Who is sending MESSAGE

2nd Hack The Pods Write-up

問題概要

問題文

うわぁ！誰かがブロードキャストで呼びかけている！？

むむ...何だこのメッセージは...？

概要

150点 - Network

呼びかけのメッセージを読んでFlagを得るのが目的

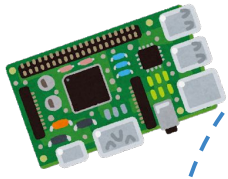
ブロードキャストで呼びかけられているらしい

Azure

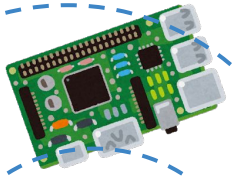
CTFd

VM

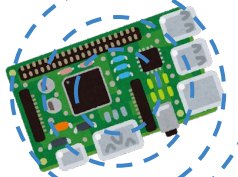
インターネット



problem-server



problem-server2



hidden-server

問題用ネットワーク

secprj-netgear

問題用ネットワーク
にのみブロードキャスト

User

ブロードキャストで呼び掛けられてる

らしいので，とりあえず問題ネットワークでパケットキャプチャしてみ

とりあえずブロードキャストならUDPだとアタリをつけてフィルタリング

実際ブロードキャストパケットはまあまあるが，中身が読めるものを探す

ブロードキャストで呼び掛けられてる

らしいので，とりあえず問題ネットワークでパケットキャプチャしてみ

とりあえずブロードキャストならUDPだとアタリをつけてフィルタリング

実際ブロードキャストパケットはまあまあるが，中身が読めるものを探す

```
  4 3.006536    192.168.0.8       255.255.255.255   UDP        73 60287 → 40630 Len=41
```

と，こんな感じのパケットが見つかる

ブロードキャストで呼び掛けられてる

```
   4 3.006536     192.168.0.8       255.255.255.255   UDP       73 60287 → 40630 Len=41
```

中身には == MESSAGE: plz check 10080 port on me == というメッセージ

```
0000  02 00 00 00 45 00 00 44  4f 92 00 00 40 11 6a 67   ····E··D O···@·jg
0010  c0 a8 00 08 ff ff ff ff  f4 71 9e b6 00 30 c0 f1   ········ ·q···0··
0020  3d 3d 20 4d 45 53 53 41  47 45 3a 20 70 6c 7a 20   == MESSA GE: plz
0030  63 68 65 63 6b 20 38 30  30 38 20 70 6f 72 74 20   check 80 08 port
0040  6f 6e 20 6d 65 20 3d 3d                           on me ==
```

送信元IPアドレスの8008ポートを見に行く

こんな感じのFlagのみが置かれたWebページが見られる

htp-ctf{We_are_Alians...}

おきもち

問題ネットワークが外に出られないと決まった時点で100点にすべきだった問題

本来は外と繋がった環境で目当てのブロードキャストパケットを探す問題だった

外に出ないラズパイ３台とクライアント数台が繋がっただけのLANなんて
大したトラフィックがあるわけもない

リアルネットワークを活かせるのがオンサイトCTFの強みなので
どんどんこういう問題作っていきたいよね