TABA - Network Security and Pentesting

Simon Lowry,
Pentester, Security Operations,
NCI Pentesters Ltd,
Dublin, Ireland,
x21168938@student.ncirl.ie

Abstract*—This is a report generated as a result a both of a construction of a network for a government agency and it's constituent systems and a subsequent penetration test conducted by NCI Pentesters Ltd on this network and systems. The report details the choices and considerations for how that network was constructed, then moves onto a number of attack vectors that were targeted. Each attack vector their own unique aspects to them revealing the broad attack surface the organization is charged with defending and then some mitigation strategies are outlined to help address the different threats highlighted by this pentest.

I. Executive Summary

The client in question is a Government Agency and as a result could face a whole host of different challenges including APT groups as well as Hacktivists targeting their networks. The network was set up in such a way to try and defend against a variety of threats, however, our penetration test was able to show how a number of different attack vectors could still compromise this network. It outlines three main attack vectors from the simple use of a high class vulnerability like Log4js can lead to a system compromise to considering how a more complex attack could occur from an Advanced Persistent Threat group. Here we outline this group leveraging a multitude of top quality tools and techniques to target specific documents and then finally, the report identifies another threat from an unlikely source, a printer. Attackers can leverage IOT devices to gain a foothold on the network, perform lateral movement and in the case of printers they have an asset that's potentially used by many orgs where they can view all that passes through them. Each of these present different dangers and require different defences from phishing and cyber training for employees to counter social engineering, to network segmentation and also effective patch management processes needing to be put in place to name a few of our recommendations. Further details are expanded in the mitigation section.

II. Network Setup

The network and its infrastructure were setup for a government organisation with significant resources at our disposal. Since the network is for a government agency, there are certain requirements needed to be able to defend against a variety of attackers from less sophisticated attackers to those using state of the art methods. Our network would have to combat against efforts to steal sensitive information, or cause disruptions to vital systems. [1] Aspects such as ensuring they are suppliers of repute and opting for systems on the higher end in terms of what they provided was of high priority. A number of the systems and tools put in place were selected due to being used in top tier enterprise networks and also highly recommended companies and tools by Gartner. Gartner is one of the leading research publications of the top players in different aspects of technology markets. Their recommendations are highly sought after in the tech. [2] [3] [4] To complement that additional research was conducted on various national cyber organisations and organisations that have worked with them, that also have recommendations for network creation for government agencies. Finally, reputable tech insight journalist providers were researched as well.

Some of the main aims for the network was to obtain resiliency, robustness, and availability aspects of a secure network. Resiliency here enables us to recover from adverse conditions, robustness is when the network can handle a variety of conditions without impact to the continuity of service and availability, ensuring that the systems and network is available to end users 24/7.

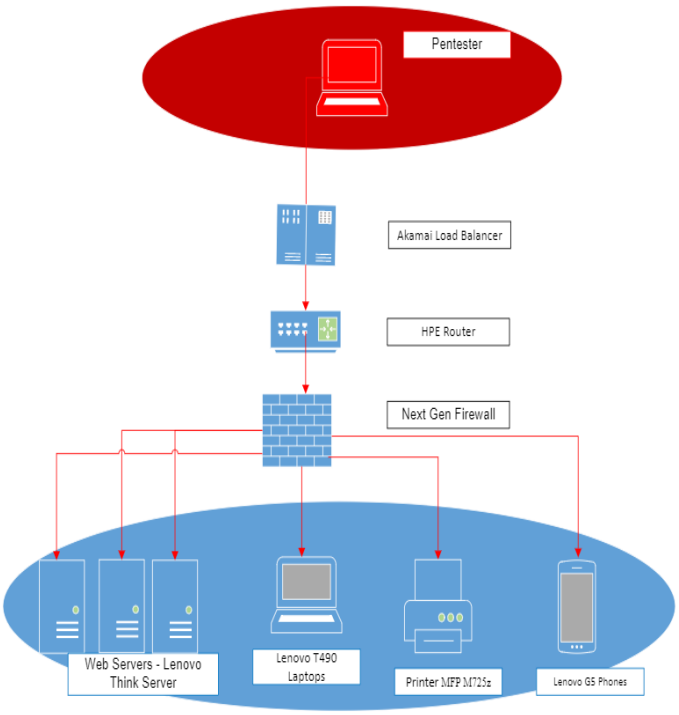
Lenovo has a strong reputation for durable, reliable systems that are tested to a high grade meeting at least one aspect of our availability needs. [35] The web servers selected are noted to be top performers with a good warranty of three years providing us with some fallback if anything were to go wrong. They also have a significant amount of storage capacity with up to 80TB and up to 64GB RAM . [5] This ought to be sufficient for the demands of our organisation as we are not a huge organisation in this regard. Load balancers are in place with the use of Akamai and Kubernetes, which in conjunction, spread the load of traffic to different areas and pods running the application while simultaneously being able to scale where necessary when the demand reaches predefined thresholds. With the rate limiting of Akamai, load balancing and scaling the network and systems are able to maintain availability and protecting against variants of Denial of Service Attacks.[6] [7] Also, if one pod goes down, others are still running and new ones will be spawned our team will be notified.

The systems in place have also undergone chaos testing deliberating pushing our pre-production environments to their maximum to see how they perform under this load whether it highlights any vulnerabilities in the infrastructure and this will take place every 6 months to maintain confidence in our infrastructure and highlight if there are improvements needed. [8] Fortinet's Next Gen Firewall in place to protect our networks and Checkpoints Intrusion Prevention is to supplement that. [9] [10]

Lenovo are also the supplier for the employee laptops.We're making use of bundles such as Microsoft Office 365 Business plan across all employee machines which has Outlook as the email client and this has some protection with Proofpoint. McAfee antivirus is on each host. McAfee has been named a leader in the endpoint protection space by Gartner, Fortinet a leader in Firewall protection. [11] [12] Data in our databases is repeatedly subjected to data replication across various sites to ensure the integrity and availability of that data is not compromised

under any adverse circumstances. Finally, multifunction printers from HP.

Network Diagram:



Summary of Devices on the Network

Device Type	Manufacturer	Model	Release Date	OS Version
Web Server	Lenovo	Think Server TS460	February 2017	Ubuntu 21.04 - Apache Web Server
Web Server	Lenovo	Think Server TS460	February 2017	Ubuntu 21.04 - Apache Web Server
Web Server	Lenovo	Think Server TS460	February 2017	Ubuntu 21.04 - Apache Web Server
Router	HPE	HPE FlexNetwork MSR1000	June 2018	VyOs
Printer	HP	MFP M725z	May 2013	
Laptop	Lenovo	T490	February 2019	Windows 10
Laptop	Lenovo	T490	February 2019	Windows 10
Mobile Phone	Lenovo	G5	March 2017	Android

Other Tools on the Network and Host Machines

Tool Type	Purpose
Outlook	Email Client
Proofpoint	Email Filtering & Security
Akamai	Rate limiting, DDoS protection
Checkpoint IPS	Intrusion Prevention System
McAfee Antivirus Protection	Host Antivirus Protection
Fortinet NextGen Firewall	Protects the network through inspecting network traffic

III. Attack Vectors

In this section we're going to discuss three different attack vectors that attackers could target for launching their attacks breaching our network and systems. We're investigating different technologies that we need to defend, as well as other threat vectors such as people, printers, networks, web applications all to highlight that our organisation has a broad attack surface with a variety of different kinds of threat actors to defend against. We'll walk through how they were conducted and then follow up with some mitigation strategies that can be used to prevent such attacks in the first place. It will aim to highlight that resources need to be applied judiciously to protect our organisation from these threats.

One of the routes that could potentially target our network and systems is via an Advanced Persistent Threat beginning with Social Engineering with spear phishing as the initial launching point and moving to more advanced methods from there.These kinds of groups operate at a high level of sophistication, with a lot of resources at their disposal and can be nation state sponsored. We'll aim to show some of the tools, tactics, techniques and different facets of their attack. It's not enough to not just cover our networks and systems but to effectively and regularly train our staff in cyber awareness. The spear phishing attack would be relying on tricking an employee of ours into performing an action that could lead to our systems being compromised. It's not enough to not just cover our networks and systems but to effectively and regularly train our staff in cyber awareness.

The tactics and approach here would drastically differ to the second attack which is exploiting a low hanging fruit of a highly publicised exploit at the moment with the Log4j vulnerability and from there using vulnerability chaining to further compromise the system. The level of capabilities required here is lower compared to the approach of the APT group however it's impact can be equally destructive or disruptive to our organisation. We need to keep a keen awareness of the latest security vulnerabilities and patch our machines. It's another route that can easily be exploited without a diverse set of security controls & policies in place.

The final threat vector explores what might be less considered as a potential attack for our networks and that is using a printer as a means of compromising a network and then looking to perform lateral movement. A printer can have a whole lot of confidential information passing through it from a lot of different people meaning it can be a rich source of sensitive information for an attacker with persistence maintained. The attackers in this case could also look to bring our network to a potential halt by launching a devastating ransomware attack alternatively as well originating from a printer compromise. This highlights the importance of not only securing our networks and servers but also any other device that could potentially be compromised and used as a means to launch further attacks which can equally still be very damaging to our organisation.

Through these different attack types, techniques and technologies we can see the broad attack surface that our organisation is charged with security and also the diverse nature of ways we'll need to employ different approaches to protect our organisation. No one security tool or two security controls can effectively cover these different routes of potential compromise. It takes a multifaceted defence in depth approach that is continually improving to meet the demands of an ever evolving threat landscape.

Summary of Attack Vectors

Attack Type	Techniques	CVE Number	Date of Incident	Description
Simulate APT Tactics	Social Engineering, OSINT, Trojan Malware Dropper, Custom Malware, Command Control Centre, Obfuscation, Detection Avoidance	N/A	20-04-2022	Making use of some tactics, tools and techniques we're looking to emulate a known APT group targeting specific intel for exfiltration.
Vulnerability Chaining	Remote Code Execution, Vulnerability Chaining, Enumeration, Web Application Vulnerablity, Transitive Dependency Vulnerabilities	CVE-2021-4428, CVE-2012-2122	18-04-2022	An attempt to exploit a number of vulnerabilities to infiltrate our network and show the compounded impact of their exploitation.
XSP - Cross Site Printing	Enumeration, Lateral Movement, Firewall Bypassing, Social Engineering, Cross-Site Printing, Firmware Vulnerabilities, Malware	CVE-2021-39237	19-04-2022	All IOT devices including printers can't afford to be neglected with security measures. Here we show what an attack on a printer can gain for attackers.

A. Attack Vector - Simulate APT Tactics

Our pentesters looked to simulate some Advanced Persistent Threat tactics for this spear phishing attack which extends on from there with their tactics.

Motives:

The aim was primarily at stealing information that could be advantageous to them in an ongoing cyber espionage campaign aimed at stealing confidential intellectual property. This was the pretext for their attack, they were not looking to perform a smash and grab approach but instead find and exfiltrate specific documents. These documents would be accessible after obtaining root privileges.

Target Technology:

Here our pentesters targeted email infrastructure as their means of compromising our network and defences. We are currently using the Microsoft Office 365 Business plan which has outlook as our email client. On top of that for email filtering we've been using Proofpoint tool which runs email filtering scans designed to help mitigate against malware infiltrating our network however the tool did not pick up this image filetype and as a result was able to make it through to a number of employees thus far.

Target Techniques:

Our pentesters looked to operate in an inconspicuous manner and where possible cause as a little noise as possible employing a variety of evasion techniques as well.. The attack involved targeting the weakest part of the cybersecurity chain first, people. This was done by using carefully curated emails tailored to their targets which were employees of the organization leveraging freely available information on various social media accounts.The attackers used very similar email addresses to the company email and made use of existing employees names in those email addresses to make it appear as if the emails were coming from a colleague.. They also targeted those within the C-suite of our company exclusively with high levels of access. They were able to identify these colleagues to use by finding their social networking profiles. From there they identified colleagues with whom they were often engaged in dialogue with and what the context of their publicly available conversations were related to. This became the basis of crafting the email to have them appear like something they already been in discussion about. This would provide the necessary cover for our pentesters and would exploit already established trust between these colleagues when effective.

Each of the emails contained an attachment which was an image that contained embedded malware. The initial payload was a trojan dropper malware that when clicked on downloaded two files. One of those files was a legitimate pdf gained from our website and is publicly avaiable. This was directly opened by a pdf applicatoin on a couple of these emploees systems.. The use of a pdf from the agency itself was as a means of misdirection to evade the detection of the additional malware that was downloaded as well.

The malware downloaded was called

Hammertoss.[13] [14] This is a particularly sophisticated kind of malware which obfuscates its actions to be very similar to regular user behaviour (making it all the more difficult to detect after being deployed to a system) and establishes persistence on the system.. It makes use of Twitter to create a daily Twitter handle from which it gains a link from a Command and Control Centre as well as an encryption key. The malware then visits the link and downloads an image from another service such as Github for example. All of this looks like normal user activity so it doesn't raise any alarms for any of the security tools deployed by the organization. This image downloaded by Hammertoss contains commands in steganography that when decrypted using the aforementioned key are instructions for Hammertoss to carry out. These were to firstly enhance visibility and enumerate the system then obtain higher privileges by making use of cron jobs and then work towards exfiltrating documents. We identified specific the documents related to certain intellectual property. From there we then looked to exfiltrate that data to their designated servers which themselves were compromised hosts (including the command and control centre used earlier). This use of compromised system again obfuscates where the data was going and who the owner of the command and control was, making true attribution difficult in this case.

o Target devices / technologies:
Web Application Server containing sensitive documents.

o Vulnerabilities / Exploit:
Human trust and staff lacking cyber training.

o Recent real world security incidents related to these methods:
Some of these techniques have been leveraged from an APT group known as APT-29 or Cozy Bear, a Russian advanced persistent threat group. Here are some of their noted incidents as well as the tools, tactics and techniques they employed:

> First up. in 2019, APT-29 attacked and were looking to obtain Covid-19 vaccine development information in the US. They operated using spear phishing, custom malware (Wellmess and Wellmail), command and control infrastructure as well as other known exploits in Citrix, VPN, Zimbra in order to compromise networks and systems in order to obtain research and development information on the vaccine. [34]
>
> Secondly, there was also the election fraud themed phishing campaigns targeting NGOs, Research Institutions, Government Agencies, looking to obtain sensitive information whereby the individual clicked on a link on those emails and an ISO file was delivered as essentially a container for the malware to infect the system and look to obtain information from there. [15]
>
> Finally there was the Solar Winds Orion supply chain attack where they trojanized the source code of Orion Software Platform which led to breaches of a whole host of US Government Agencies from the Department of Treasury to the Department of Homeland Security and ended up costing Solar Winds up to 3.5 million dollars in order to remediate the incident. [16]

*B. **Attack Vector - Vulnerability Chaining***

The next attack vector exploited was using vulnerability chaining with a Log4j vulnerability and a MySQL vulnerability compounding the effect of each vulnerability when coupled together. It shows that while one vulnerability may for example not appear that much of a risk, particularly to those outside of a security background but when chained together they can be devastating. For example, the MySQL bypass authentication vulnerablity on its own requires access to the web server first before being able to exploit it. Choosing to ignore vulnerabilities based on this kind of thinking can be a recipe for disaster as other exploits can clear the path for later being able to exploit this very kind of vulnerability. It's not the most glamorous part of a tech role maintaining a full list of your assets and keeping them up to date. The same applies for determining whether or not your web application or server is susceptible to a given vulnerability but choosing to ignore doing these things can result in disastrous consequences. [36]

The attackers targeted one of our web applications that was a Java based Spring-boot web application with MySQL database on the backend where Log4j was a dependency of the project and being used to perform logging for both debugging and auditory purposes. For the Log4j vulnerability attackers are able to run remote code on a server as a result of this vulnerability. This was deemed to have a 10 out 10 severity score by the Apache Software Foundation due to the fact that it could be exploited extremely easily and the impact it could have as well.. From that entry point they can gain greater access and cause all kinds of havoc to the system.

In this case it's the vehicle towards the greater prize of being able to get at the MySQL database. There was a choice made a number of years ago to ignore patching the MySQL database by our database administrators in order to not impact on the running of the web application and whatever ensuing adjustments may be needed to operate the latest version of MySQL. This choice comes at a price as the current version of MySQL operating on our web servers is susceptible to a number of security vulnerabilities including a bypass authentication vulnerability which allows attackers to get all of the usernames and hashed passwords from the database. The security team raised these issues but were rebuked by the database administrators claiming that it requires a whole host of different conditions to be met first before you could even reach the databases and as a result we were not at risk from this or other security vulnerabilities. Here we document the compounded effect of vulnerablity chaining and why this is dangerous thinking for an organisation especially when it comes to securing a trove of sensitive data and intellectual property that's contained within our databases. We need to reassess our approach and have a unified way of ensuring updates are happening and potential security vulnerabilities are not overlooked.

o Motives:

Tamper with a MySQL database using vulnerability chaining. Highlight the dangers of neglecting security vulnerabilities and how they can be chained together to have greater impact.

o Techniques:

The attack made use of a log4j script freely available tool on github which looks to check for a log4j vulnerability. [17] The tool used generates a string that can be input into a web application's API and can help to ascertain whether it's vulnerable. Here's an example of what was generated: ${jndi:ldap://*.dns.log4shell.tools:12345/*}.

The tool then looks to do a DNS lookup to obtain the IP address of *.dns.log4shell.tools. In the event that this succeeds, we have the first indication of the vulnerability through information leakage and then a LDAP search occurs and we got to see that the web application is fully vulnerable. From there, our team adopted and edited another script from github that sets up a fake ldap server and web server and allows the attacker to force the web application to download a file which executes and opens up a reverse shell to an attacking system and as a result we had compromised the web server. [18]

From there our next step was enumerating the system and by assessing the version of MySQL we could begin vulnerability chaining and moving onto target MySQL. Here we used a metasploit auxiliary scanner known as `mysql_authbypass_hashdump` we were able to bypass authentication and and extract the usernames and encrypted password hashes from MySQL. [32] Then using another module from Metasploit which is a John the Ripper module called `jtr_mysql_fast` we were able to get the passwords into readable format. These credentials were then tested out and we were able to successfully login to MySQL, at this point we had admin access and we could complete our objective of being able to tamper with some piece of information in the database to prove that this could be done as well. This was done on some trivial table which was agreed upon prior to conducting the testing as any other tampering was beyond the purview of the penetration test. This exploit used to bypass the authentication of MySQL shows that while some systems have been updated there's some inconsistencies in applying updates to all of the technologies and tools being utilised in the organisation.

o Target devices / technologies

Java Web application, Web Server, MySQL database.

o Vulnerabilities:

CVE-2021-44228 [19], CVE-2012-2122 [33]

o Exploits:

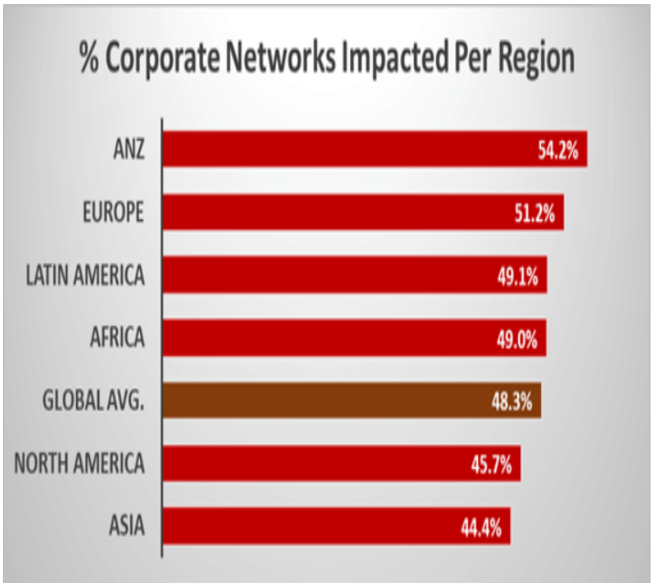
log4j-shell-poc [18]
mysql_authbypass_hashdump [32]

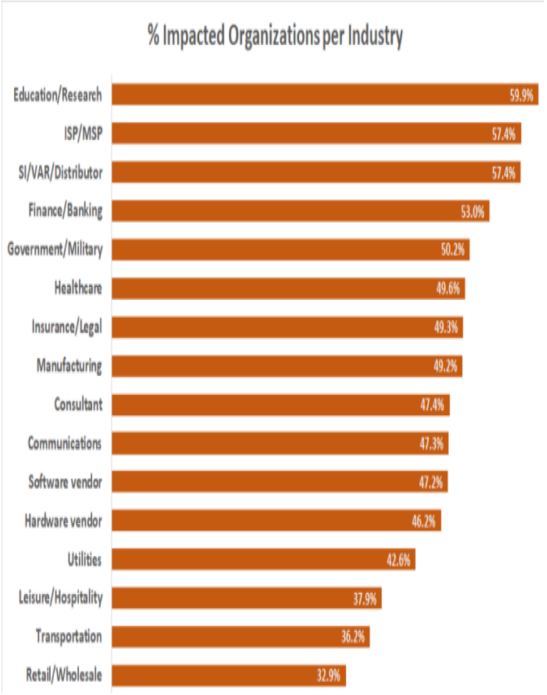
o Impact of the attack if successful:

The attacker is able to perform remote code execution or download files and in this case a reverse shell to further exploit the system. Beyond that, we're able to perform any action we would like on the databases after gaining all credentials which is a huge danger to the organisation, it could be released online and result in huge fines from GDPR, loss of reputation for the company, the data could be tampered with or wiped causing a lot of damage to the organisation and its credibility.

o Recent real world security incidents related to this vulnerability:

According to Checkpoint, there has been 4,300,000 attempts to exploit the log4j vulnerability with over 48% of corporate networks being targeted. [20] This is the figure going through their systems alone.





Researchers at Microsoft have also identified attempts at installing Cryptomining malware and also Cobalt Strike as part of an attempt to gain credentials amongst other efforts [21]

There has also been work done at Sophos and their intrusion prevention systems detecting hundreds of thousands of attempts to initiate remote code execution attacks on the log4j vulnerability [22]

C. Attack Vector - XSP - Cross Site Printing Attack

o Motives:

Steal information and highlight the importance of properly securing IOT devices.

o Techniques:

The next attack began with social engineering. In this case, a HR employee was sent an email from our attackers requesting that they print off a CV for an upcoming round of interviews. [23] [24] This employee was found out to be a HR employee by searching LinkedIn for HR employees of the company in the relevant area that we were working in. The email was also making use of a relevant job posting on Linkedin for the content of the email to legitimise the email. It was also sent from a very similar email address to her bosses email which was established after some further digging. Our company had access to some email domains with almost identical characters to your target company, however the letter i in the email addresses were substituted out for a Russian character that looks very similar to an i but is in fact a different character. The email address structure for employees was also easy to mimic as they used a structure with firstname.lastname@mycompany.com. The content of the email made use of some common social engineering techniques such as urgency and authority (by having the email appear to be from her boss) to get the employee to take it seriously and to act without thinking too much about the email itself and what the ask was. All of these factors contributed to the legitimacy of the request. Other techniques such as firewall bypassing, exploiting software vulnerabilities, lateral movement, cross-site printing are discussed in later section

Unbeknownst to the HR employee that email contained a pdf document which had an exploit in it that would make use of a vulnerablity in HP Printers [25] which allows for remote code execution by taking advantage of a font based exploit. This exploit sets up a SOCKS proxy since the print is behind a firewall which does not allow TCP connections to outside servers unless they are done through a SOCKS proxy server. This allowed us to perform firewall bypassing and gain a presence on the network. From there we were able to gain any information that was printed, scanned or faxed by the device as well as credentials that allows the printer to connect to the rest of the network.

It also served as a means to pivot and perform some lateral movement to another machine on the network. We looked at different ways to get into other systems on the network via SMB and other routes and were able to pivot from the printer to another web server on the network which interacts with the printer. This highlighted again that any networked devices can be a means of gaining a foothold on a network and could lead to greater trouble beyond that.

o Target devices / technologies:

In this case it was email, printers, people and then using that as a springboard for further attacks.

o Vulnerabilities:

CVE-2021-39237 [26]

o Impact of the attack if successful:

Attackers could compromise sensitive data, move laterally to compromise other systems, utilise the printer as part of a DDOS attack or as part of launching some ransomware on the network and potentially bringing the network to a halt.

o Recent real world security incidents related to this attack vector:

Over the past 12 months, 68% of organisations that took part in a study quocirca have experienced data losses due to unsecure printer practices. That has led to an average cost of data breach reaching 631,915 pounds [27]

An attacker known as Stackoverflowin launched a non-malicious attack on 150000 printers where he compromised the devices and printed a message to the owners such as “You are now part of a Flaming Botnet” or “close the port, skid” as a way to highlight to the owners of these devices they are not properly secure and could be used in a botnet or exploited in other ways if they didn’t improve their security [28]

At a Defon conference it was revealed that at least 35 significant vulnerabilities had been identified in enterprise printers at HP, Xerox, Ricoh, Brother, Lexmark.[29] These included Cross Site Printing, Buffer Overflow, Cross site forgery to name a few. These can allow attackers entry to a network and a place to maintain persistence as well as access to sensitive information passing through them and a means to enumerate and compromise or disrupt operations of other systems on the network.

Printers can be exploited from cryptomining, DDOS attacks, paper Dosing the printer itself, ransomware attacks, data breaches that lead to GDPR issues [30]

IV. Mitigation

Mandatory Cyber Training

In order to combat against social engineering attacks of different varieties, employees need to have repeated training carried out.

Internal Phishing Campaigns

To build on the cyber training the employees would benefit from our security engineers running some phishing campaigns and administering additional training to those who are duped by the emails.

Faster Rollout of Antivirus to All Corporate Systems

Our company had put in place some intentions of getting antivirus out to a certain designated cohort of employees on a phased basis. This process needs to be hastened and extended company wide to increase the likelihood of being able to detect malware on these systems and stop these kinds of attacks. Otherwise we leave ourselves susceptible to further breaches having an equally significant impact and allowing their activities to be prolonged. The attackers in this case were able to persist their activities for a number of months without our notice.

Asset identification: Identify all tools, systems and technologies on our network and systems

It's not possible to properly and effectively employ security controls or measures unless we have a full and comprehensive list of all of these. Otherwise any security updates as well may not reach all technologies like the MySQL database exploited in this report.

Introduce a patch management program

By introducing a patch management program we can reduce one of the likely routes of compromise that attackers look to exploit. Tools like Tanium patch management system can help here.

Separation of duties for investigating and applying fixes for security vulnerabilities

By separating these roles out to separate teams we can have one team in charge of investigating and applying the fixes and another which is responsible for making sure that these fixes have been put in place. The monitoring team would have final say on whether the assessments are valid or not for choosing to address or not address given security vulnerabilities. This can reduce the likelihood of security vulnerabilities going unpatched.

Network Segmentation

IOT devices (including printers) ought to be placed on separate VLANs with extremely limited networking capabilities. It would be best to have them separated out from any other corporate network to present them from being a means of pivoting and lateral movements to increasingly more dangerous targets to the organization. Any outbound connections need to be restricted to an allowlist of Ip addresses. Any ability to connect to wider internet ought to be restricted unless there are legitimate business reasons to do so. [24]

Disable all usb connections to printers

When USB connections are permitted for printing they can be leveraged as a vehicle for loading malware onto the printer posing a risk to the organisation even if it does require the additional step of being physically present to do so.

Change the password access to printer regularly

Changing the passwords regularly helps in the event that any password is compromised, having the regular change can disrupt any attackers using those credentials.

Change the printers name on the network

This can help to stop identifying information being displayed that attackers could use to find exploits with.

Increase security staffing

A number of security employees are spread across maintaining and using a host of different systems too thinly. Increasing the number of security employees can help here.

5. Conclusions

Overall there are a number of different attack vectors and threat actors to consider when securing a government network. Resources and defences need to be properly allocated across many domains, employees need to be effectively trained and sufficiently staffed to protect against these attackers.Without a broad approach to consider the full attack surface and sufficient investment we run the risk of our data being compromised and our systems being disrupted. Any technology on our network can potentially be a target for attackers and none should be considered lightly, even IOT devices. We are target for some of the most sophisticated threat actors around so we can't afford to be negligent in our duties or it come at a heavy cost for all of us as well as the nation at large.

Some limitations of this study were due to the fact that this is a theoretical study, there wasn't the scope, resource or time to actually create any kind of real network and make use of that to gain a real life creation of both the network and the subsequent attacks. Therefore, it's fundamentally an approximation of the interplay between a this theoretical network and these attacks. If there was more time it would be good to actually play out some of these attacks on virtualized machines to attempt to get a closer approximation to how this would be in reality. If more time was available even greater study could have been spent on a government grade network however this was purposefully designed with some weaknesses to illustrate how attackers could get in.

References

[1] - Cybersecurity and Infrastructure Security Agency, [Online] Available: https://www.cisa.gov/securing-federal-networks

[2] - R. Bernett, American Eagle, September 2020, [Online] Available: https://www.americaneagle.com/insights/blog/post/2020/09/11/what-is-the-gartner-magic-quadrant-and-why-does-it-matter/

[3] - S. Leaden, Genesys, November 2020, [Online] Available: https://www.genesys.com/blog/post/how-to-leverage-the-gartner-magic-quadrant-in-your-decision-making-process

[4] - Version 2, May 2021, [Online] Available: https://version-2.com/en/2021/05/the-importance-of-gartners-magic-quadrant/

[5] - D. Athow, TechRadar, June 2021, [Online] Available: https://www.techradar.com/news/best-small-business-servers

[6] - Akamai, May 2019, [Online] Available: https://www.akamai.com/site/en/documents/product-brief/application-load-balancer-cloudlet-product-brief.pdf

[7] - Akamai, July 2016, [Online] Available: https://www.akamai.com/newsroom/press-release/akamai-wins-anti-ddos-solutions-vendor-of-the-year.

[8] - E. Patriciono, IBM, [Online] Available:

https://www.ibm.com/cloud/architecture/articles/well-architected-framework/reliability-factors

[9] - Fortinet, [Online] Available:
https://www.fortinet.com/products/next-generation-firewall

[10] - Checkpoint, [Online] Available:
https://www.checkpoint.com/quantum/intrusion-prevention-system-ips/

[11] - Fortinet, [Online] Available:
https://www.fortinet.com/solutions/gartner-network-firewalls

[12] - G Rittenhouse, McAfee, February 2022, [Online] Available:
https://www.mcafee.com/blogs/enterprise/cloud-security/mcafee-enterprise-sse-named-a-leader-in-2022-gartner-magic-quadrant-for-sse/

[13] - Hammertoss: Stealthy Tactics Define a Russian Cyber Threat Group, Fireye, July 2014, [Online] Available:
https://www.mandiant.com/sites/default/files/2021-09/rpt-apt29-hammertoss-1-1.pdf

[14] - K.J. Higgins, Dark Reading, July 2015, [Online] Available:
https://www.darkreading.com/attacks-breaches/can-t-touch-this-hammertoss-russian-cyberspies-hide-in-plain-sight

[15] - D Cash, Volexity, May 2021, [Online] Available:
https://www.volexity.com/blog/2021/05/27/suspected-apt29-operation-launches-election-fraud-themed-phishing-campaigns/

[16] - S.Gatlan, Bleeping Computer, July 2021, [Online] Available:
https://www.bleepingcomputer.com/news/security/doj-solarwinds-hackers-breached-emails-from-27-us-attorneys-offices/

[17] - A. Bakker, Log4shell, 2021, [Online] Available:
https://log4shell.tools/

[18] - Kozmer, 2021, [Online] Available:
https://github.com/kozmer/log4j-shell-poc

[19] - Mitre, [Online] Available:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2021-44228

[20] - Checkpoint, December 2021, [Online] Available:
https://blog.checkpoint.com/2021/12/11/protecting-against-cve-2021-44228-apache-log4j2-versions-2-14-1/

[21] - Microsoft, December 2021, [Online] Available:
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[22] - S. Gallagher, Sophos, December 2021, [Online] Available:
https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/

[23] - A. Bolshev, F-Secure, 2021, [Online] Available:
https://labs.f-secure.com/assets/BlogFiles/Printing-Shellz.pdf

[24] - Avertium, December 2021, [Online] Available:
https://www.avertium.com/blog/wormable-security-vulnerability-found-in-hp-printer-models#:~:text=Vulnerability%20CVE%2D2021%2D39237%20is,lead%20to%20potential%20information%20disclosure.

[25] - HP, November 2021, [Online] Available:
https://support.hp.com/us-en/document/ish_5000383-5000409-16/hpsbpi03749

[26] - NIST, 2021, [Online] Available:
https://nvd.nist.gov/vuln/detail/CVE-2021-39237

[27] - Quocirca, 2021 [Online] Available:
https://www.myq-solution.com/files/2022/01/quocirca-print-security-2022-excerpt-report-myq.pdf

[28] - N. Goud, Cybersecurity Insiders, [Online] Available:
https://www.cybersecurity-insiders.com/cyber-attack-launched-on-150000-printers-working-worldwide/

[29] - T. Seals, ThreatPost, July 2019, [Online] Available:
https://threatpost.com/office-printers-hackers-open-door/147083/

[30] - SecureTeam, November 2021, [Online] Available:
https://secureteam.co.uk/news/what-is-a-printjack-attack/

[31] - HP, 2021 [Online] Available:
https://support.hp.com/us-en/document/ish_5000383-5000409-16/hpsbpi03749

[32] - J. Cran, Rapid7, May 2018, [Online] Available:
https://www.rapid7.com/db/modules/auxiliary/scanner/mysql/mysql_authbypass_hashdump/

[33] - H.D. Moore, June 2012, [Online] Available:
https://www.rapid7.com/blog/post/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql/

[34] - National Cyber Security Centre, July 2020, [Online] Available:
https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

[35] - Lenovo, [Online] Available:
https://www.lenovo.com/us/en/thinkpad-milspec/?orgRef=https%253A%252F%252Fwww.google.com%252F

[36] - A.Kapoor, Inse Journal, July 2019, [Online] Available:
http://insejournal.co.in/vulnerability-chaining.html