Foreman - Bug #1208

Unauthenticated IP spoofing should not be allowed

10/04/2011 08:49 AM - Marcello de Sousa

Status:	Closed		
Priority:	Normal		
Assignee:	Ohad Levy		
Category:	Unattended installations		
Target version:	0.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

Now any server can spoof and get a kickstart file that might have interesting info (such as root password hash). This can be considered a security weakness as you shouldn't be allowed to spoof IPs unauthenticated anyway.

Next to that, as a workaround for #969, I've been forced to filter the allowed URLs in my apache config file (/etc/httpd/conf.d/foreman.conf - Check template sample below).
There is one important issue though. This won't match query strings such as **"?spoof="** giving me one more reason for this request.

```
 <Location />
    Order Deny,Allow
    Deny from all
    <% scope.lookupvar('foreman::params::allowed_ips').split(',').each do |ip| -%>
    Allow from <%= ip %>
    <% end -%>
    Allow from 127.0.0.1
    Allow from <%= ipaddress %>
  </Location>
  <Location ~ "^/unattended/(kickstart|built)$" >
    Order Deny,Allow
    Deny from all
    <% scope.lookupvar('foreman::params::unattended_allowed_ips').split(',').each do |ip| -%>
    Allow from <%= ip %>
    <% end -%>
  </Location>
```

Related issues:

Related to Smart Proxy - Feature #969: Direct Client->Foreman communication s...	**Closed**	**06/09/2011**

Associated revisions

Revision 224783a1 - 10/25/2011 11:02 AM - Ohad Levy

fixes #1208 - Unauthenticated IP spoofing should not be allowed

History

#1 - 10/04/2011 11:21 AM - Marcello de Sousa

...and if auth required, via HTTPs only of course.

#2 - 10/25/2011 11:22 AM - Ohad Levy

- Status changed from New to Closed

- % Done changed from 0 to 100

Applied in changeset 224783a1d0926b8d78d0e03aaf2ff4e856ae3aa7.