ViryaTechnologies
ETHICAL TECHNOLOGY SOLUTIONS

White Paper: The Importance of Changing Default Passwords.

Introduction

In today's connected world, passwords are absolutely everywhere. We are constantly asked to create new passwords, whether for a Facebook account, financial management systems or a new router.

Whilst new accounts seldom come with a default password, many devices do ship with a generic username and password. Despite wide awareness of the importance of password control, many people still fail to change these default passwords.

Most users are aware that the username/password combination exists to confirm that you are who you claim to be, and so should be kept secret. Why then, do so many people choose not to change a combination as widely known as a default password?

The Dangers of Not Changing Default Passwords

Before we examine the potential pitfalls of changing that default password, let us complete an exercise intended to highlight just how *easy* it is for an attacker to determine the username/password combination of a device.

Let's assume we are connected to a small business network, and wish to take control of the network's router for our nefarious use. So to begin we access the router through our web browser (*for example by typing 192.168.1.1 into the address bar*).

Unsurprisingly, the router asks us to provide a username and password. Obviously, We don't yet know this, but by looking at the webpage or password dialog we can often identify the router's manufacturer and model. In this case, the router is a NetGear DG834G.

So now, we go to our favourite search engine and enter the search term "Netgear DG834G default password" [1]

The first five results all divulge that the default username/password combination is admin/password

So in less than a minute, we have retrieved the authentication credentials for our target device. If the default password had been changed, this effort would have failed.

So now that we have access, what can we do?

With full control of the router, we may choose to do a range of activities, such as;

1. Disrupt the network
2. Change the passwords to deny administrators access
3. Install our own software on the router
4. Attack other systems
5. Set up a webserver

Although Option 1 would be *immediately noticeable* by the networks users, if we had already completed Option 2 there would be very little that they could do about it. We also stand to gain very little apart from the knowledge that we have made someone's life miserable.

A much more beneficial approach (to us, the attacker) would be to use our access to complete one or all of Options 3 to 5. By installing our own software, and slightly reconfiguring the network, we could launch a *'Man In The Middle Attack' (MITMA)*.

A *MITMA* allows us to discreetly log the content of any connections the users make, **including encrypted connections** such as those used for Internet Banking. So by discreetly installing our own software, we stand to potentially gain the credentials needed to access the businesses Internet Banking account. At the very least, it's likely we'll gain the Internet Banking credentials for at least one employee.

Of course, if we were in the employ of another company, a *MITMA* is also very **useful for Industrial Espionage**. We could log the content of all internal connections and so record any sensitive material transmitted over the network whilst our software is running.

A *MITMA* is very difficult to detect, and could be in place for years before it is noticed. During this time, we may have had access to any information that passed over your network.

Alternatively, we could simply be accessing the system to try and disguise our location. It's likely that we wouldn't do this whilst physically on the network, but instead from a remote location. If this were the case, our new level of access would allow us to use the corporate network in order **to attack another machine or network**.

This could result in the company network being used in a *Distributed Denial of Service* (*DDoS*). It's unlikely that the business would be aware of this until they were contacted by the police in relation to the *DDoS*.

Our final option is potentially very dangerous for the company involved. We could choose to set up a webserver to serve content of our choosing to the Internet. If an attacker does choose to do this, you can be certain that the content being served is illegal.

If the company is lucky, it may simply be copyrighted content, but it's far more likely that it'll be child pornography or malware. In either case, the company involved is unlikely to know about this webserver until they are inevitably visited by the police for possessing illegal content.

In the latter two cases, it's likely that a Police Investigation would show that the Company was not responsible for the attack or the content. However, it's also very likely that the **equipment involved will be seized by the Police** in the course of their investigation, which would leave our target company without connectivity for quite some time.

In addition to losing business and assets, it's highly likely that any police investigation would cause bad PR for the unfortunate company.

As you can see it's very easy to lose control of your corporate network once an attacker has gained access.

Attackers are everywhere

So far, we've assumed that the attacker will be a person within your organisation. However, the list of potential attackers is much longer including;

- *Malware – Worms, Viruses etc.*
- *Disgruntled Employees*
- *Curious Employees*
- *External Hobbyist Hackers*
- *Internet Criminals (Often financially motivated)*
- *So-called 'Script Kiddies'*
- *'Grey Hats' – Unethical Security Researchers*
- *Competing Organisations*
- *Governments (Foreign and Domestic)*

As you can see, the range of potential attackers is huge. Which group is most likely to attack your network depends largely on your particular area of business. For most businesses, the most likely sources of attack are employees and malware.

In the previous section, we looked at examples of activities we could undertake once we'd gained access. Malware can also complete any of those tasks without any need for human involvement. We'll see an example of malware spreading as a result of users failure to change default passwords in the Case Studies.

Case Studies

Case Study 1: BTHomeHub Exploit [2]

In 2007 BT wisely chose to stop using a generic default administrator password on their BTHomeHub routers. Instead they opted to use the devices serial number instead, thus ensuring that the password was unique to that particular device.

Unfortunately, a weakness was discovered by GNU Citizen that allowed a user connected to the HomeHub via either the local area network (LAN) or wi-fi to force the device to disclose its serial number.

Thankfully, to our knowledge, this exploit has not been weaponised. It does, however, highlight the risks of using the default password, even if the password itself is not known. If the attacker knows how the default password is created, they can calculate what the password is.

If a business was using a BTHomeHub (Some smaller businesses do), this vulnerability would have allowed a disgruntled employee to take control of the device.

Not long after news of this exploit was released, BT updated the firmware on the HomeHub to force users to change the default password the next time they logged into the device.

Case Study 2: ‘Millions’ of Routers vulnerable to web hack [3]

A recently disclosed vulnerability in the Domain Name System (DNS) could potentially allow remote attackers to access your network using a method known as DNS Rebinding.

The attack works by utilising a feature that allows webservers to balance their load between multiple servers, the attacker simply creates a page that tells the client to access a device on their own network.

Many of the popular defenses against attack, such as OpenDNS and the Firefox plugin ‘NoScript’ are powerless to stop this kind of attack.

The attack is, however, rendered largely impotent if the default passwords on the target network have all been changed. The attacker could feasibly still take control by exploiting a known vulnerability in the device, but this is far more difficult and targeted than using a known default username/password combination.

Although elements of this case study are undoubtedly scaremongering, it does serve to highlight exactly how a remote attacker could take advantage of your failure to change default passwords on your network.

Case Study 3: iPhone Malware – Rick Rolling [4]

The iPhone is a smartphone released by Apple, and is very tightly controlled by the company. Apple controls exactly what software you are able to install on the device through use of it’s ‘App Store’.

Some users are unhappy with Apple having this level of control, and so choose to ‘Jailbreak’ their phones. It is these phones that were targeted by the malware known by the name Ikee or Rick Roller.

The malware changed the users background to a picture of Rick Astley, and changed their SSH (See note below) password. The malware also displayed worm like characteristics in that it copied itself to other vulnerable devices.

Ikee/Rick Roller spread by utilising the devices wireless connection to locate other iPhones in the immediate vicinity. It then attempted to access the target phones SSH server by using the default root password (‘alpine’). Users who had not ‘jailbroken’ their iPhones were unaffected, as were those who had changed the default password after ‘jailbreaking’ the device.

This case shows that a failure to change default passwords can put a wide range of devices at risk. Whilst most people consider the risk to network equipment, they often forget about mobile devices. It was this failure by the owners of the affected iPhones that allowed the malware to spread.

Note: SSH stands for Secure Shell. It is a remote administration protocol that allows a user to remotely access the console of a device as though they were physically at the device itself.

Conclusion

As more and more of our devices are becoming connected to networks, it has never been quite so important to change default passwords. Any device connected to a network is potentially a target for abuse, whether it be a shared printer, a webserver or the network's router/firewall.

Although changing the default passwords is very important, it is not a panacea. It's very important that users continue to follow best practice when using and creating passwords. Do not share passwords between users or accounts and ensure that your passwords are alphanumeric and non-obvious.

Your password is usually your first line of defence against this kind of attack, using a default password makes it very easy for an attacker to do absolutely anything. Depending on the attackers activity this could lead to sensitive data being leaked, a network outage or even a visit from the Police.

References

[1] http://www.google.co.uk/search?q=Netgear+DG834G+default+password
[2] http://www.gnucitizen.org/blog/dumping-the-admin-password-of-the-bt-home-hub/
[3] http://blogs.forbes.com/firewall/2010/07/13/millions-of-home-routers-vulnerable-to-web-hack/
[4] http://www.machackpc.com/iphone/3g/iphone-virus-ikee-protect-your-iphone/

About the Author

Ben Tasker is an IT Manager & Linux Specialist at Virya Technologies. He has substantial experience within the IT Industry, and a keen interest in Network security.