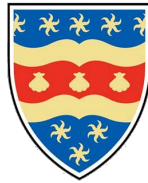


Analyzing and Improving Brown-Raths Security and Network Architecture

Osbourne Clark



**UNIVERSITY OF
PLYMOUTH**

Plymouth University
United Kingdom
1st March 2023

Contents

1	introduction	2
2	solving security problem	2
2.1	Preventing phishing attacks	3
2.1.1	Network level protection	3
2.1.2	Client side protection	3
2.1.3	User education	3
3	networking	4
3.1	explain why the network speed is low and if the issues is inside or outside the intranet	4
3.1.1	Ping	4
3.1.2	trace route	4
3.2	purpose new network architecture to allow for more security and expandability	5
3.2.1	IDS (intrusion detection system)	5
3.2.2	firewalls	5
3.2.3	demilitarisation zone	5
4	conclusion	6



Figure 1: example phishing email

1 introduction

The retail company Brown-Rath is looking into their security and network infrastructure and is wanting to improve on both aspects. Improving the security of the company, particularly against phishing attacks, will prevent potential harm to: PII(personally identifiable information) such as card numbers, phone numbers, email addresses and house addresses , data theft, data erasure as well as preventing the company from breaching the UKs data protection act [7] which would, in the best scenario, lead to a 10 million euros fine or 2% worldwide annual turnover in the preceding financial year, which ever is highest [5]. The improved network side will come with the benefit of faster data transfer allowing for quicker access to websites, as well as increased speed of uploading and downloading allowing for information to be quickly transferred and shared both inside and out side the intranet. Another aspect on the network is to anticipate for growth of the company to ensure that the networks architecture is modular and can easily be added to without the reducing the performance of uploading and downing.

2 solving security problem

The company recently had a security scare where an employee was sent a phishing email. The email contained a promised prize draw to a sports game as well as gift certificates to several restaurants. While the email seemed to be tailed towards the employee as it had their favourite sports team and restaurant making it a spear phishing attack, it could have just included a team widely supported by people in that particular area. This would make sense as there were several restaurant and only one was the the employees favourite, this would classify the attack as a email phishing attack that uses a "spray and pray" technique. Common email phishing attacks that utilizes a "spray and pray" technique will use a generic email format that targets no one in particular. The attacker sends this email to a wide range of emails and hopes that at least one recipient will act upon the email.

Figure1 is an example email taken from "Phishing attacks: A recent comprehensive study and a new anatomy" [2] and is figure3 in the article.As you can see the email isn't directed at anyone particular, it is just addressed to "neighbour". This example can easily be fact checked as it contains broken grammar and if you know your neighbour you can ask, if you don't have a neighbour then you know its a phishing attack. Another tell tell sign in this email is that the sender has requested for payment to a bitcoin account. Bitcoins are commonly used by criminals and scammers when transferring money as there is no way to identify the sender or receivers, if this was somehow legitimate i would image they would ask for the money to be transferred using a more widely used method.

2.1 Preventing phishing attacks

This particular case involves a common phishing attack that takes advantage of a trojan. A trojan is a piece of malware that hides it self as legitimate software and will execute malicious code when executed. Techniques laid out in the article "A survey of phishing email filtering technique" [3] will help to prevent phishing attacks, techniques include: network level protection, authentication, client side tools, user education, and server side filters and classifiers. We'll focus on only 3 of the techniques but with thorough implementation would provide effective security protection, especially against phishing attacks. We'll look at network protection, client side tools and user education.

2.1.1 Network level protection

Network level protection involves: black listing ip addresses or white listing IP addresses. Both have different uses, advantages and disadvantages. The recommended one would be blacklisting. This would be the best approach for a retail company as they will want potential buyers to be able to access their website without need to ask for permission first , as this is what will be needed for whitelisting. Black-listing can be tiresome as you would need to add IP address that aren't allowed into the network, but with online resources and automation a list of blacklisted IP addresses can be automatically implemented, saving your time and knowing that a majority of nuisance IP address are going to be blocked.

	advantages	disadvantages
black listing	only need to block the IP address that are from malicious, or nuisance entities	a ever grow list will form as more and more IP address will need to put onto the blacklist
white listing	only allows in verified IP address, no need to manually stop other address from coming in as they are automatically filters	need to manually put IPS into whitelist so they can enter the network

Table 1:

2.1.2 Client side protection

Client side protection can be used to further defend the user from spam and phishing emails as well as malicious URLs, and downloads. The protection tool would sit on computer and would monitor incoming traffic that it would then scan and, if noticing that it came from an unethical source, would block you or it from gaining accessing. While the program will still utilize blacklisting address, it will also look more closely at the content, analysing potentially harmful links and download sites, this would stop emails that got past the network blacklist from entering the users inbox. As well as scanning emails and blocking them, these client side programs can also analyse websites being visited to make sure they are genuine. To add one more level of protection an antivirus should be used. This would add email scanning, web page scanning, and download scanning.

2.1.3 User education

User education is a big factor when detection and preventing phishing attacks. User education can be supplied in an array of methods: mandatory training before work placement commences, routine refresher

courses, and surprise tests sent to workers to see how they would react. By building user educations as well as procedures to what should need to be done in case there is a need for verification, most if not all phishing attack that were to be pass into the networks and on to the emails of workers should be detected, prevented and flagged/reported if needed so future attacks can also be blocked.

3 networking

3.1 explain why the network speed is low and if the issues is inside or outside the intranet

There are two inbuilt tool on both windows and Linux systems to help diagnose issues that occur on the network, particularly when it comes to speed. While using one can be very useful, both together will give the best result when tracking down the issue.

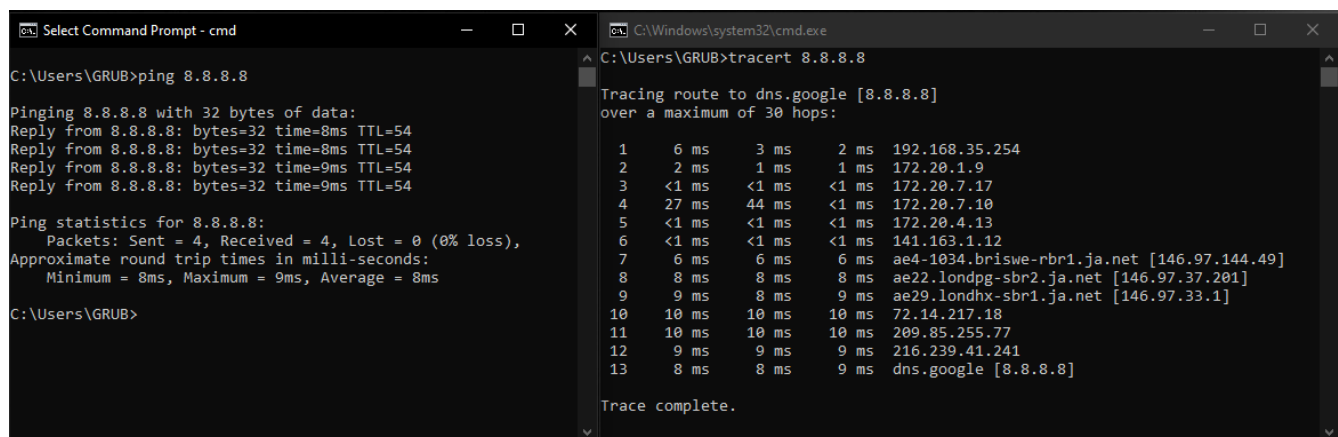
3.1.1 Ping

The first tool is called ping and it is easily called from a desktops terminal or command prompt. The information the ping gathers is the round trip time, time to live(how many jumps to get there) and specifys how many bytes were sent with that request. With this information you can quickly gauge if there is an issue as you can compare how many bytes are being sent against the round trip time. If the bytes are low while the round trip time is high there is something going wrong either at the destination or along the way to it.

3.1.2 trace route

Trace route is the second tool. It also come with windows and Linux systems, and is easy to use. It utilizes ping to trace the route of the packet as it traverses the intranet then internet. The use of trace route is to see and analyse each hop. This allows you to pin down where exactly the issue could be as the round trip time will be significantly longer on one of the hops.

Both of these tools together will help to identify the issue but finding out if the issue is inside or out side the network will require further analysis. This can can be achieved by tracrouting and pinging devices both inside and out side the network at least three times to get an accurate result and monitoring the RTT(round trip time) for each one If there is a particularly long RTT thats consistent on one of the hops, and pinging the device results in the same RTT then the issue will most likely be with the device currently being pinged.



```
Select Command Prompt - cmd
C:\Users\GRUB>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=8ms TTL=54
Reply from 8.8.8.8: bytes=32 time=8ms TTL=54
Reply from 8.8.8.8: bytes=32 time=9ms TTL=54
Reply from 8.8.8.8: bytes=32 time=9ms TTL=54

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 9ms, Average = 8ms

C:\Users\GRUB>

C:\Windows\system32\cmd.exe
C:\Users\GRUB>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:
  0  6 ms  3 ms  2 ms  192.168.35.254
  1  2 ms  1 ms  1 ms  172.20.1.9
  2  <1 ms  <1 ms  <1 ms  172.20.7.17
  3  27 ms  44 ms  <1 ms  172.20.7.10
  4  <1 ms  <1 ms  <1 ms  172.20.4.13
  5  <1 ms  <1 ms  <1 ms  141.163.1.12
  6  6 ms  6 ms  6 ms  ae4-1034.briswe-rbr1.ja.net [146.97.144.49]
  7  8 ms  8 ms  8 ms  ae22.londpg-sbr2.ja.net [146.97.37.201]
  8  9 ms  8 ms  9 ms  ae29.londhx-sbr1.ja.net [146.97.33.1]
  9  10 ms  10 ms  10 ms  72.14.217.18
 10  10 ms  10 ms  10 ms  209.85.255.77
 11  9 ms  9 ms  9 ms  216.239.41.241
 12  8 ms  8 ms  9 ms  dns.google [8.8.8.8]

Trace complete.
```

Figure 2: Ping on the left. Trace route of the right

3.2 purpose new network architecture to allow for more security and expandability

With the new network architecture, Brown-Rath needs both an extendable and easily maintainable network layout as well as added security. There are three potential technologies that can help with the network security: IDS(intrusion detection system) on both network and host(client), firewalls, and demilitarisation zone.

3.2.1 IDS (intrusion detection system)

Instead of actively monitoring network traffic and blocking the potential harmful packets, the IDS will passively monitor the traffic and if something does look suspicious will flag it and send an alert so action can be taken to prevent the attack. There are two types of detection systems: one will monitor for anomalies, for example computer being accessed out of working time, and the other will monitor for attack signatures that can come from spyware and other pieces of malware. [4]

3.2.2 firewalls

Firewalls usually sit just before entering the network and its job is to look at and block restricted packets from entering the network, this is essentially blacklisting/whitelisting. It can work with inbound packets, outbound packets, ip addresses, and ports. With this level of customizability the firewall can be tuned to only allow certain packet in and out. [1]

3.2.3 demilitarisation zone

Demilitarisation zone is sort of an extension of the fire wall and is a way of dividing up public facing devices from devices that shouldn't be shown to the public. This adds a layer of defence as the firewalls dividing the zone can have different policies depending on which network is being entered or exited. [8]

For making the network more expandable and understandable, it is recommended to subnet the network. This involves using host bits as network bits to implement a new subnet, for example if your current network IP is 172.16.0.0\16 (the subnet uses sixteen 1s) you can split this network into 2, you first borrow one host bit and convert it to a network bit resulting in 2 new networks, 172.16.0.0\17 and 172.16.128.0\17 (because it starts with MSB to LSB.

255₁₀.255₁₀.10000000₂.0₁₀). Unless the current organisation is particularly big or is planning on have a rather big location with millions of devices connected, it is recommended to use class C IP address as there will be less IPS to keep track of, but still have plenty for future use [6].

ip class	number of hosts(devices) per network	typical range	subnet mask
Class A	16,777,216	10.0.0.0 to 10.255.255.255	\8 or 255.0.0.0
Class B	1,048,576	172.16.0.0 to 172.31.255.255	\12 or 255.240.0.0
Class C	65,536	192.168.0.0 to 192.168.255.255	\16 or 255.255.0.0

Table 2: table on private ip addresses [6]

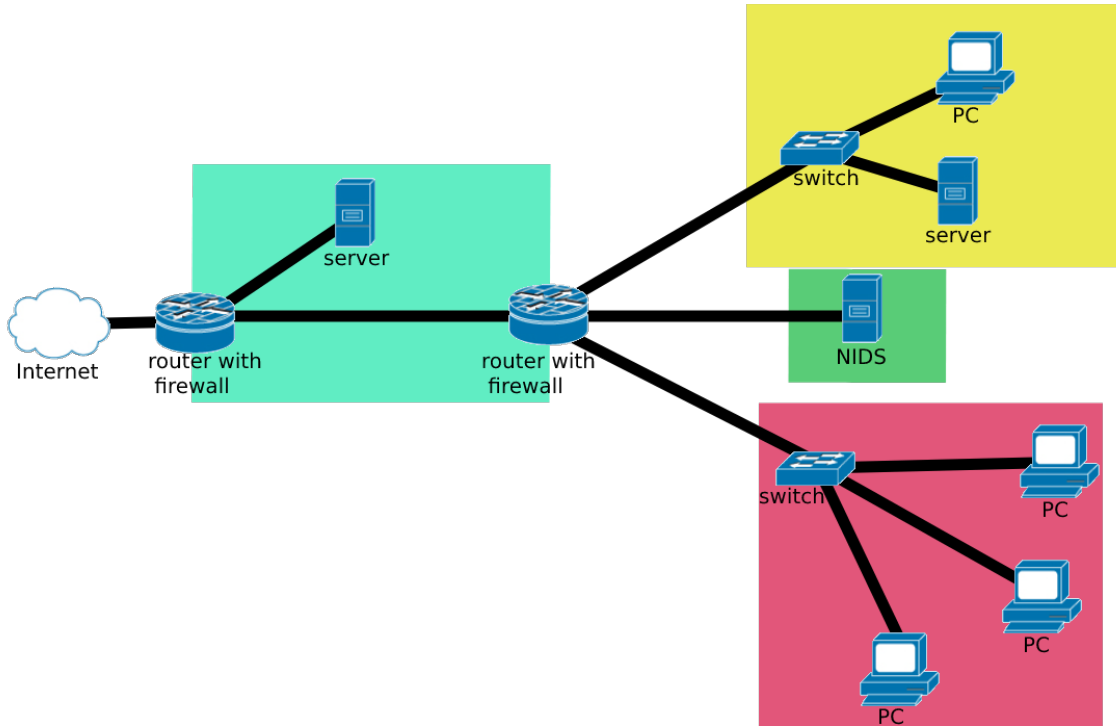


Figure 3: example of a network layout using demilitarisation zone(teal colour), routers with firewalls, and subnets(yellow, red, green)

4 conclusion

There are good ways to both improve both Brown-Raths security and network infrastructure. Helping potentially to stay clear of a hefty fine, and loss of valuable data that could inconvenience their customers, as well as pin point network work issues in an effective manner. Phishing emails are always getting sent and catching people off guard, but with proper protection on both the network and the hosts(clients) the amount that get through can be greatly decreased. Going through 2 layers of hands off security will block the majority of phishing emails with only a few getting through that will need manual attention. Debugging network issues isn't as hard as one might expect, knowing the right tools, what manner to use them in and the information to look out for results in quite a simple but effective procedure. Subnetting on the other hand could be a little tricky as it requires knowing how to divide networks up and the layout of masks and IP classes, but isn't necessarily difficult once these few things are known. This report has highlighted key features and information on the subjects that were required, but to fully gain proper insight and understanding of the methods and tools mentioned, additional research is needed as there is far too much to be able to write it in this report.

References

- [1] Ehab S Al-Shaer and Hazem H Hamed. Modeling and management of firewall policies. *IEEE Transactions on network and service management*, 1(1):2–10, 2004.
- [2] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3:563060, 2021.

- [3] Ammar Almomani, Brij B Gupta, Samer Atawneh, Andrew Meulenberg, and Eman Almomani. A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, 15(4):2074–2077, 2013.
- [4] Ismail Butun, Salvatore D Morgera, and Ravi Sankar. A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1):266–282, 2013.
- [5] The Information Commissioner’s Office and Henry Ashton. Data protection act 2018, May 2018.
- [6] Timothy Rooney. *Introduction to IP address management*, volume 17. John Wiley & Sons, 2010.
- [7] Government Digital Service. Data protection, Sep 2015.
- [8] Jack Webb. Network demilitarized zone (dmz), 2014.