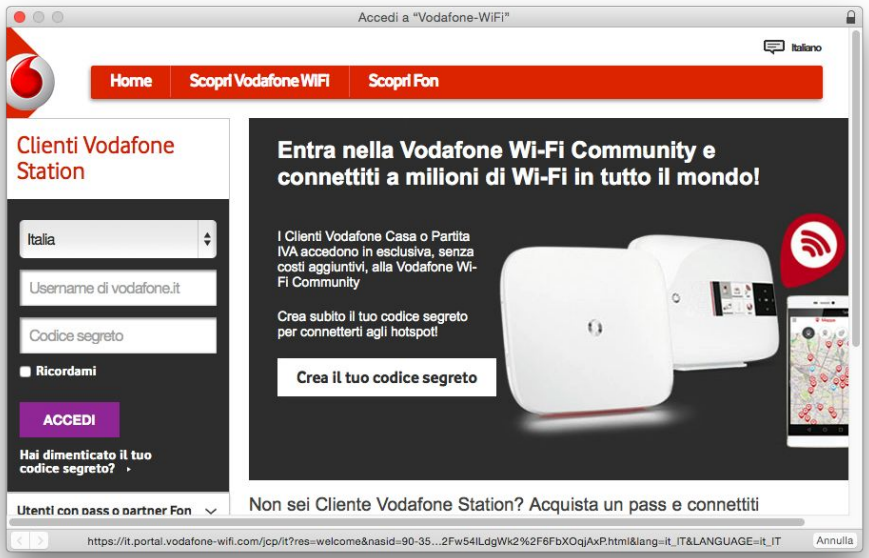
1. http://www.lastampa.it/2015/04/17/tecnologia/vodafone-italia-lancia-il-wifi-condiviso-FOMpjJEfQ1FhGGH7BWu9bK/pagina.html
2. http://www.vodafone.it/portal/Privati/Vantaggi-Vodafone/Per-i-gia-Clienti/wifi-community

2. Vulnerabilità

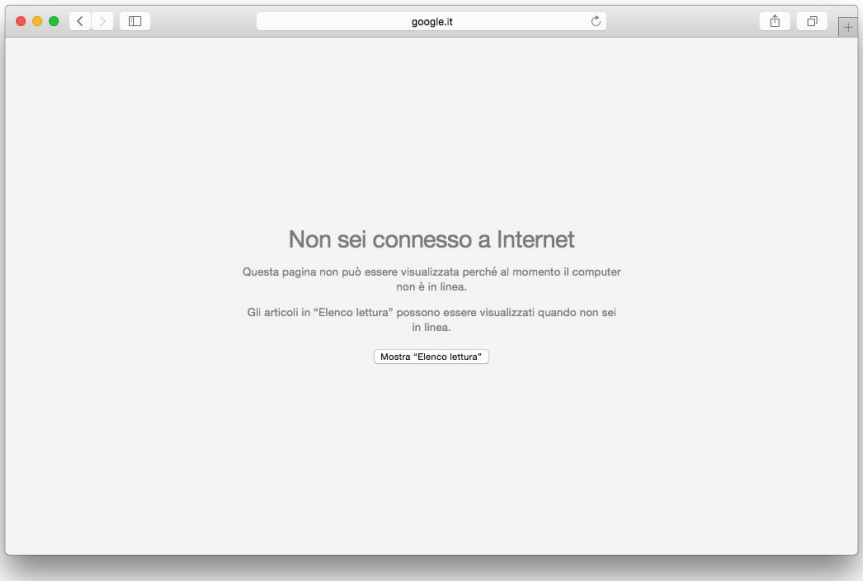
In questo capitolo elencheremo tutte le vulnerabilità individuate.

2.1 Uauthenticated full router backend access (Vodafone Station Consumer)

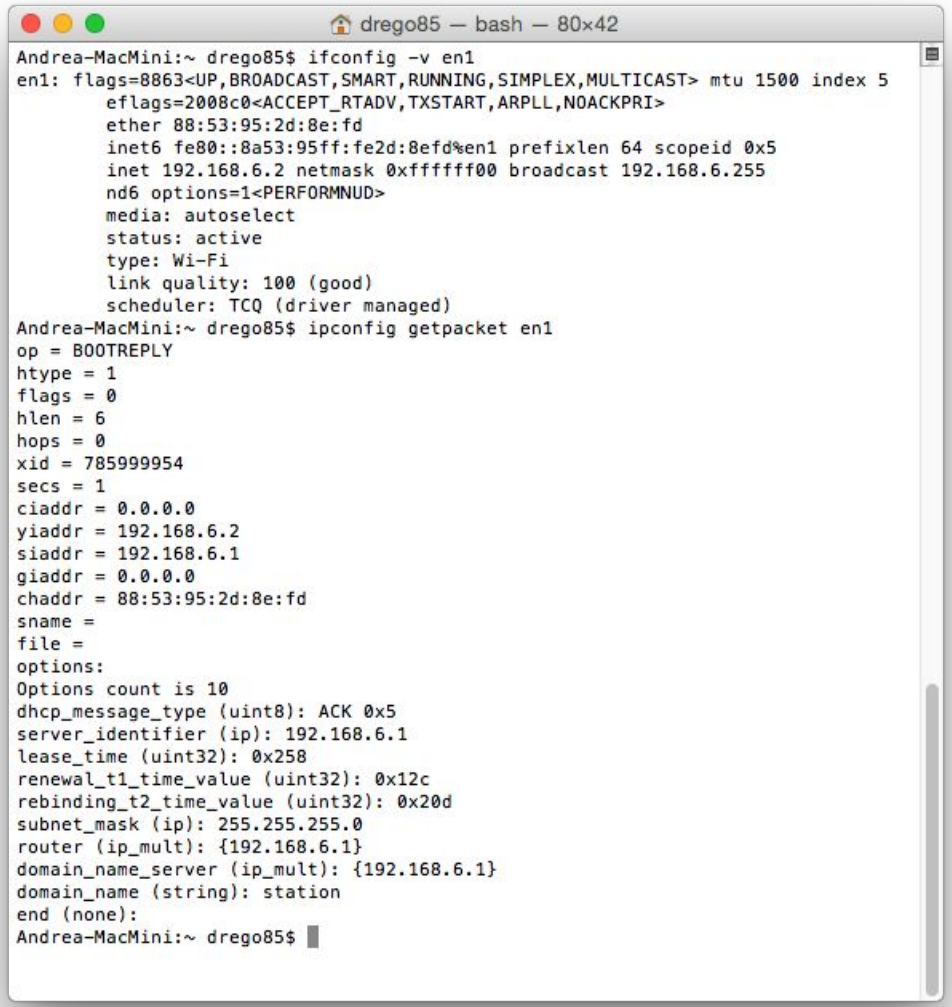
Accedendo alla rete Wireless dedicata alla Comunuty avente SSID “Vodafone-WiFi” e di libero accesso, appare automaticamente il Captive Portal che richiede l’autenticazione dell’utente.



Ignorando il Captive Portal e tentando di navigare su internet il browser ci avvisa che non abbiamo alcun collegamento ad internet e pertanto la navigazione non può proseguire.



Analizzando l'interfaccia di rete apprendiamo che la classe di IP assegnata ai clienti connessi al servizio Vodafone Comunity è diversa dalla classe assegnata all'abbonato, infatti quest'ultimo avrà la tradizionale classe 192.168.1.x mentre l'utente Guest avrà classe 192.168.6.x.

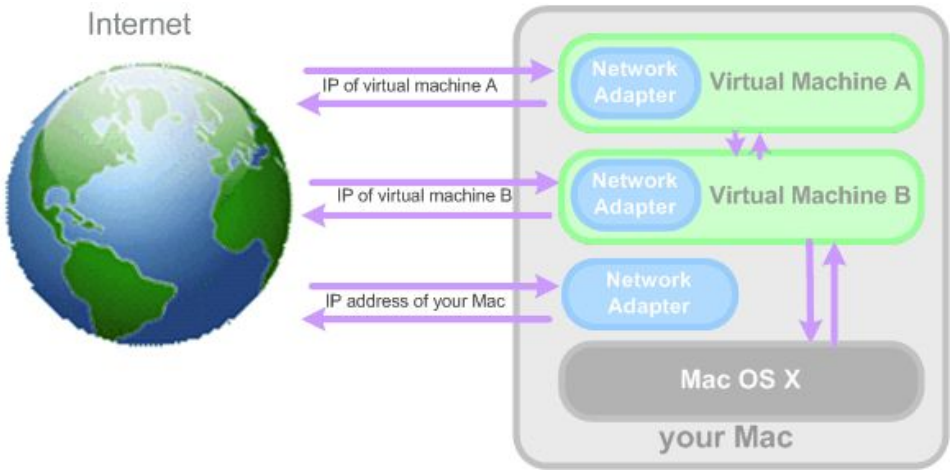


Dalla precedente immagine apprendiamo inoltre il MAC Address (88:53:95:2d:8e:fd) della macchina utilizzata per accedere alla rete WiFi Comunity di Vodafone, MAC Address che dovremo tenere a mente per apprendere al meglio la vulnerabilità della Vodafone Station.

Tentando infine di accedere all'indirizzo IP 192.168.1.1 per visualizzare il pannello di controllo della Vodafone Station la nostra richiesta viene automaticamente negata dal software e il browser ci farà visualizzare la seguente pagina di errore

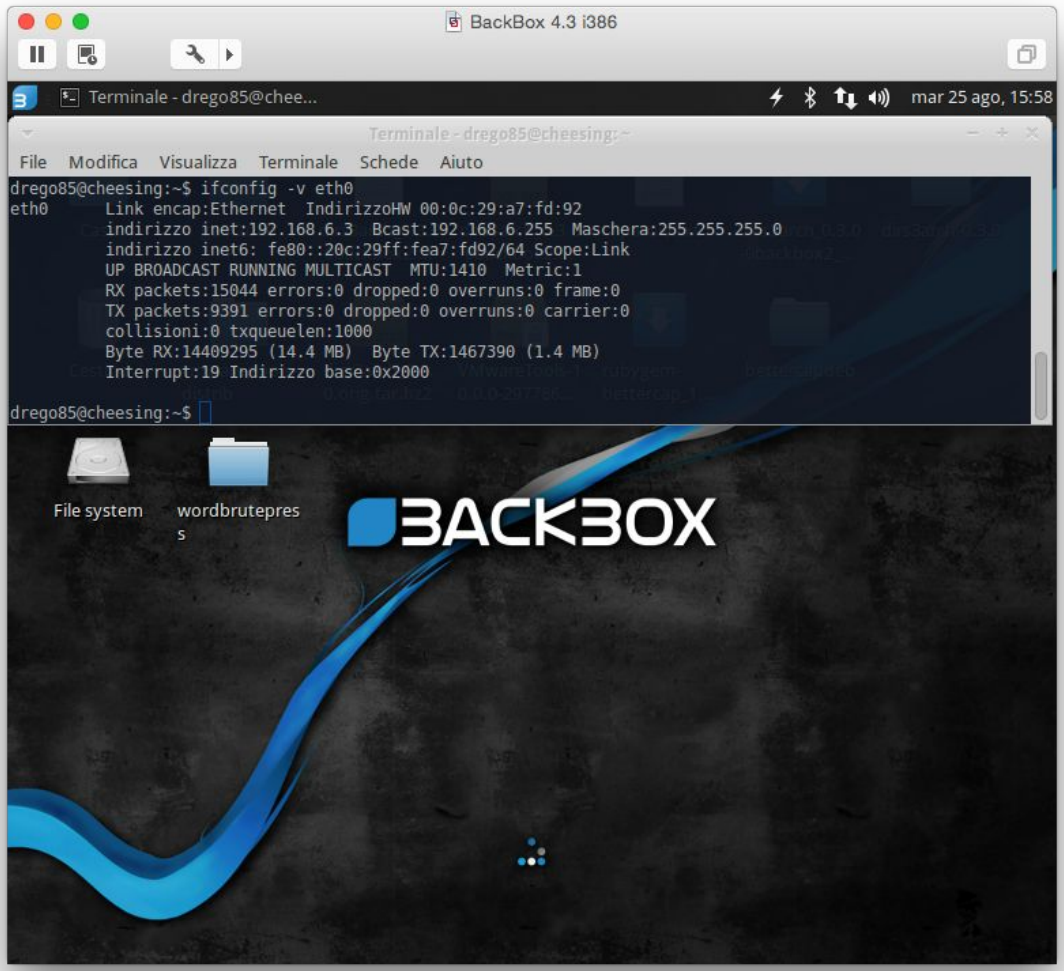
Il firmware della Vodafone Station ci impedisce correttamente l'accesso ad Internet se non paghiamo e alla pagina di configurazione del Router, ma cosa succede se il nostro MAC Address cambia inaspettatamente?

Abbiamo provato a simulare l'accesso ad Internet da una macchina virtuale in Bridge tramite la macchina fisica sullo stesso Network, come da seguente illustrazione[1].



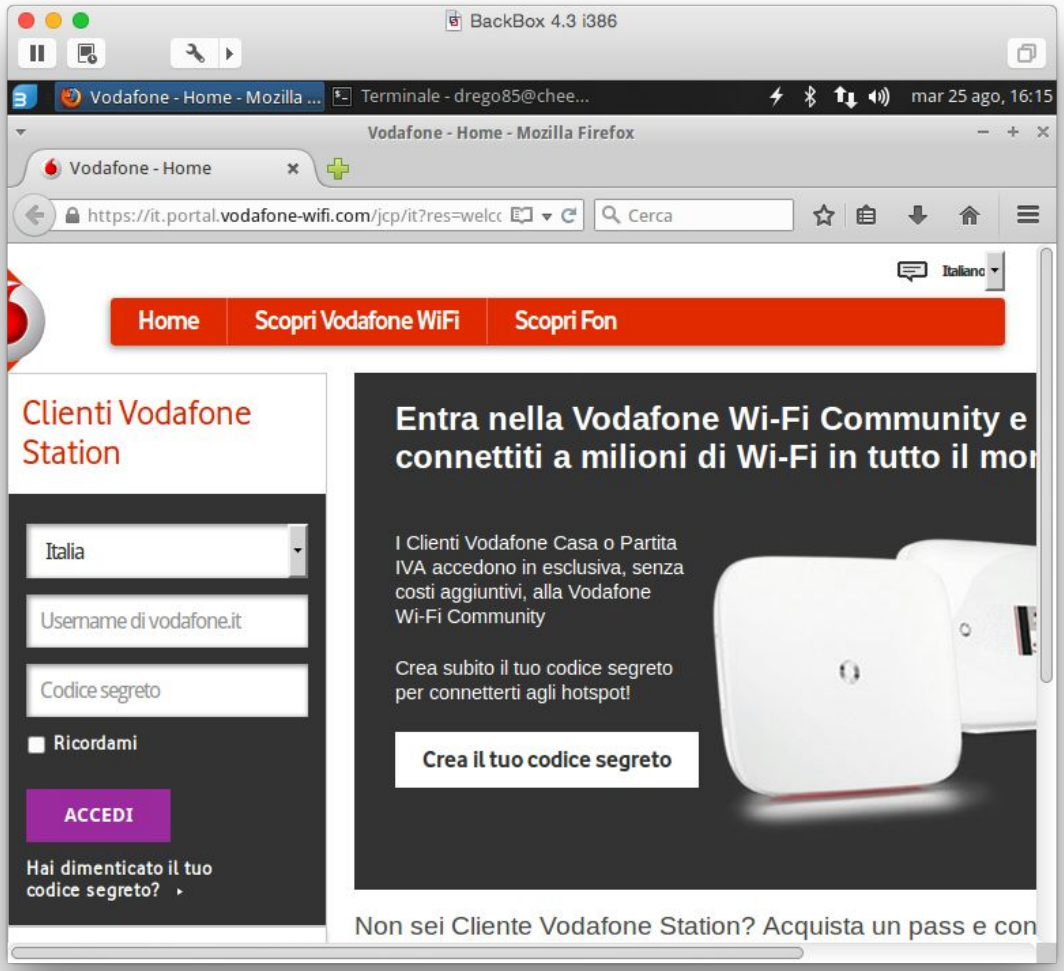
1. Fonte immagine Parallels IP Holdings GmbH.

In questa modalità il MAC Address della macchina fisica risulta primario rispetto a quello della macchina virtuale, pertanto la Vodafone Station bloccherà il traffico internet del MAC Address del PC fisico ma inaspettatamente non bloccherà totalmente il traffico generato dalla macchina virtuale.



La macchina virtuale ha quindi MAC Address diverso come vediamo dalla precedente immagine (00:0c:29:a7:fd:92) e ovviamente IP diverso.

Tentando di accedere ad internet veniamo automaticamente portati sul Captive Portal, confermandoci che comunque non possiamo accedere ad internet senza digitare le credenziali o pagare la quota oraria/giornaliera.

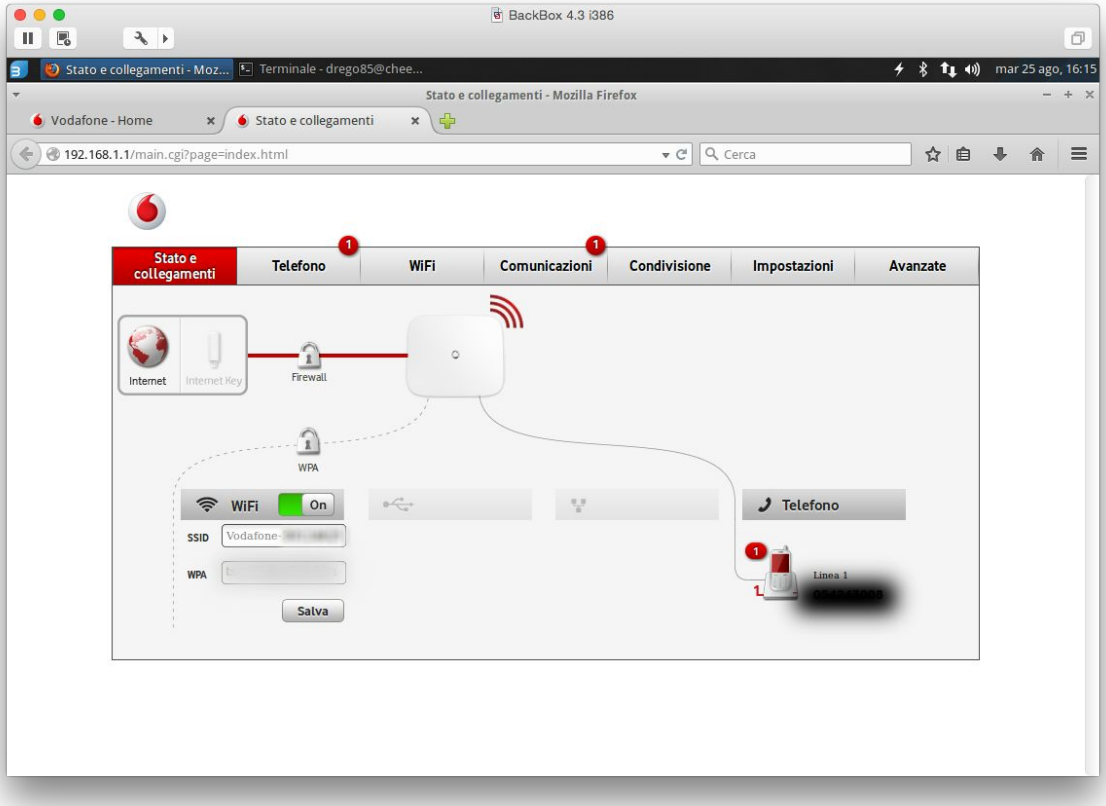


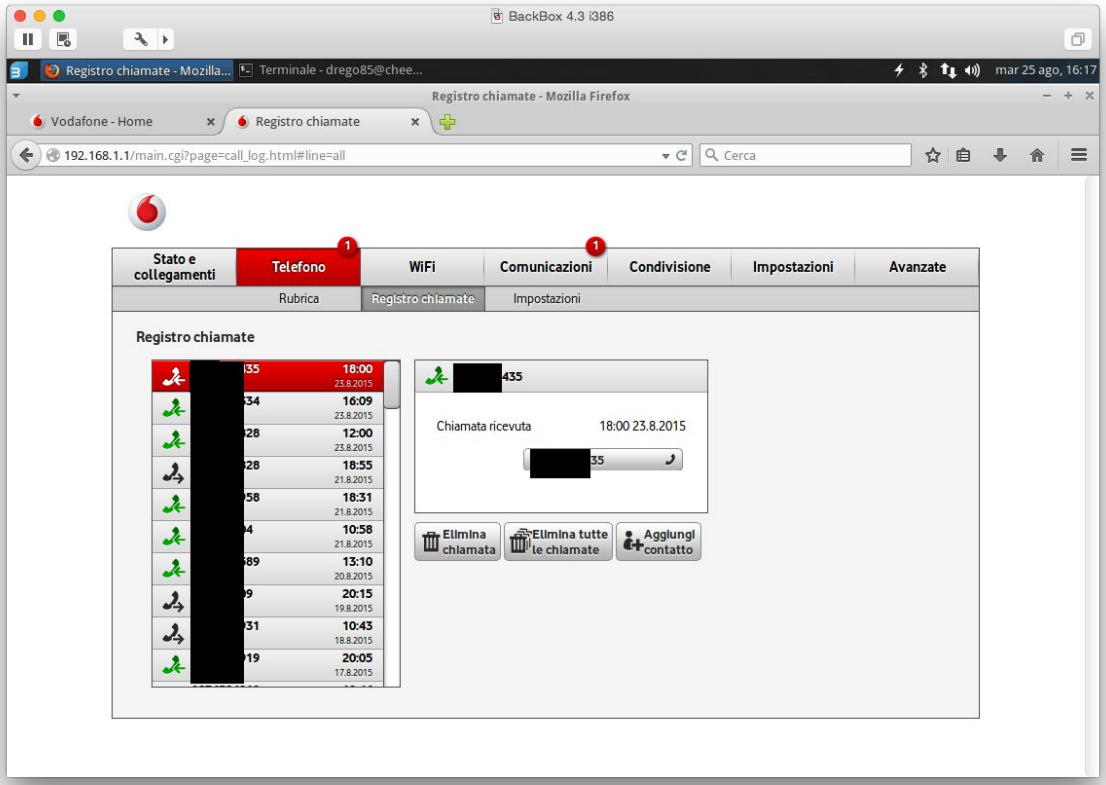
È invece possibile accedere alla pagina di configurazione del router, ovvero http://192.168.1.1. La totale assenza di un metodo di protezione predefinito (è possibile inserire manualmente in post-installazione una password per accedere al pannello di controllo) ci permette di visualizzare e modificare tutte le impostazioni della Vodafone Station.

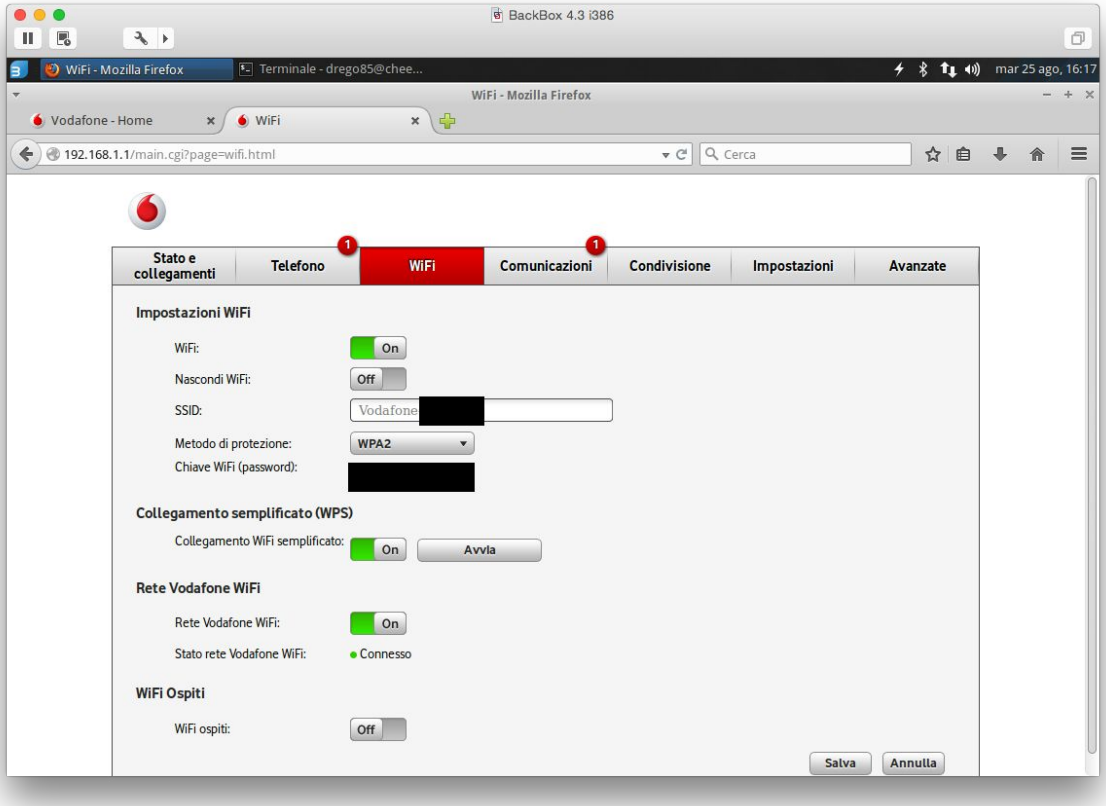
Ottenendo le credenziali della rete wireless dell'abbonato, siamo in grado di connetterci alla rete wireless a lui dedicata eludendo la richiesta di pagamento e navigando alla massima velocità offerta dalla sua linea. Possiamo inoltre analizzare il traffico di rete dell'abbonato per carpire credenziali, cronologia di navigazione, ecc, effettuare un attacco Man in the Middle, o se ha una chiavetta USB collegata al Vodafone Station accedere ai suoi file personali.

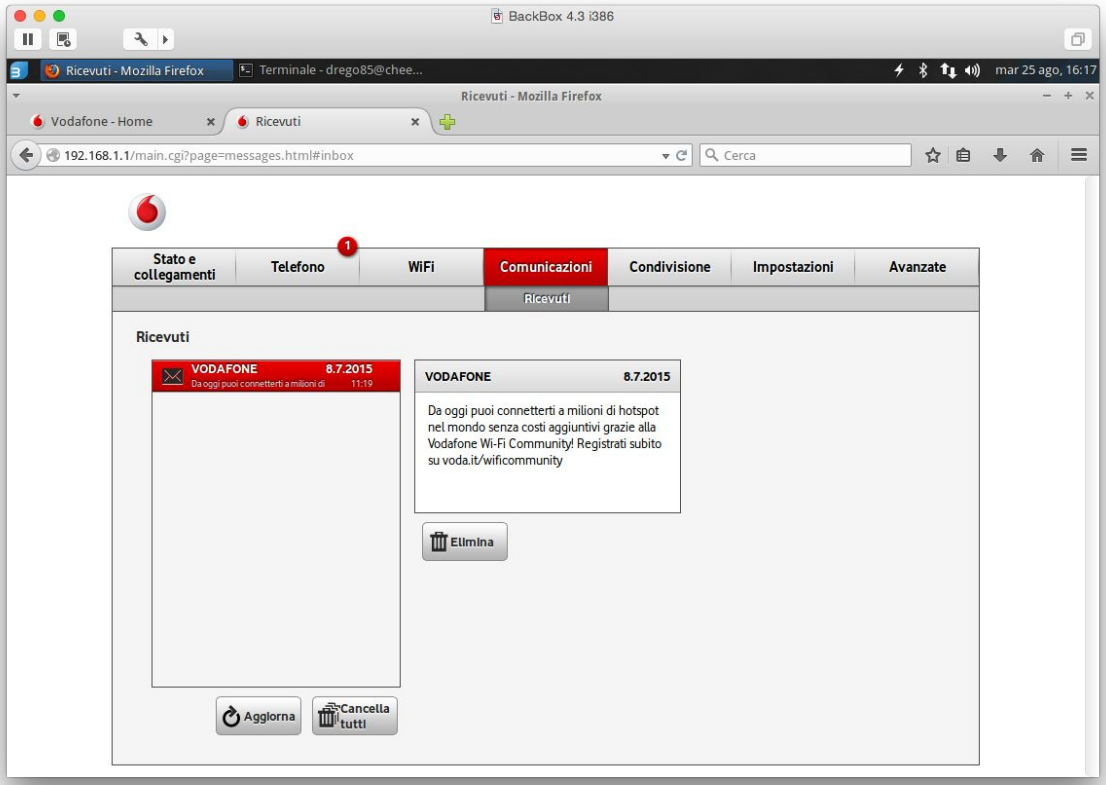
Un video dimostrativo della vulnerabilità è presente al seguente link: http://cloud.draghetti.it/owncloud/public.php?service=files&t=9ad91fa5e2f01ddc5bd3a3404f15d124

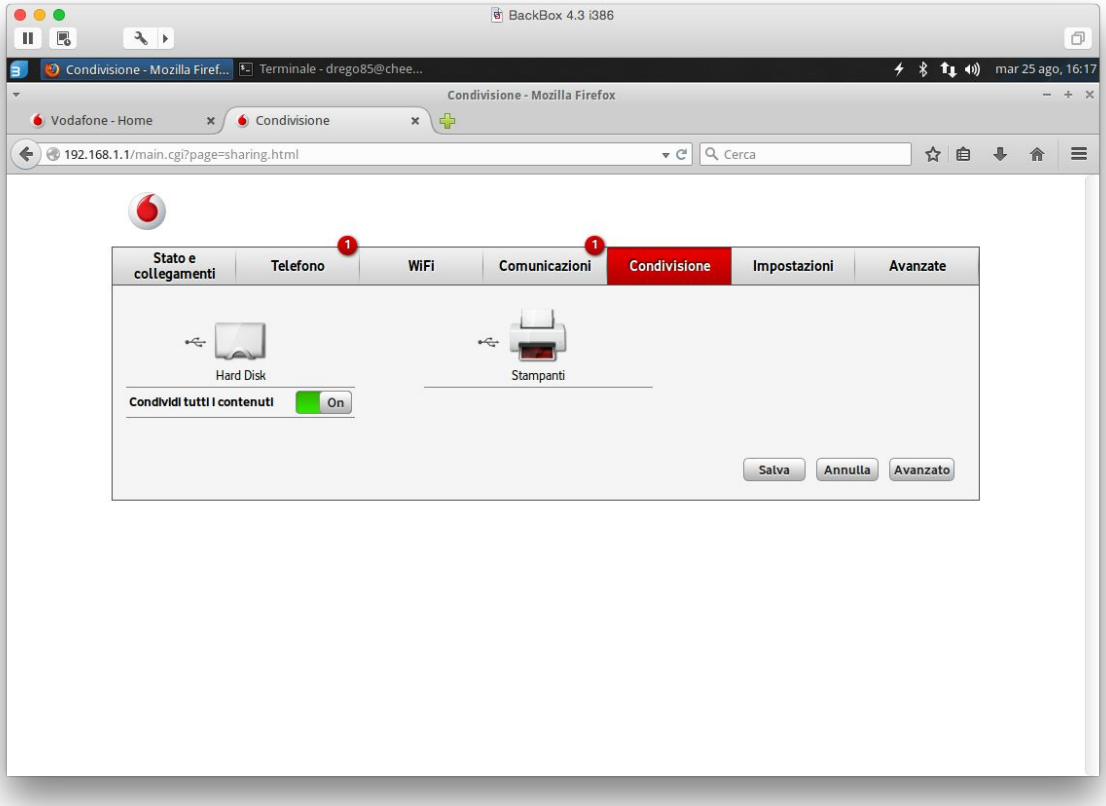
Le pagine che seguono mostrano una serie di screenshots del pannello di controllo del Vodafone Station, accessibile con il metodo descritto in precedenza.

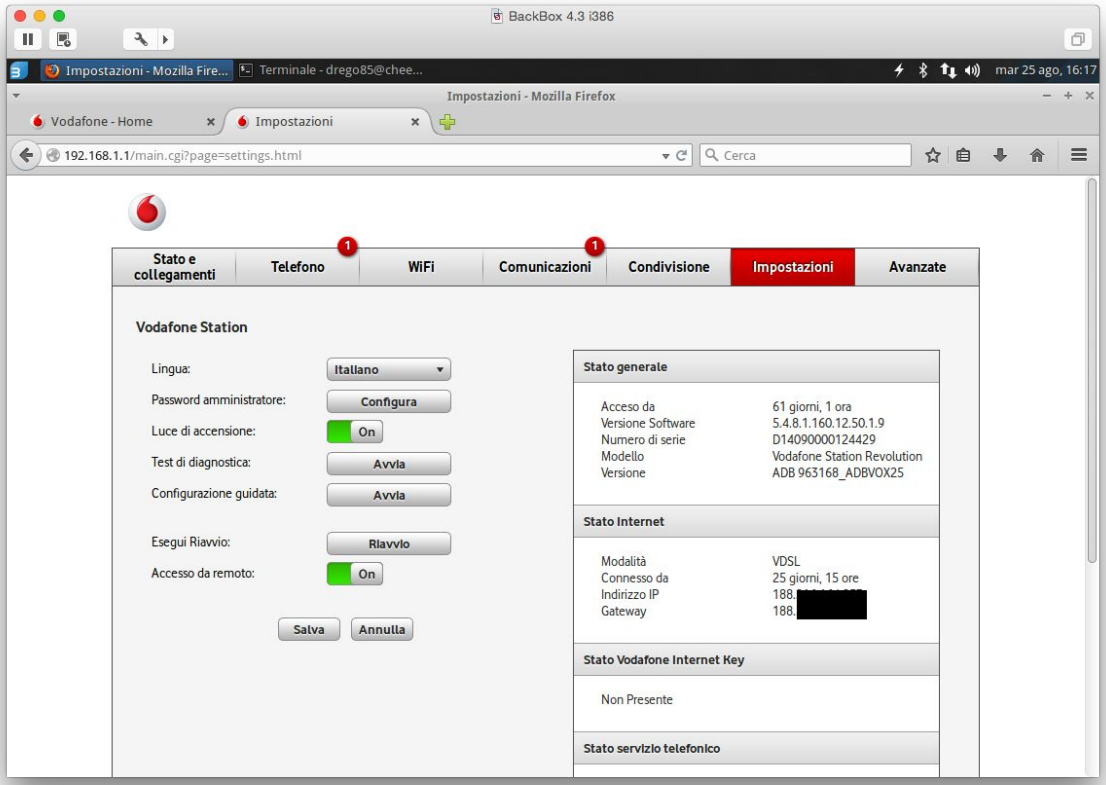

BackBox 4.3 i386
Stato e collegamenti - Moz...
Terminale - drego85@chee...
mar 25 ago, 16:15
Stato e collegamenti - Mozilla Firefox
Vodafone - Home
Stato e collegamenti
192.168.1.1/main.cgi?page=index.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Internet
Internet Key
Firewall
WPA
WiFi
On
SSID
Vodafone-
WPA
Salva
Telefono
Linea 1

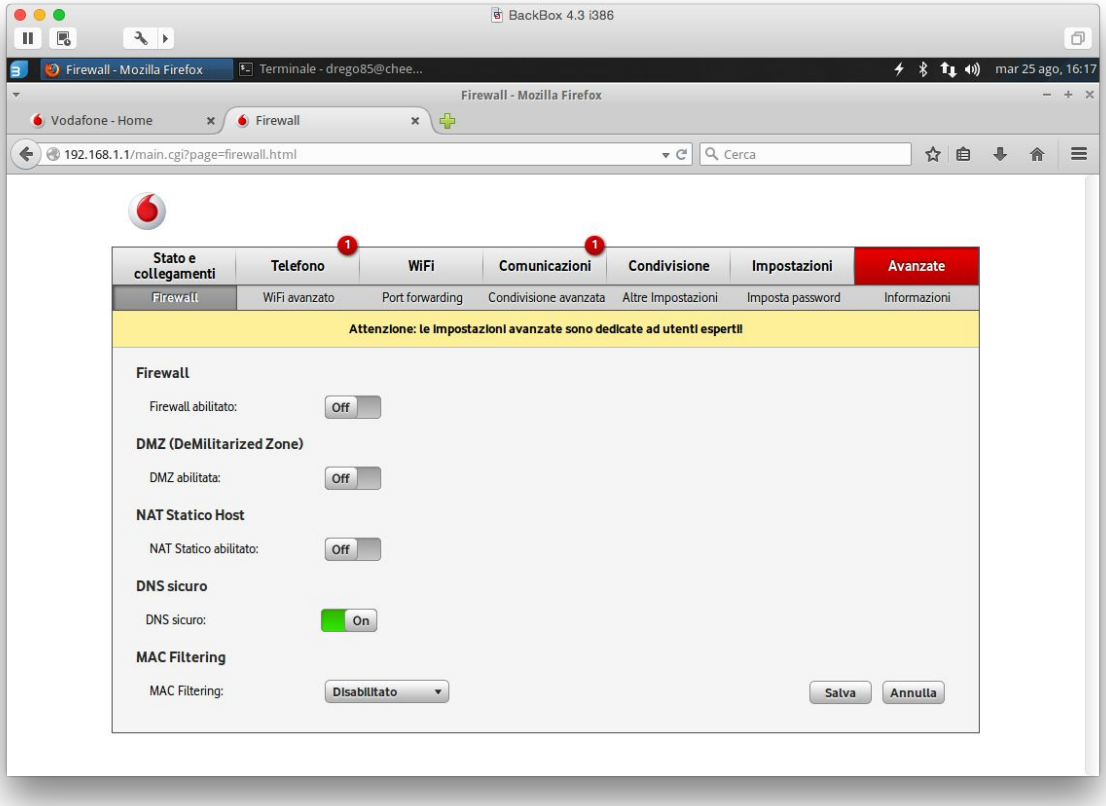

BackBox 4.3 i386
Registro chiamate - Mozilla...
Terminale - drego85@chee...
mar 25 ago, 16:17
Registro chiamate - Mozilla Firefox
Vodafone - Home
Registro chiamate
192.168.1.1/main.cgi?page=call_log.html#line=all
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Rubrica
Registro chiamate
Impostazioni
Registro chiamate
18:00 23.8.2015
16:09 23.8.2015
12:00 23.8.2015
18:55 21.8.2015
18:31 21.8.2015
10:58 21.8.2015
13:10 20.8.2015
20:15 19.8.2015
10:43 18.8.2015
20:05 17.8.2015
Chiamata ricevuta
18:00 23.8.2015
Elimina chiamata
Elimina tutte le chiamate
Aggiungi contatto

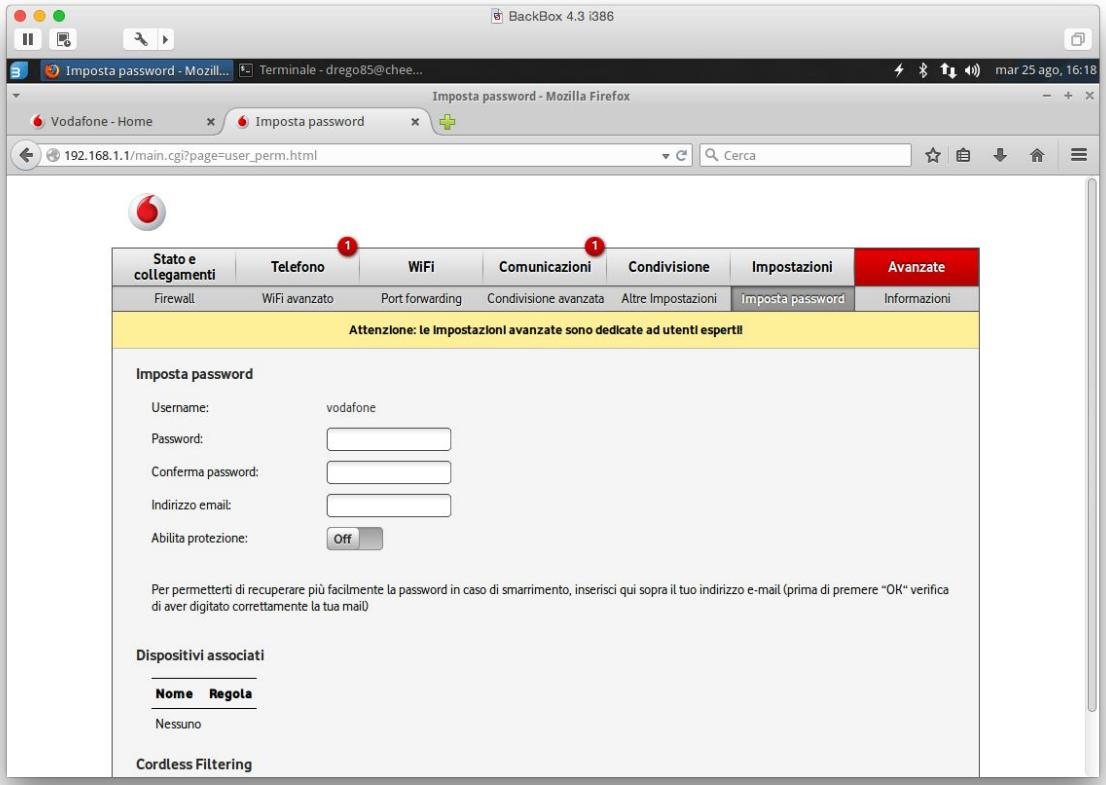

BackBox 4.3 i386
WiFi - Mozilla Firefox
Terminale - drego85@chee...
mar 25 ago, 16:17
WiFi - Mozilla Firefox
Vodafone - Home
WiFi
192.168.1.1/main.cgi?page=wifi.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Impostazioni WiFi
WiFi:
On
Nascondi WiFi:
Off
SSID:
Vodafone
Metodo di protezione:
WPA2
Chiave WiFi (password):
Collegamento semplificato (WPS)
Collegamento WiFi semplificato:
On
Avvia
Rete Vodafone WiFi
Rete Vodafone WiFi:
On
Stato rete Vodafone WiFi:
Connesso
WiFi Ospiti
WiFi ospiti:
Off
Salva
Annulla


BackBox 4.3 i386
Ricevuti - Mozilla Firefox
Terminale - drego85@chee...
mar 25 ago, 16:17
Ricevuti - Mozilla Firefox
Vodafone - Home
Ricevuti
192.168.1.1/main.cgi?page=messages.html#inbox
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Ricevuti
Ricevuti
VODAFONE
8.7.2015
Da oggi puoi connetterti a milioni di
11:19
VODAFONE
8.7.2015
Da oggi puoi connetterti a milioni di hotspot nel mondo senza costi aggiuntivi grazie alla Vodafone Wi-Fi Community! Registrati subito su voda.it/wificommunity
Elimina
Aggiorna
Cancella tutti


BackBox 4.3 i386
Condivisione - Mozilla Firef...
Terminale - drego85@chee...
mar 25 ago, 16:17
Condivisione - Mozilla Firefox
Vodafone - Home
Condivisione
192.168.1.1/main.cgi?page=sharing.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Hard Disk
Stampanti
Condividi tutti i contenuti
On
Salva
Annulla
Avanzato


BackBox 4.3 i386
Impostazioni - Mozilla Fire...
Terminale - drego85@chee...
mar 25 ago, 16:17
Impostazioni - Mozilla Firefox
Vodafone - Home
Impostazioni
192.168.1.1/main.cgi?page=settings.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Vodafone Station
Lingua:
Italiano
Password amministratore:
Configura
Luce di accensione:
On
Test di diagnostica:
Avvia
Configurazione guidata:
Avvia
Esegui Riavvio:
Riavvio
Accesso da remoto:
On
Salva
Annulla
Stato generale
Acceso da
61 giorni, 1 ora
Versione Software
5.4.8.1.160.12.50.1.9
Numero di serie
D14090000124429
Modello
Vodafone Station Revolution
Versione
ADB 963168_ADBVOX25
Stato Internet
Modalità
VDSL
Connesso da
25 giorni, 15 ore
Indirizzo IP
188.
Gateway
188.
Stato Vodafone Internet Key
Non Presente
Stato servizio telefonico

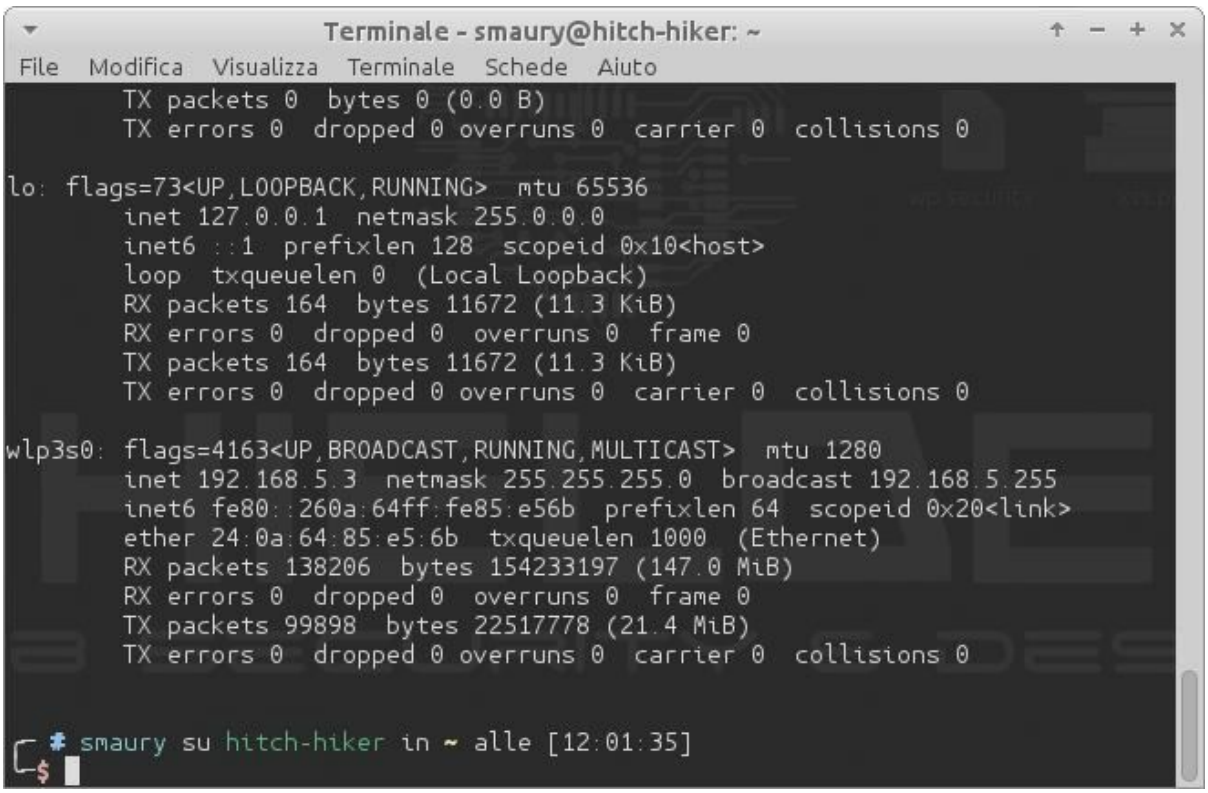

BackBox 4.3 i386
Firewall - Mozilla Firefox
Terminale - drego85@chee...
mar 25 ago, 16:17
Vodafone - Home
Firewall
192.168.1.1/main.cgi?page=firewall.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Firewall
WiFi avanzato
Port forwarding
Condivisione avanzata
Altre Impostazioni
Imposta password
Informazioni
Attenzione: le impostazioni avanzate sono dedicate ad utenti esperti!
Firewall
Firewall abilitato:
Off
DMZ (DeMilitarized Zone)
DMZ abilitata:
Off
NAT Statico Host
NAT Statico abilitato:
Off
DNS sicuro
DNS sicuro:
On
MAC Filtering
MAC Filtering:
Disabilitato
Salva
Annulla


BackBox 4.3 i386
Imposta password - Mozill...
Terminale - drego85@chee...
mar 25 ago, 16:18
Imposta password - Mozilla Firefox
Vodafone - Home
Imposta password
192.168.1.1/main.cgi?page=user_perm.html
Cerca
Stato e collegamenti
Telefono
WiFi
Comunicazioni
Condivisione
Impostazioni
Avanzate
Firewall
WiFi avanzato
Port forwarding
Condivisione avanzata
Altre Impostazioni
Imposta password
Informazioni
Attenzione: le impostazioni avanzate sono dedicate ad utenti esperti!
Imposta password
Username:
vodafone
Password:
Conferma password:
Indirizzo email:
Abilita protezione:
Off
Per permetterti di recuperare più facilmente la password in caso di smarrimento, inserisci qui sopra il tuo indirizzo e-mail (prima di premere "OK" verifica di aver digitato correttamente la tua mail)
Dispositivi associati
Nome
Regola
Nessuno
Cordless Filtering

2.2 Uauthenticated full router backend access (Vodafone Station Corporate)

Nonostante esteticamente le Station siano identiche il firmware della versione Business differisce da quello Consumer, anche SSID delle reti guest è differente, ovvero: “Vodafone-Guest”.

Su questo modello la funzionalità di WiFi Guest non è infatti nata con lo scopo di “subaffittare” la propria linea, ma di dare la possibilità ai clienti di navigare in rete attraverso la propria connessione, separandoli però in una subnet dedicata, dalla quale non dovrebbe essere possibile effettuare richieste all’indirizzo ip che viene risolto digitando http://vodafone.station.

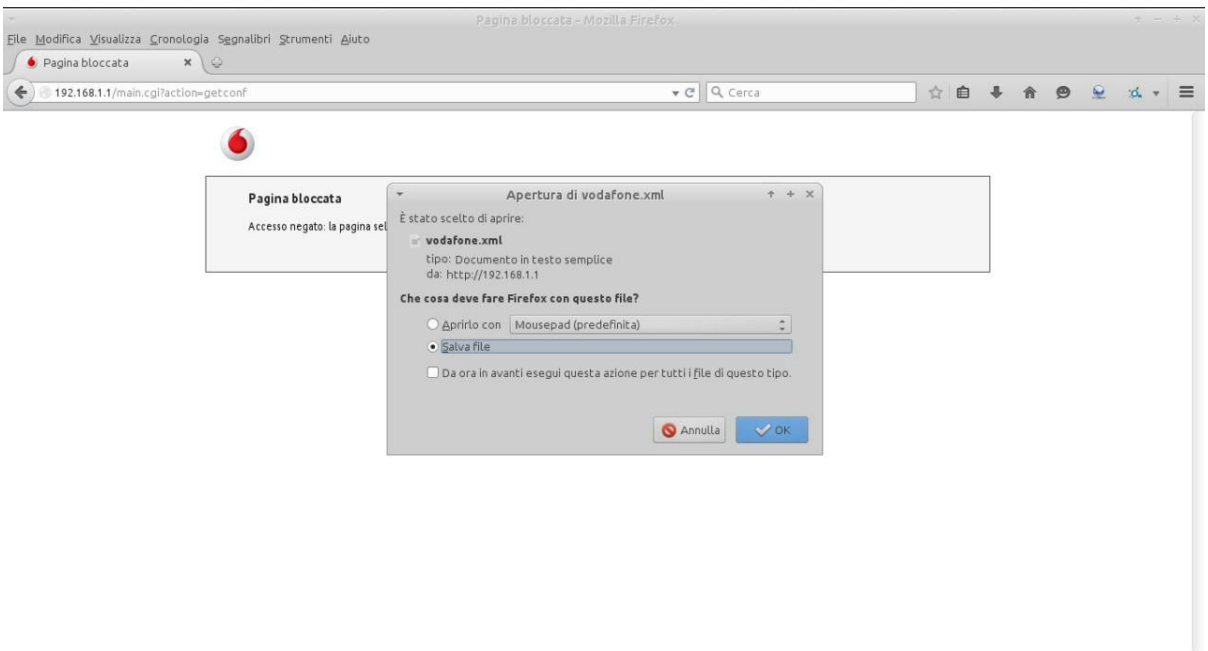


Collegandosi alla rete WiFi Guest della Vodafone Station Business otterremo un indirizzo IP della classe 192.168.5.x differente dal 192.168.1.x standard per gli utenti legittimi.

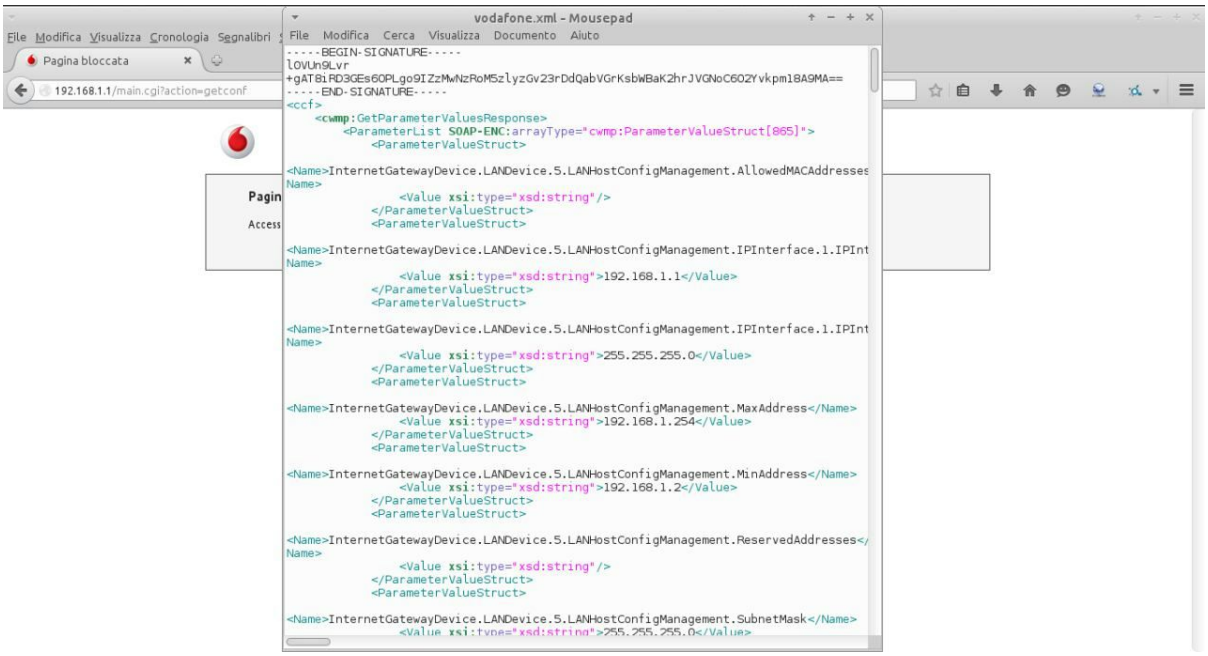
Sarà quindi impossibile accedere al pannello di controllo della Vodafone Station dalla rete Guest digitando l’indirizzo http://192.168.1.1, come possiamo visualizzare nella successiva immagine.

È però possibile scaricare il file di configurazione delle impostazioni della Vodafone Station, file XML contenente tutti i parametri in chiaro tra i quali troviamo:

- SSID
- Chiave WPA e WEP
- Registro Chiamate
- Dettaglio utenza (numero di telefono, comunicazioni, ecc)



Ottenuta quindi la chiave WPA dal file XML è possibile collegarsi alla rete WiFi dell'abbonato eludendo qualsiasi restrizione. È inoltre possibile analizzare il traffico di rete tramite un attacco Man in The Middle.



3. Conclusioni

Attraverso la rete wireless dedicata agli ospiti, è possibile ottenere pieno accesso alla rete wireless primaria.

Questa violazione permette a un attaccante di anallizzare il traffico di rete, effettuare attacchi Man In The Middle o di avere accesso diretto alle risorse di rete (stampanti, NAS, telefoni VoIP, ecc.) dell'abbonato.

4. Appendice

4.1 Tools

Per effettuare questa analisi abbiamo utilizzato:

- Macchina Fisica (Mac OS X)
- Macchina Virtuale (BackBox Linux)

In alternativa si può sfruttare un Range Extender, in modo da avere due diversi indirizzi MAC.

4.2 Firmware Vodafone Station

Abbiamo analizzato i seguenti firmware di Vodafone Station:

Software Version	Model	Hardware Version
5.4.8.1.160.8.51.2.1	Vox 1.5	SerComm SHG1500 (LCDv6, WiFi-RFv3)
5.4.8.1.160.12.50.1.9	Vodafone Station Revolution	ADB 963168_ADBVOX25
5.4.8.1.160.8.62.1.4	Vox 1.5	SerComm SHG1500 (LCDv2, WiFi-RFv2)
5.4.8.1.160.12.56.1.28	Vodafone Station Revolution	ADB 963168_ADBVOX25

4.3 About People

I test sono stati condotti da:

- Andrea Draghetti;
- Stefano Valentini;
- Abdel Adim Oisfi.