Virtual Machine Network Report:

Author: Andrew Michael Koch Student ID: U5371834

Organization:

For my company network I chose to emulate a small online retailer.

I assumed the name of this company to be Sixth Domain, a small online retailer located in Canberra.

They run an e-commerce website and have asked me to set up and secure their network for them.

To do this I first needed to know what potential risks the organization might face in order to figure out how best to defend against them.

Organizational Risks:

As my organization would be involved in the sale of objects one of the biggest risks to the organization would be that somebody might steal their customers credit card or other personal information. This could be done by some form of Man in the Middle attack or by an attacker accessing the database on which this information is stored. This could be protected against by utilizing SSL Man in the Middle filtering with Squid.

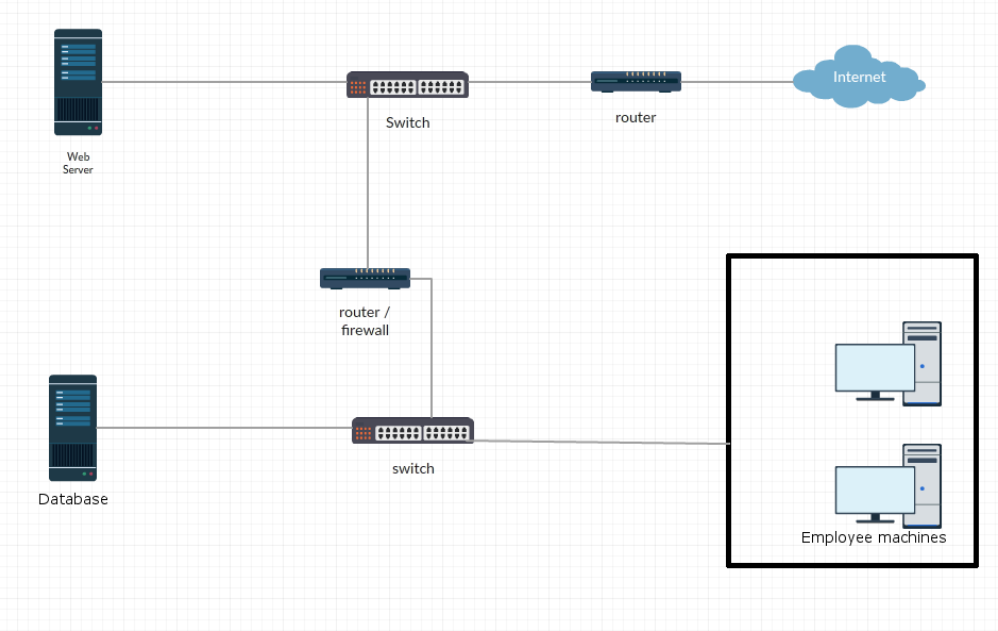
One secondary threat to my organization could be the company website being taken down. This could be done through some form of DDOS attack. While this cannot be completely protected against it is possible to mitigate this threat somewhat by increasing the maximum number of connections to hold in the firewall state table and the maximum number of table entries. While this will not work with a single firewall against an attack of millions of incoming connections it is possible to share the load of this attack amongst several different firewalls implementing firewall load balancing.

A third threat to my organization could be someone gaining unauthorized access to a machine on the company network and using it to either steal client information, refund a bank account that never purchased anything using company money, or to otherwise inflict malicious attacks. This can be defended against by increasing the protection on employee machines to mitigate the chances of an attacker gaining unauthorized access to one of them.

Another threat to the organization would be an internal one. A disgruntled employee could choose to leak customer information or try to infect the systems on the company network with a virus. One way of mitigating this threat is to block access to known malicious websites and limit employee access to websites affiliated with hacking activities. It is also a good idea to set up some form of detection to show when an employee machine attempts to access a malicious website or otherwise perform a malicious action as this will allow the company to quickly respond in the cases where it is necessary to do so.

Network Design:

My general network design for my company can be viewed below:



A simple network diagram for an online retailers network.

The basic network design includes implementation of a DMZ to separate what the clients interact with from the rest of the company machines.

This is done to help provide protection for the rest of the network as end-user services are the most vulnerable to attacks and therefore the most likely to be compromised systems.

In this case the first router between the internet and the rest of the network is the VirtualBox networking engine which maps to and from the Virtual Machines inside VirtualBox.

The second router/firewall is my PfSense Virtual Machine which I have configured to function as a DMZ between the Web Server and the rest of the network.

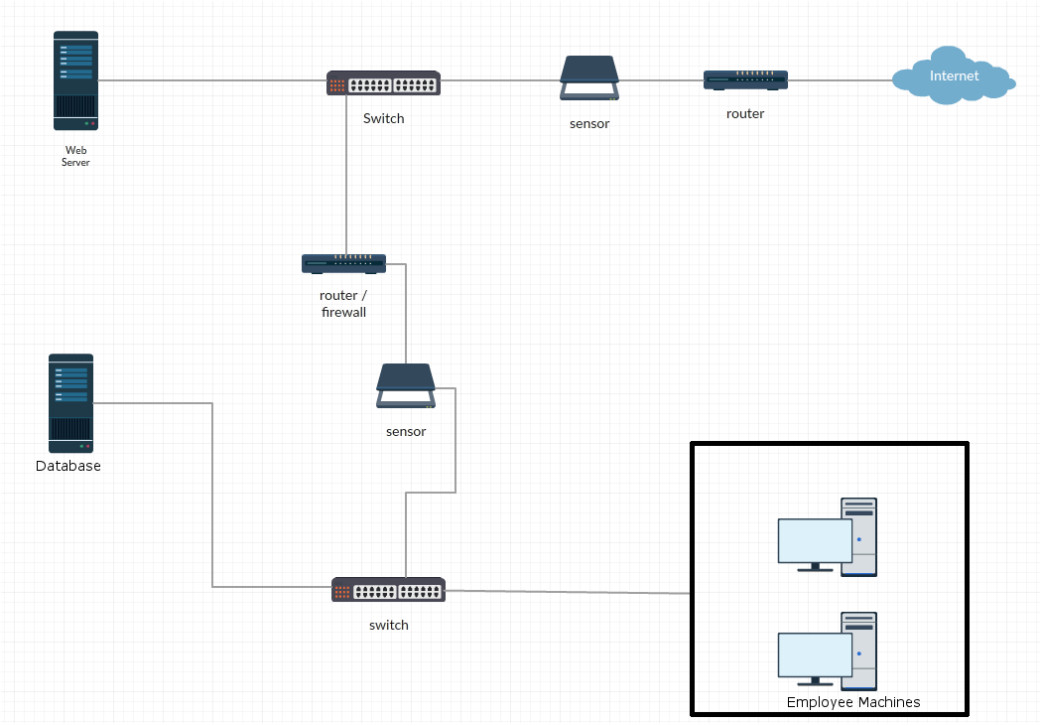
Note that in a production environment it may be a good idea to set up the first router yourself so as to ensure adequate firewall protection. This was not done in my installation as an edge router was already provided by the VirtualBox system but this could be easily accomplished by duplicating the PfSense Virtual Machine configured router.

While this network layout does serve its purpose as a functional network it does not allow for much detection for the DMZ, nor does it provide much protection against internal network attacks such as email spoofing.

It is therefore ideal to place some sensors on the network in order to be able to detect any issues with machines on the network.

These sensors should ideally be placed at each ingress/egress point into the network.

My updated network design for my company with sensors included can be viewed below:



A simple network diagram with added scanners.

This network design now includes implementation of some sensors in order to monitor network activity.

For each of these sensor platforms a Security Onion Virtual Machine was used.

After my network layout was designed I needed to set up my Virtual Machines to mimic it.

To do this I first started by installing VirtualBox and downloading iso files for each of my desired Virtual Machine operating systems.

The sources used for download of these operating system iso files can be found at the end of this report.

Virtual Network Setup:

I first started by creating a few virtual machines in Oracle VM VirtualBox Manager in order to have them take part in my virtual network.

For a firewall I chose to create a PFSense virtual machine.

For a server I chose to create a Windows Server 2016 virtual machine.

For a user machine I decided to use a Windows 7 virtual machine. I chose to use this instead of later versions of Windows due to the its prevalence of usage worldwide. While a less commonly used operating system such as Arch Linux may be more secure due to the lack of malware specifically targeted towards them I chose to use a Windows operating system because I believe that they are more commonly used in most small company computer networks and would therefore lead to a more accurate simulation of a company network.

For detection tools I also chose to use Security Onion virtual machines.

Windows 7 Setup:

For an employee machine I decided to use Windows 7 Ultimate SP1. This was done for a number of security reasons as well as usability reasons.

One security reason to use Windows 7 instead of Windows 8 or Windows 10 is that ASLR does not work as well in Windows 8 or Windows 10.

One usability reason for using Windows 7 is greater control via the control panel when compared to Windows 10's settings app.

To begin with I set up protection for my Windows 7 VM.

I started by installing Firefox for use as the default browser. This was done in order to use some security based addons to make browsing the internet safer. The addons installed onto Firefox are uBlock Origin, NoScript Security Suite, and HTTPS Everywhere. uBlock Origin functions as a general ad blocker and is useful for mitigating the chances of malicious advertising attacks affecting the machine. NoScript Security Suite is useful for preventing malicious files such as Flash files from running in your browser without your consent. The HTTPS Everywhere addon is useful for preventing any Man in the Middle attacks from occurring.

After this I then installed all missing security updates using Windows Update. Note that this was a very large download and due to my local hard disk size being quite small this prevented me from having more than one Windows 7 Virtual Machine present within my network.

More employee machines could easily be created by copying my Windows 7 Virtual machine.

I next followed various steps outlined by the Australian Cyber Security Centre for hardening Windows 7.[1]

One of these included changing the group policy settings for passwords in order to achieve a secure password policy as defined by the Australian Cyber Security Centre.

Another of these included installing the Enhanced Mitigation Experience Toolkit. This is useful for reducing the risk of an attacker exploiting any security vulnerabilities in Windows or third-party programs.

After completing all of the steps outlined in the ACSC document I then ensured that Windows Defender Antivirus was activated and properly configured.

After this I set up detection on my Windows 7 VM so that any malware breaches could be detected.

To do this I installed a KfSensor to use as a honeypot form of detection.

I then set up PfSense to function as a firewall/proxy/antivirus service. This involved adding the Windows 7 VM to the same network as the PfSense machine and configuring PfSense through the PfSense web-GUI.

PFSense Setup:

For a network firewall I decided to use PFSense.

After the initial PfSense Virtual Machine setup I configured PfSense via the web-GUI interface using my Windows 7 VM.

For PFSense I decided to use the following packages:

- Pfblocker – Used for DNS and GeoIP blocking
- Squid – Used as a caching proxy and as an antivirus
- Squidguard – Used for Url filtering via Blacklisting
- LightSquid – Used to monitor network traffic by Squid proxy users
- Snort – Used for intrusion detection and prevention
- Ntopng - Network usage probe

I decided to start by configuring the protection packages.

PfBlocker Configuration:

To begin with I decided to configure DNS filtering for PfBlocker. For this I used a bunch of domain lists found through reddit in order to block some known adware domains, prevent browser based cryptocurrency mining, and generally make internet browsing much safer for the company.

It should also be mentioned that during the initial DNS filtering configuration I decided to enable the TLD option. This was done in order to block not only the domains contained in the domain lists used but also their subdomains. This can be quite memory intensive but I believe that the payoff is worth it.

A full list of the domain lists that I used for this can be found at the end of this report.

After setting up DNS filtering I then set up GeoIP blocking. My assumptions here were that the company which I am setting up my network for would not be doing business with Africa due to being a small Australian based business which only sells products within Australia. I therefore blocked all of Africa as any request sent from there would most likely be malicious.

Furthermore I decided to block the top 20 spammer locations as none of them were in Australia and would therefore be highly unlikely to be a valid connection.

After this I decided to configure Squid.

Squid Configuration:

I decided to use Squid as a proxy server for the network. I did this by installing Squid via the package manager and then configuring it to allow users of the network to use it as a transparent proxy. One of the reasons for using a proxy server was to save bandwidth as I believe that would be an issue for a new Australian company.

Furthermore it also helps to reduce latency, making transactions faster. Squid accomplishes this by storing frequently visited websites in the PfSense cache.

I decided to increase the default hard disk cache size as the default is quite small and doing so enables more frequently visited websites to be stored on the PfSense Virtual Machine, thereby saving the company time and money.

I also enabled SSL Man in the Middle filtering through the Man in the Middle bumping mode. This is required in order to ensure that the Squid antivirus works on https websites.

To implement this I made a certificate authority for SSL interception. I also made a Certificate for the GUI for the Squid bumping method. This certificate is signed with the SSL interception certificate authority that I created.

I then exported and installed the Certificate Authority I created in both Windows and Firefox.

After this I decided to use ClamAV Antivirus which comes with the Squid package and set it to redirect to google.com whenever a virus is detected. This was done as an extra layer of protection on top of the native antivirus software installed on machines within the network. Ideally this would instead redirect to a page on the company website which mentions that a virus has been detected, but google.com has been used as a placeholder in the meantime.

I also implemented google safe browsing support as a blacklist service.

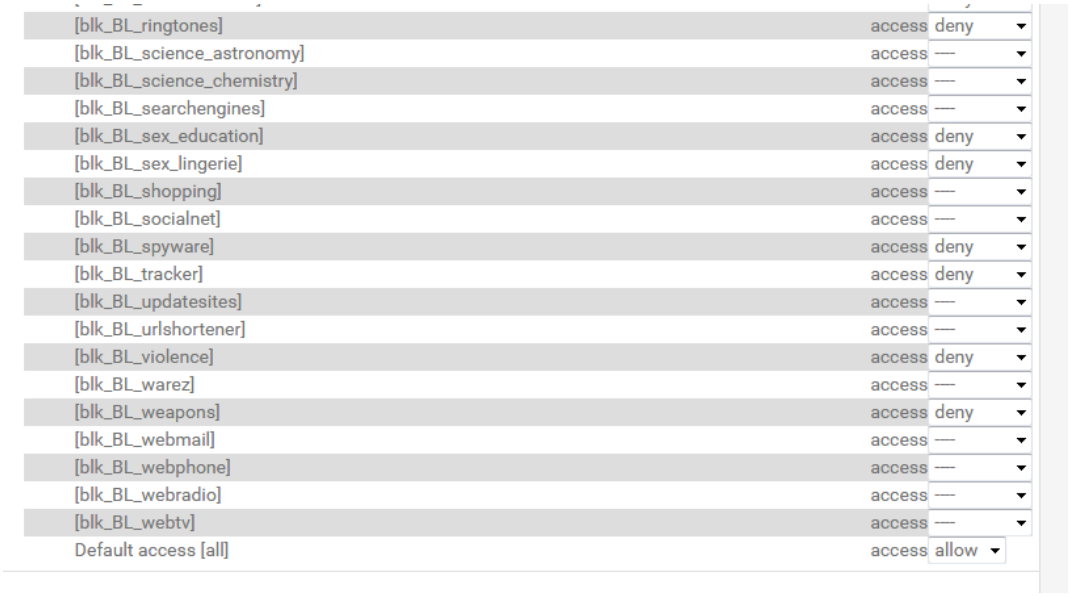
After this I configured SquidGuard.

SquidGuard Configuration:

Squidguard filters based on the URL of the website.

I set up logging with SquidGuard and also downloaded the blacklist located at http://www.shallalist.de/Downloads/shallalist.tar.gz

After this I set the target rules for the blacklist to block specific categories as seen below:



SquidGuard Common ACL configurations

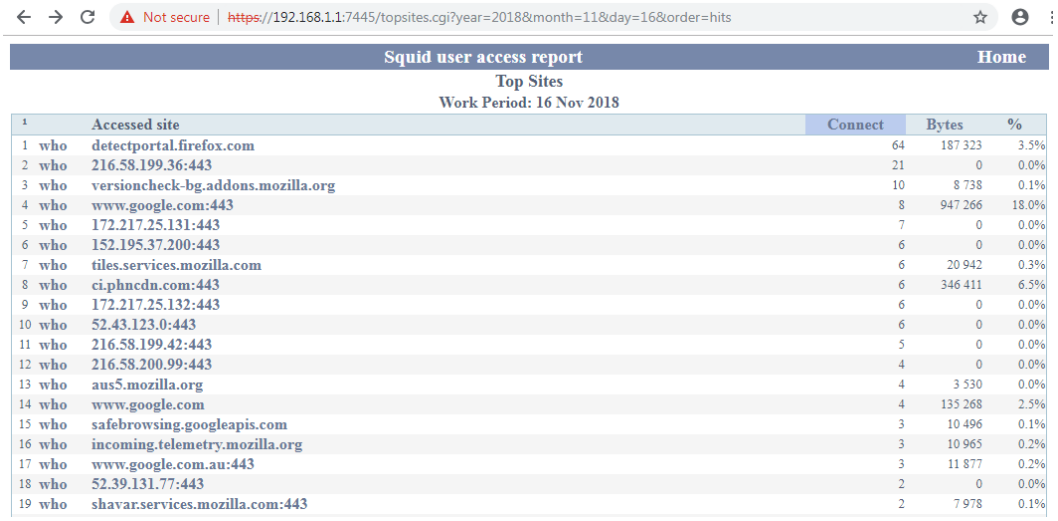
I also enabled protected modes for search engines in order automatically enable adult content protection on any search engines used.

This was done to decrease the risk of any malware or phishing sources being accessed by employees.

A full list of blacklists used for squidguard can be seen at the end of this report.

LightSquid Configuration:

After this I installed LightSquid in order to view the network activity of employees. This allows me to view and sort a wide array of network data such as the most commonly connected to websites or any large files downloaded. This can be viewed by individual users on an individual day or otherwise ranked according to overall users of the network as shown below.



¹		Accessed site	Connect	Bytes	%
1	who	detectportal.firefox.com	64	187 323	3.5%
2	who	216.58.199.36:443	21	0	0.0%
3	who	versioncheck-bg.addons.mozilla.org	10	8 738	0.1%
4	who	www.google.com:443	8	947 266	18.0%
5	who	172.217.25.131:443	7	0	0.0%
6	who	152.195.37.200:443	6	0	0.0%
7	who	tiles.services.mozilla.com	6	20 942	0.3%
8	who	ci.phncdn.com:443	6	346 411	6.5%
9	who	172.217.25.132:443	6	0	0.0%
10	who	52.43.123.0:443	6	0	0.0%
11	who	216.58.199.42:443	5	0	0.0%
12	who	216.58.200.99:443	4	0	0.0%
13	who	aus5.mozilla.org	4	3 530	0.0%
14	who	www.google.com	4	135 268	2.5%
15	who	safebrowsing.googleapis.com	3	10 496	0.1%
16	who	incoming.telemetry.mozilla.org	3	10 965	0.2%
17	who	www.google.com.au:443	3	11 877	0.2%
18	who	52.39.131.77:443	2	0	0.0%
19	who	shavar.services.mozilla.com:443	2	7 978	0.1%

An example view of LightSquid showing the most commonly connected to addresses.

There is no real configuration required for LightSquid after installation.

There are some downsides to using Squid proxy. One example is that Squid cannot transparently handle IPv6 traffic. This is a compromise that I believe the company must make in order to ensure a secure network.

After configuring Squid I then decided to configure Snort.

Snort Configuration:

Snort is an Intrusion Detection System and Intrusion Prevention system. I chose to install Snort in order to help mitigate the threats posed by any infected systems within the company network.

To configure Snort I started by enabling and downloading the Snort Vulnerability Research Team rules, the Snort GPLv2 Community rules, the Emerging Threats Open rules, and the AppID Open rules. This was done in order to allow Snort to identify and apply changes to traffic passing through Snort.

For Snort rule configuration I configured Snort to use the IPS policy of Security due to it blocking any dangerous flash files. I considered using the Balanced policy due to the fact that the excel file rules could lead to some false positives if excel files are often shared within the company but decided against it as if this is ever a problem it would

not be difficult to change the rule policies. I believe that this is one of the trade-offs required by the company in order to have a secure network.

I then configured Snort to send alerts to the firewalls system logs, set up Snort to automatically block hosts that generate a snort alert, and set the time for them to remain on the block lists to 30 minutes. During network usage it might be a good idea to test common company activities in order to ensure that any rules generating alerts from them are removed from the from the current rules set and disabled. This can be done via the Alerts tab.

I configured an internal LAN interface and an external WAN interface for Snort. The reason for also configuring Snort on a LAN interface was so that I could obtain information on which employee machine was triggering the alert. This makes it easier to remove a threat as you are able to tell which employee machine has been infected.

After this I decided to install Ntopng.

Ntopng Configuration:

I decided to use Ntopng in order to further monitor network activity. This is useful for viewing host and port activities as they are represented very well in a graphical manner, making it a lot easier to quickly make sense of what is happening within your network.

With all of this done my PfSense installation was configured.

I then set up my Windows Server 2016 Virtual Machine to function as my company web server. This mainly involved configuring detection and protection systems as I did not actually implement a full e-commerce web server.

Windows Server 2016 Setup:

I chose to use Windows Server 2016 for my Web Server. This is the server which will be contacted by potential customers in order to purchase items from my company.

I chose to use the Datacentre Evaluation version of Windows Server 2016 because it includes shielded virtual machines with hyper-v and a host guardian service. It also has better networking performance.

I did not actually implement the services required to have Windows Server 2016 function as an e-commerce web server as I did not believe it necessary for the scope of this assignment.

I did however set it up to interact with the other machines on the network using the DMZ set up in PfSense.

I then set up protection for my Windows Server 2016 VM.

To start with this I downloaded Firefox and set it up as done previously for the Windows 7 VM.

I then used various steps outlined by the Australian Cyber Security Centre for hardening Windows 10. [2]

This included changing password policies to achieve a secure password policy as defined by the Australian Cyber Security Centre.

While their document does refer to workstations the group policy settings are equally applicable for Windows Servers as stated in their document.

Furthermore in order to comply with Payment Card Industry Data Security Standard requirements I installed Bitdefender as an antivirus software for the server. Alongside this I also enabled Windows Defender in order to further harden the protection of the server.

After this I set up detection on my Windows Server 2016 VM so that any malware breaches could be detected.

To do this I installed a KfSensor to use as a honeypot form of detection.

After this I chose to install and configure my Security Onion Virtual Machine.

Security Onion Setup:

I decided to use a Security Onion Virtual Machine as a sensor platform.

The primary use of Security Onion is to perform intrusion detection, network security monitoring and log management.

The setup for this is not very in-depth and mainly involves just the initial installation and configuration of the Security Onion VM.

The only real parts of note during this is that I set Security Onion to listen to the traffic generated by PfSense in order to view network activity and I set the Snort IDS Engine to use the Emerging Threats GPL ruleset.

Conclusion:

Throughout this assignment I have designed and built a network of virtual machines that represent a small e-commerce company. While setting up the network I have hardened the machines on the network in various ways as well set up multiple methods of detection in case any of the machines on the network are compromised so that any damage done by a network intruder can be quickly detected and the intruder cut off from the network.

Domain Lists used for DNSBL:

- http://someonewhocares.org/hosts/hosts
- https://hosts-file.net/ad_servers.txt
- https://raw.githubusercontent.com/quidsup/notrack/master/trackers.txt
- https://adaway.org/hosts.txt
- http://sysctl.org/cameleon/hosts
- https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt
- https://isc.sans.edu/feeds/suspiciousdomains_Low.txt
- https://mirror1.malwaredomains.com/files/immortal_domains.txt
- https://osint.bambenekconsulting.com/feeds/dga-feed.gz
- https://zerodot1.gitlab.io/CoinBlockerLists/list_browser.txt
- https://gist.githubusercontent.com/BBcan177/b6df57cef74e28d90acf1eec93d62d3b/raw/f0996cf5248657ada2adb396f3636be8716b99eb/MS-4
- https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts
- https://mirror1.malwaredomains.com/files/justdomains
- https://zeustracker.abuse.ch/blocklist.php?download=domainblocklist
- https://s3.amazonaws.com/lists.disconnect.me/simple_tracking.txt
- https://s3.amazonaws.com/lists.disconnect.me/simple_ad.txt

Squidguard Blacklist:

- http://www.squidblacklist.org/downloads/squidblacklists/squidblacklist.tar.gz

Virtual Machine ISO Sources:

- https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md
- https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016?filetype=ISO
- https://softlay.net/operating-system/windows-7-ultimate-full-version-free-download-iso-32-64-bit.html
- https://www.pfsense.org/download/

BIBLIOGRAPHY:

1. https://acsc.gov.au/publications/protect/Hardening_Win7_SP1.pdf
2. https://acsc.gov.au/publications/protect/Hardening_Win10.pdf