

Testing the Security of Devices within -a Home Network (HN)

Samuel Richards (1901717)

School of Applied Computing, Faculty of Architecture, Computing and Engineering, University of Wales Trinity St David, IQ, Swansea, SA1 8EW, Email: 1901717@student.uwtsd.ac.uk

1 - Introduction

In recent years Hacking has become a serious problem, especially with Covid happening and everyone has been working from home. This project is being conducted to show how easy/hard it is for a hacker to gain access to devices within a home network, in which 3 devices have been choosing which are a WAP (wireless access-point), Computer and smart phone.

```
File Actions Edit View Help
--SecKCoin++e.AMd'      --://///hbove.913.ElsMNH+-
--/.ssh/id_rsa.Des-      'htN01UserWroteMe!-
:dopeAW.No<nano>o        :is:TRIKC.sudo-.A:
:we're.all.alike'        The.PFYroy.No.D7:
:PLACEDRINKHERE!        yxp_cmdshell.Ab0:
:msf>exploit -j.         :Ns.B0B8ALICEes7:
:--srwxrwx-.            'MS146.52.No.Per:
:<script>.Ac816/         sENbove3101.404:
:NT_AUTHORITY.Do        'T:/shSYSTEM-.N:
:09.14.2011.raid        /STFU|wall.No.Pr:
:hevnsntSurb025N.       dNVRGOING2GIVUUP:
:#OUTHOUSE- -s:        /corykennedyData:
:$nmap -oS              SSo.6178306Ence:
:Awsm.da:              /shMTL#beats3o.No.:
:Ring0:                dDestRoyREXKC3ta/M:
:23d:                  sSETEC.ASTRONOMYist:
:/-                    /yo-
                        .ence.N:(){ :|: 6 ;;
                        :Shall.We.Play.A.Game?tron/
                        --ooy.ifightf0r+ehUser5'
                        ..th3.H1V3.U2VjRFNN.jMh+.
                        MjM--WE.ARE.se--MMjMs
                        --KANSAS.CITY's--
                        J--HAKCERS--./-
                        .esc:wq!:-
                        +++ATH'

-[ metasploit v6.0.50-dev ]
+ -- --[ 2144 exploits - 1142 auxiliary - 365 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 8 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
```

Figure 2 – MetaSploit

3 – Research

Research was conducted within multiple aspects in order to gain a high level of knowledge to complete this project. In order to doo this project I had to improve my knowledge within hacking such as tools used for certain scenarios, for example “Fern WIFI Cracker” being used within Routers and Wireless Access Points, and MetaSploit being used to hack computer and smart phones. Improvement was needed with knowing the weaknesses of each device and so on.



Figure 3 – Oracle VM



Figure 4 – Kali Linux

5 - Conclusion

Overall the project was a success, this conclusion is based off of the result, which were three successful hacks. The aims and objectives set for this project were achieved. The hacker was able to gain access to the three devices (WAP, Computer and Smart Phone) and were able to exploit them further.

Opportunities for improvements for further attacks would be to use other tools, explore further because only pre-installed tools were used within this project, and having anti-virus software would have made the hack more challenging, that is another improvement which could be used for future purposes.



Figure 1 – Fern WIFI Cracker

2 - Aims & Objectives

The aim of this research is to attempt to hack a HN to test the security features of the system and devices in order to find and exploit vulnerabilities.

The main objectives are as followed: -

Perform a review of existing research on HN, Smart devices, the security features which are involved, and hacking tools and software which are used in hacking such networks.

Create a hybrid virtual/physical network with connected physical HN devices.

Attempt to find and exploit vulnerabilities within the home network using the chosen tools and methods and report the results.

Offer recommendations for securing HN based on findings.

4 – Implementation

This project was done within a virtual network (Oracle VM VirtualBox) using Kali Linux as a operating system, the reason for this is because Kali Linux comes with pre-installed tools in which they were used (Fern WIFI Cracker and MetaSploit).