1. [Perimeter Basics](#PerimeterBasics)
2. [DMZ](#DMZ)
3. [Domain Spoofing](#DomainSpoofing)
4. [Endpoints](#Endpoints)
5. [Firewalls](#Firewalls)
6. [Intrusion Detection System](#IntrusionDetectionSystem)
7. [Intrusion Prevention](#IntrusionPrevention)
8. [VPN](#VPN)
9. [SSL VPN](#SSL_VPN)
10. [HoneyPot User](#HoneyPotUser)
11. [PowerShell Transcript](#PowerShellTranscript)
12. [Parallel Pipelining](#ParallelPipelining)
13. [Create Macro](#CreateMacro)
14. [AD Hardening](#ADHardening)
15. Perimeter Basics

**Securing Your Network Perimeter**  - Cybercriminals are always on the lookout for weaknesses in one’s network. Since companies today allow data access to several employees, partners, and consumers for efficiency, it exposes the network to multiple threats.

**What is a Network Perimeter?**  - A network perimeter is a boundary between the internal network and the Internet. It is the edge of what a company has control over. In perspective, it’s like a virtual wall that allows and prevents specific aspects based on rules and policies.

**Network Perimeter includes the following:**

**Firewalls:** A firewall can either be hardware, software, or both. It serves as the first line of defense in network security wherein it monitors inbound and outbound network traffic and decides whether to block or allow it based on security policies.

Some types of firewalls include:

* Proxy firewall
* Stateful Inspection Firewall
* Unified Threat Management Firewall
* Virtual Firewall

**Importance of Network Perimeter**  - In today’s business environment, we rely heavily on our devices to stay connected and our dependence on network security has increased due to the growing number of cyberattacks. However, as businesses expand, so are the location and the addition of devices and many of which are being used outside the network perimeter, then, presents a problem when it comes to security.

Since most people can now work anywhere, data can be shared and collected on a massive scale and the security team’s capacity to monitor all these data could be out of control. The concept of network perimeter will allow your organization to think strategically about how you can protect critical internal data from external threats.

So, how can you secure your network perimeter?

A picture containing text, parking

Description automatically generated

**Creating a Secure Network Perimeter**  - The security of your network perimeter is an important defense to safeguard important data. Understanding that having multiple layers of security is important since threats and other potential risks can evolve.

Here are some best practices:

**Strengthen device configurations and update software**

The first line of defense is to have a solid foundation or wall to [prevent attackers from penetrating the system](https://mcas-proxyweb.mcas.ms/certificate-checker?login=false&originalUrl=https%3A%2F%2Funiserveit.com.mcas.ms%2Fblog%2Freasons-why-software-updates-are-important-for-your-business%3FMcasTsid%3D15600&McasCSRF=3865d4ed019f6d5cb6744af2fb635a38ee6d0d4c2e47fcdcc329d1f0f782f9eb). This typically includes network security devices such as firewalls, routers that serve as the guard to your system.

Each software, device, or operating system you are using to protect your network should be kept up to date and properly configured. One frequent problem among organizations is being complacent with all the layers of security they have but one misstep can already give a cybercriminal entry to your system.

What is a Network Perimeter?  - A network perimeter is the secured boundary between the private and locally managed side of a network, often a company’s intranet, and the public facing side of a network, often the Internet.

A network perimeter includes:

* **Border Routers:** Routers serve as the traffic signs of networks. They direct traffic into, out of, and throughout networks. The border router is the final router under the control of an organization before traffic appears on an untrusted network, such as the Internet.
* **Firewalls:** A firewall is a device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic.
* **Intrusion Detection System (IDS):** This functions as an alarm system for your network that is used to detect and alert on suspicious activity. This system can be built from a single device or a collection of sensors placed at strategic points in a network.
* **Intrusion Prevention System (IPS):** Compared to a traditional IDS which simply notifies administrators of possible threats, an IPS can attempt to automatically defend the target without the administrator's direct intervention.
* **De-Militarized Zones / Screened Subnets:** DMZ and screened subnet refer to small networks containing public services connected directly to and offered protection by the firewall or other filtering device.

Network Perimeter Requirements

For most modern businesses, there is no single defensible boundary between a company’s internal assets and the outside world.

* Internal users are not simply connecting from inside an organization’s building, network, or inner circle. They are connecting from external networks and using mobile devices to access internal resources.
* Data and applications are no longer housed on servers that businesses physically own, maintain, and protect. Data warehouses, cloud computing, and software as a service present immediate access and security challenges for both internal and external users.
* Web services have opened a wide door to interactions outside of normal trust boundaries. To serve multiple clients, or simply to communicate with other services, both internal and external, insecure interactions on external platforms occur all the time.

Also, individually protecting each software application, service, or asset can be quite challenging. While the concept of a “network perimeter” has meaning for certain network configurations, in today’s environment it should be treated abstractly, rather than as a specific setup.

**Network Perimeter Guidelines  -** With this in mind, there are a few guidelines that can help to deliver a secure and modular network environment:

* Strong authentication to allow controlled access to information assets. Two factor authentication acts as an extra layer of security for logins, ensuring that attempted intrusions are halted before any damage is done.
* Hardening of mobile and IoT devices that connect to the network. Access control policies define high-level requirements that determine who may access information, and under what circumstances that information can be accessed.
* Embedded security services inside devices and applications. Embedded security solutions can help protect devices ranging from atm’s to automated manufacturing systems. Features including application whitelisting, antivirus protection, and encryption can be embedded to help protect otherwise exposed IoT devices.
* Collecting security intelligence directly from applications and their hosts. Maintaining an open communication line with cloud service providers like AWS can greatly increase security protections. Application and service managers understand how to integrate shared security with their systems better than anyone else.

Why a Network Perimeter is Important  - The increasing reliance on an interconnected ecosystem of online devices in today's business environment has greatly increased our reliance on network security in order to prevent cyber attacks. Data is collected, collated, and interpreted on a massive scale, and it’s security is dependent on the protections that surrounds it. The concept and evolution of a network perimeter allows organizations to think effectively on how to safeguard their internal information from untrusted or malicious actors.

1. DMZ

**De-Militarized Zones:** The purpose of DMZ is to enable access to resources from the untrusted network while keeping the system or host on an internal private network secure. Resources that are commonly placed within the DMZ are Mail servers, [FTP servers](https://mcas-proxyweb.mcas.ms/certificate-checker?login=false&originalUrl=https%3A%2F%2Fsource.raysync.io.mcas.ms%2Fnews%2Fwhat-is-ftp-server-and-how-does-it-work%3FMcasTsid%3D15600&McasCSRF=3865d4ed019f6d5cb6744af2fb635a38ee6d0d4c2e47fcdcc329d1f0f782f9eb), Web servers, and VoIP servers.

**Segmenting the DMZ**  - Firewall rules should be tightened to only allow traffic to necessary services within the DMZ, so you need to configure the DMZ managed by the security system. One rule is to allow source IP addresses to specific servers and add proxies within the network from which admins are allowed access. Also, consider segmenting systems within the DMZ to limit the effect if the system is breached.

The first step to protect your data is to secure your network perimeter effectively. A multi-level defense system is strongly recommended to reduce cyberattacks on your internal network. If you want to check the efficiency and improve your network perimeter’s security

What is a DMZ Network?  - In computer security, a DMZ Network (sometimes referred to as a “demilitarized zone”) functions as a subnetwork containing an organization's exposed, outward-facing services. It acts as the exposed point to an untrusted networks, commonly the Internet.

The goal of a DMZ is to add an extra layer of security to an organization's local area network. A protected and monitored network node that faces outside the internal network can access what is exposed in the DMZ, while the rest of the organization's network is safe behind a firewall.

When implemented properly, a DMZ Network gives organizations extra protection in detecting and mitigating security breaches before they reach the internal network, where valuable assets are stored.

Purpose of a DMZ  - The DMZ Network exists to protect the hosts most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network, the most common examples being email, web servers, and DNS servers. Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of the network if they become compromised.

Hosts in the DMZ have tightly controlled access permissions to other services within the internal network, because the data passed through the DMZ is not as secure. On top of that, communications between hosts in the DMZ and the external network are also restricted to help increase the protected border zone. This allows hosts in the protected network to interact with the internal and external network, while the firewall separates and manages all traffic shared between the DMZ and the internal network. Typically, an additional firewall will be responsible for protecting the DMZ from exposure to everything on the external network.

All services accessible to users on communicating from an external network can and should be placed in the DMZ, if one is used. The most common services are:

* **Web servers:** Web servers responsible for maintaining communication with an internal database server may need to be placed into a DMZ. This helps ensure the safety of the internal database, which is often storing sensitive information. The web servers can then interact with internal database server through an application firewall or directly, while still falling under the umbrella of the DMZ protections.
* **Mail servers:** individual email messages, as well as the user database built to store login credentials and personal messages, are usually stored on servers without direct access to the internet. Therefore, an email server will be built or placed inside the DMZ in order to interact with and access the email database without directly exposing it to potentially harmful traffic.
* **FTP servers:** These can host critical content on an organization's site, and allow direct interaction with files. Therefore, an FTP server should always be partially isolated from critical internal systems.

A DMZ configuration provides additional security from external attacks, but it typically has no bearing on internal attacks such as sniffing communication via a packet analyzer or spoofing via email or other means.

DMZ Designs  - There are numerous ways to construct a network with a DMZ. The two major methods are a single firewall (sometimes called a three-legged model), or dual firewalls. Each of these system can be expanded to create complex architectures built to satisfy network requirements:

* **Single firewall:** A modest approach to network architecture involves using a single firewall, with a minimum of 3 network interfaces. The DMZ will be placed Inside of this firewall. The tier of operations is as follows: the external network device makes the connection from the ISP, the internal network is connected by the second device, and connections within the DMZ is handled by the third network device.
* **Dual firewall:** The more secure approach is to use two firewalls to create a DMZ. The first firewall (referred to as the “frontend” firewall) is configured to only allow traffic destined for the DMZ. The second firewall (referred to as the “backend” firewall) is only responsible for the traffic that travels from the DMZ to the internal network. An effective way of further increasing protection is to use firewalls built by separate vendors, because they are less likely to have the same security vulnerabilities. While more effective, this scheme can be more costly to implement across a large network.

Why DMZ Networks are Important  - On many home networks, internet enabled devices are built around a local area network which accesses the internet from a broadband router. However, the router serves as both a connection point and a firewall, automating traffic filtering to ensure only safe messages enter the local area network. So, on a home network, a DMZ can built by adding a dedicated firewall, between the local area network and the router. While more expensive, this structure can help to protect internal devices from sophisticated attacks better protects the inside devices from possible attacks by the outside.

DMZ’s are an essential part of network security for both individual users and large organizations. They provides an extra layer of security to the computer network by restricting remote access to internal servers and information, which can be very damaging if breached.

1. Domain Spoofing

What is Domain Spoofing?  - Domain spoofing, a common form of phishing, occurs when an attacker appears to use a company’s domain to impersonate a company or one of its employees.

This can be done by sending emails with false domain names which appear legitimate, or by setting up websites with slightly altered characters that read as correct. Commonly, a spoof website or email will use logos, or any other kind of accurate visual design to effectively imitate the styling and branding of a legitimate enterprise or business. Users will commonly be prompted to enter financial details or other sensitive data, trusting that they are being sent to the right place.

**Domain Spoofing Classifications**

**Email Spoofing:** forging of an email header so that the message seems to originate from someone or somewhere different from the actual source. Email spoofing is a scheme used in both phishing and spam campaigns because users don't want to open an email if they don’t trust the legitimacy of the source. The purpose of email spoofing is to trick recipients into opening, or even corresponding with a solicitation.

**Website spoofing:** Website spoofing is the act of building a fake website with the goal of misleading users, gaining their trust, and assuming the identity of a legitimate group or organization. The spoof website will frequently adopt the design of the target website and sometimes mimic the URL with alternate characters.

A more sophisticated attack can involve the perpetrator building a ‘shadow’ version of the World Wide Web by routing all of the user’s web traffic through the attackers console. This type of attack captures all of the victims sensitive information. Another method used by domain spoofing attackers is to use a cloaked URL. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual website.

Email Spoofing Solutions  - Email spoofing is possible because the Simple Mail Transfer Protocol (SMTP) does not provide a mechanism for address authentication. Although email address authentication protocols and mechanisms have been specified to battle email spoofing, adoption of those mechanisms has been slow.

* **Sender Policy Framework (SPF):** an email validation system, SPF allows domain managers to authorize individual hosts to use a domain in email. This list of approved domain names in protected, and can be used to verify authenticity.
* **Domain-based Message Authentication, Reporting and Conformance (DMARC):** is an email authentication protocol based on reporting and enforcement components. Built on two components, reporting and enforcement. Through reporting, DMARC can automate authenticity verification, and alert administrators to false email domains immediately. When false domains are used DMARC will stop the email from entering the inbox.
* **DomainKeys Identified Mail:** (DKIM) which provides a way to validate a domain name identity associated with a message. When a message is built, a digital signature is added to the email to ensure authenticity. DKIM does not offer filtering capabilities, but can be used to guarantee legitimacy of the message.
* **Sender ID (SID):** a protocol based largely on SPF and promoted by Microsoft, SID is built into exchange servers, by reading the SMTP header. The service the queries the DNS records to verify the sender's address.

Why Domain Spoofing is Important  - Experts recommend that users only access financial sites and other sensitive sites directly through a main page or other verified avenue in order to avoid being cheated by a spoof website. According to the FTC, over 96% of companies operating today suffer from domain spoofing attacks in one form or another. Therefore, having the right solutions in place to protect against the possibility of an attack is a necessity for any person or business.

1. Endpoints

What is an Endpoint Device?  - An endpoint device is a LAN- or WAN-connected hardware device that communicates across a network. Broadly speaking, the term can refer to any network connected device: desktop computers, laptops, smartphones, tablets, printers, or other specialized hardware like POS terminals or retail kiosks, that act as a user endpoint in a distributed network. The term is more specifically applies to Internet-connected hardware found on a TCP/IP network.

One of the biggest issues with endpoint devices involves comprehensive security for a network or enterprise system. Security managers must determine whether various endpoint devices could be security gaps for a network – that is, whether unauthorized users can access an endpoint device and use it to pull off important or sensitive data.

Endpoint Device Security Challenges - A policy-based approach to network security is paramount when safeguarding a network. The policy should require endpoint devices to meet specific criteria before being granted access to network resources. Security architecture is designed to handle endpoint devices in order to safeguard the data assets accessed through these systems.

Companies that allow employees to bring their own device, as in laptops or smartphones, frequently face endpoint device security issues. Without a well-considered bring your own device (BYOD) policy, employee-owned devices may compromise the security of company information, or of the network.

Organizations believe that [close to 45%](https://mcas-proxyweb.mcas.ms/certificate-checker?login=false&originalUrl=https%3A%2F%2Fwww.code42.com.mcas.ms%2Fnews-releases%2F2016-03-15-one-in-four-it-professionals-say-companies-are-not-doing-enough-to-protect-data%2F%3FMcasTsid%3D15600&McasCSRF=3865d4ed019f6d5cb6744af2fb635a38ee6d0d4c2e47fcdcc329d1f0f782f9eb) of corporate data is held on endpoint devices. These laptops, tablets and smartphones pose a huge risk to data security.

The industry-wide growth of endpoint device exposure means that it’s easier than ever for data to be put at risk. Each time an employee connects over public WiFi, downloads a suspicious app, or is targeted by a phishing scam, the risk is amplified.

This is especially important because endpoint devices not only expose their data to possible seizure, they also serve as a potential conduit for a network wide breach of security.

Endpoint Device Weaknesses - Security policies, especially as they relate to BYOD protections, are an essential part of protecting endpoint devices from being exposed to attack. But the largest contributor to vulnerability is the quality of training and awareness given to employees. Bad habits can have a serious effect on the integrity of a secure network:

* **Lost or improperly decommissioned devices:** Employees who lose devices that are connected to the company network may expose that network to attacks.
* **Poor adoption of security updates:** Out-of-date operating systems and applications can lead to any number of vulnerabilities within a device that has been given access to sensitive company information.
* **Employees switching encryption off/on:** people are more likely to adjust the security controls on devices they own, and will rework settings to suit their needs. This can lead to unwanted access points.

With a proactive, always on’ technology, IT can avoid these types of issues, while maintaining compliance and mitigating risk.

Managing Endpoint Device Security  - Traditionally, endpoint security systems are built on the framework of a client-server model. The security program is managed by a central server that controls the client program installed on all network drives. More recently, with the increasing adoption of software as a service platforms (SaaS), the program and host server are both managed remotely by the SaaS provider. This business model gives organizations a chance to lower costs while ensuring constant updates to security parameters.

Why Endpoint Devices are Important - Endpoint security management is a necessary part of ensuring a secure network. Proper controls can help to identify and manage user access over a personal or corporate network, giving security services the time they need to locate and deter possible threats.

1. Firewalls

**Firewalls:** A firewall can either be hardware, software, or both. It serves as the first line of defense in network security wherein it monitors inbound and outbound network traffic and decides whether to block or allow it based on security policies.

Some types of firewalls include:

* Proxy firewall
* Stateful Inspection Firewall
* Unified Threat Management Firewall
* Virtual Firewall

1. Intrusion Detection System

I**ntrusion Detection System:** The IDS detects and notifies your systems for any malicious events or policy violations. An IDS can be host-based or network-based depending on its environment.

* **Host-Based IDS:** Designed for specific endpoint and protect it against internal and external threats. A host-based IDS is limited only to its host machine, but it allows deep visibility to monitor traffic to and from the machine.
* **Network-Based IDS:** Designed for monitoring an entire network. It provides wider visibility into the traffic flowing through the network and has the ability to uncover extensive threats. However, this system doesn’t have deep visibility into the endpoints they protect.

1. Intrusion Prevention

**Intrusion Prevention System:** This system is designed to monitor intrusions and prevent threats from developing. The system monitors your network continuously and scans for possible risk to gather more information and administer the proper preventative actions. This system can be used to identify violations against rules and policies.

1. VPN - **Virtual Private Network**

VPN’s employing data encryption can enable users outside of the network to access the internal network. Passwords are essential but most breaches are a result of weak password or password theft, thus, utilizing [two-factor authentication](https://mcas-proxyweb.mcas.ms/certificate-checker?login=false&originalUrl=https%3A%2F%2Funiserveit.com.mcas.ms%2Fblog%2Fauthenticator-app-microsoft-or-google%3FMcasTsid%3D15600&McasCSRF=3865d4ed019f6d5cb6744af2fb635a38ee6d0d4c2e47fcdcc329d1f0f782f9eb) to ensure identification and integrity of the user trying to connect to the network is necessary.

1. SSL\_VPN

What is an SSL VPN? - A Secure Socket Layer Virtual Private Network (SSL VPN) lets remote users access Web applications, client-server apps, and internal network utilities and directories without the need for specialized client software. SSL VPN’s provide safe communication for all types of device traffic across public networks and private networks.

All traffic between a Web browser and SSL VPN device is encrypted with the SSL protocol, or its successor protocol (TLS). SSL VPN’s solve the long standing frustrations found within both the traditional Wide Area Network (WAN) as well as IPSEC based VPNs. This ease of use quality allows for greater work efficiency, lowering costs and increasing employee and business practices. When properly used SSL VPN’s do not impact security network at all.

SSL VPN Types

There are two major types of SSL VPNs:

* **SSL Portal VPN** - This type of SSL VPN allows for a single SSL connection to a website, through which a user can access a variety of private network services. The SSL VPN type is called a “portal” because it is essentially a single web page that leads to many other resources. Users can generally access this gateway using any modern browser, only requiring the identification and password provided by gateway service.
* **SSL Tunnel VPN** - This alternative type of SSL VPN allows a Web browser to securely access multiple network services that may not just be web-based, through a tunnel that is running under SSL. SSL tunnel VPNs necessitate a browser which can interact with and display active content increasing the versatility over just a simple SSL Portal VPN. Active content can mean anything from JavaScript to Flash based technology.

IPSEC VPN versus SSL VPN Technology  - Traditional VPN’s rely on IPSec (Internet Protocol Security) to tunnel between the two endpoints. IPSec works on the Network Layer of the OSI Model and must be managed deep within the actual OS network code, rather than within an software application. When connected through an IPSec VPN, the client computer is for all intents and purposes mimicking the qualities of terminal within the corporate network, allow to access anything an internal computer could. Most IPSec VPN solutions require either third-party hardware or software to be installed to interface with the network.

The main benefit of an IPSEC based VPN is the extra layer of security inherent to a system which requires specific and compatible hardware to run properly. This removes the ease of access that so often allows cyber criminals to attack exposed networks.

On the flipside, one of the cons is that it can be pretty heavy burden on a business to pay for and maintain the licenses for both the initial software installation, not to mention the tech support needed to maintain and update said software. This issue can be exacerbated even further if onsite installation isn’t always possible.

SSL is a common protocol and supported by most modern web browsers without any additional installations needed. At this point, an overwhelming majority of internet accessible computers already have the “client software” necessary to connect through an SSL VPN.

Another major benefit of SSL based VPNs is that they allow tunneling to specific applications, when network wide access is unnecessary. This is a great security and data safety feature. Not only that, but within the SSL framework, it is much easier to assign different administrative rights to users depending on the their seniority and access needs.

One of the benefits of SSL VPN can also be a hindrance when considering security. The fact that a VPN is simply accessed through a web browser means that only web based applications are useable within a the VPN without intensive technical customization, customization which defeats some of the benefits allowed by SSL VPNs.

Another issue with SSL VPN’s relates to the inherent security of its terminal. Web browsers are susceptible to malware downloads, so a VPN with an open SSL terminal might have a chance of becoming infected. Not only that but the digital gateway of a webpage gives hackers a more direct line of sight for where to attack if they want to access sensitive information of any kind.

Why an SSL VPN is Important

As VPNs in general become a much larger part of corporate and educational environments, simplifying and expanding the ease of use will become paramount. SSL VPN’s are useable by people with little to no computer literacy, are accessible from within any modern personal computer or device, and can be configured to be as secure as the IPSEC VPN protocol that preceded it. Businesses that can exist globally have access to a wider network of employees, and can expand securely without the overhead and knowledge required by more antiquated VPN technologies.

1. HoneyPot User

4662 – an operation was performed on an object. Active Directory logs this event when a user accesses an AD OBject

Can be uesd to create a honeypot user, using and event that does not come up often, but for specific auditing, this log will happen when a user is enumerated.

View the current audit settings

> auditpol /get /category:\*

> auditpol /get /category:\* /success:enable /failure:enable

Instructions

* DC >> server manager >> tools >> AD users and computers
* 'View' >> Check the Advanced Features option
* Create users across the Organizational Units
* Ex: User Name     'AAALDAPcheck'
* Once the user is create right click on that user in their OU, select Properties
* If Advanced Features was checked, the nuser now has a 'Security' tab in the properties.
  + Click on the Security tab >> Advanced
* Then click the 'Auditing' tab then the 'Add' button
  + Adjust the settings to:
    - 'Principal' = 'Everyone'
    - 'Applies to' = 'This object only'
    - 'Permissions' = 'Read all properties'
  + Apply >> OK

Now with this user created and settings applied, now an EventID 4662 will be logged in the DC any time that one of these honeypot users is enumerated.

Examples of enumerating users:

External: Bloodhound, nmap

Or:

CMD> net user

That will list all users

Or get specific:

CMD> net user AAALDAPcheck

PowerShell> get-localuser

s

1. PowerShell Transcript

OTS Over the Shoulder Transcription

1. PS:> gpedit.msc
2. Go to:
   1. User Configuration >> Administrative Templates >> Windows PowerShell
3. Check "Enabled"
4. Set the results directory
5. Check "Include Invocation headers"
6. Click OK

Now this will save transcripts for any action in PowerShell

You can also add "Start-Transcript –Path $transcriptPath" to the PowerShell profile.

So now, if you are running the FolderWatcher, and actions that happen and are stated in the PowerShell terminal will then also be saved to the transcript.

1. Parallel Pipelining

Powershell 7 introduced the new parallel parameter for the ForEach-Object cmdlet, which allows you to run a script block in parallel for each element in a collection.

In prior versions of Powershell, if you pass an array of 10 objects such as event logs, it would run the code for eac hobject in sequential series. If we sent an array with numbers 1-10 and put the program to sleep for 1second each, it would be approximately 10 seconds.

But with PS7 we can run this in parallel even though it is an array. We can also set a throttle limit to make sure that the processes don't overstep their capabilities. So here, if we set the throttle limit to 10, then each member of the array will run in parallel and the entire process, even though each array member is still sleeping for 1second, it will fully complete in about 1 second as all 10 array members go in parallel.

If done correctly and accounting for a systems resources, this can greatly speed up a process especially when doing something like searching through different event logs.

1. Create Macro

View >> Macros >> View Macros (excel, word, etc)

Run or Edit  or Step into or Create after name with no spaces is entered

If they exist already, right click on sheet >>View Code

NOTE the examples below are not directly connected. We just pulled bits and pieces out or our Endpoint Training

We work on a 'Module'

Call SetGlobalVariables

Dim ws As Worksheet

Set ws = Worksheets("SANSC15")

Dim row As Integer, col As Integer

Dim theButton As Object

With theButton.TopLeftCell

row = .row

col = .Column

End With

Dim userArray() As String

Dim rng As Range

Set rng = ActiveSheet.Range("B3:B100")

If (IsEmpty(ws.Range("A" & row).Value)) Then

UserArray = Split(users, ";"

End If

1. AD Hardening

* Block Int. Access for DCs
* DC Audit (event logs)
* GP Settings
* Only Software and services that support AD
* Patch and Config. Management
* Perim. Firewall Restrictions – Block outbound Cons
* RDP Restrict
* Open DNS Zone Transfer Hardening
* SMB Usage