Hardening em rede wireless

21 de abril de 2015 / Fnkoc

Bom galera, hoje iremos falar sobre hardening em rede wireless. Irei apresentar algumas ações que acho interessante para tornar sua rede wireless mais segura. Não irei demonstrar como realizar as mudanças na prática porque cada roteador tem uma configuração então isso faria o post limitado a um determinado modelo de roteadores. Irei fazer uma enumeração das mudanças que irei abordar

Para quem quiser se aprofundar mais eu irei deixar links que podem ser úteis

1. Utilizar uma criptografia WPA2-PSK
2. Desabilitar o WPS
3. Mudar o nome da rede
4. Esconder a rede
5. Realizar um filtro por MAC
6. Mudar a senha do administrador
7. Desabilitar o gerenciamento por dispositivo conectado a rede

WPA2 – Wi-Fi Protected Access II:

É sistema padrão atual e também o mais seguro, implementado pela Wi-Fi Alliance em 2006. Ele lida com senhas e algoritmos de uma meneira que exclui completamente a possibilidade de um ataque de força bruta. Sendo assim, esse é o tipo mais seguro da atualidade. Segundo especialistas, risco de intrusões para usuários domésticos com WPA2 é praticamente zero.

http://canaltech.com.br/o-que-e/seguranca/O-que-e-WPA2/

WPS – WI-FI Protected Setup:

É uma opção que permite ao usuário uma maneira mais fácil de configurar e conectar seus dispositivos ao roteador. O WPS foi uma ótima idéia porém ele coloca em risco os roteadores ao ataque de força bruta (brute-force) um vez o ataque visa PIN do roteador

http://www.howtogeek.com/176124/wi-fi-protected-setup-wps-is-insecure-heres-why-you-should-disable-it/

Mudar o nome da rede:

O motivo de julgar isto necessário é porque normalmente o nome da rede (ESSID) do roteador é também o modelo dele, dando assim informações para um potencial atacante. Sabendo o modelo o atacante pode procurar por falhas específicas naquele modelo.

Esconder a rede:

Ninguém ataca aquilo que não se pode ver, não é mesmo? É claro que existem ferramentas que descobrem estas redes, porém é mais difícil alguém procurar por redes ocultas uma vez que o que mais tem são redes WIFI.

Filtro por MAC:

Isto é uma medida mais radical uma vez que limita os dispositivos que podem ser conectados a rede. Para acessar a rede é necessário que o MAC Address do seu dispositivo – smartphone por exemplo – esteja cadastrado e com acesso permitido.

Senha do administrador:

Maioria dos roteadores vem com a senha e usuários “admin”, portanto mudar é uma excelente escolha.

Gerenciamento por rede wireless:

Essa opção é para prevenir que caso o atacante obtenha sucesso em se conectar a sua rede ele não consiga mudar as configurações do roteador e fazer com que você perca o acesso a sua própria rede. Sendo assim só será possível alterar as configurações quando conectado ao roteador via cabo.

Gerenciamento remoto

Essa opção é muito usada por administradores de rede, para que os mesmos possam modificar as configurações do roteador sem ter que se deslocar até o local. O problema é que isso permite que qualquer pessoa tenha acesso a página de login do roteador.
Normalmente se usa a porta 8080 então caso queira ver exemplos bastar utilizar um range de ip e

passar o nmap filtrando na porta 80

```
nmap -p 8080 -sC 192.168.0.0/24
## onde -p é a porta
## -sC é para utilizar os NSE
## 192.168.0.0/24 seria o range de IP. (/24 se refere a mascara de subrede)
```

Espero que tenham gostado. Qualquer dúvida só nos contatar aqui, no grupo ou na página. FUI!