What is security audit

A cybersecurity audit involves a comprehensive analysis and review of the IT infrastructure of your business. It detects vulnerabilities and threats, displaying weak links, and high-risk practices. It is a primary method for examining compliance. It is designed to evaluate something (a company, system, product, etc.)

What is a cyber security audit?

A cyber security audit is a systematic and independent examination of an organization's cyber security. An audit ensures that the proper security controls, policies, and procedures are in place and working effectively.

Your organization has a number of cyber security policies in place. The purpose of a cyber security audit is to provide a 'checklist' in order to validate your controls are working properly. In short, it allows you to inspect what you expect from your security policies.

The objective of a cyber security audit is to provide an organization's management, vendors, and customers, with an assessment of an organization's security posture.

Audits play a critical role in helping organizations avoid cyber threats. They identify and test your security in order to highlight any weaknesses or vulnerabilities that could be expolited by a potential bad actor.

What does an audit cover?

A cyber security audit focuses on cyber security standards, guidelines, and policies. Furthermore, it focuses on ensuring that all security controls are optimized, and all compliance requirements are met.

Specifically, an audit evaluates:

- Operational Security (a review of policies, procedures, and security controls)

- Data Security (a review of encryption use, network access control, data security during transmission and storage)
- System Security (a review of patching processes, hardening processes, role-based access, management of privileged accounts, etc.)
- Network Security (a review of network and security controls, anti-virus configurations, SOC, security monitoring capabilities)
- Physical Security (a review of role-based access controls, disk encryption, multifactor authentication, biometric data, etc.)

Unlike a cyber security assessment, which provides a snapshot of an organization's security posture. An audit is a 360 in-depth examination of an organization's entire security posture.

Benefits of a cyber security audit

A cyber security audit is the highest level of assurance service that an independent cyber security company offers.

It provides an organization, as well as their business partners and customers, with confidence in the effectiveness of their cyber security controls. Unfortunately, internet threats and data breaches are more prevalent than ever before. As a result, business leaders and consumers increasingly prioritize and value cyber security compliance.

An audit adds an independent line of sight that is uniquely equipped to evaluate as well as improve your security.

Specfically the following are some benefits of performing an audit:

- Identifying gaps in security
- Highlight weaknesses
- Compliance
- Reputational value
- Testing controls
- Improving security posture
- Staying ahead of bad actors
- Assurance to vendors, employees, and clients
- Confidence in your security controls
- Increased performance of your technology and security

At aNetworks, we offer a 360 cyber security audit for organizations. Our audit consists of multiple compliance and vulnerability scans, security and risk assessments, and a myriad of other cyber security tools used to conduct an in-depth examination into an organization's cyber security.

If you are interested in performing a cyber security audit for your company, then please contact us for a free quote.

How often do you need security audits?

How often you will need to perform an audit depends on what compliance or security framework your business follows.

For instance, FISMA requires federal agencies to have audits twice a year. If you work with a federal agency, then you also must comply with FISMA.

Failure to comply with laws that require cyber security audits can result in fines and penalties.

Other compliance regulations require annual audits. Some require none. How often you perform audits is entirely dependent on what type of data your company works with, what industry you are in, what legal requirements you must follow, etc.

However, even if you are not required to perform an audit, most security experts recommend you perform at least one annual audit to ensure your controls are functioning properly.

If you are unsure whether you require an audit, then contact us and we will get you squared away.

Cyber security audit checklist

Your audit checklist will depend on your industry, size, and compliance framework. Therefore, each organization's checklist will vary.

However, there are some basic categories that every audit should include. Specifically, the following are essential categories to review:

- Inventory and control of hardware assets
- Inventory and control of software assets
- Continuous vulnerability management
- Controlled use of administrative privileges
- Secure configuration for hardware and software on mobile devices, laptops, workstations, and servers
- Maintenance, monitoring, and analysis of audit logs
- Email and web browser protection
- Malware defenses
- Limitation and control of network ports, protocols, and servers.

The above checklist is just a start. It's a beginner's guide to ensure basic security controls are both present and effective. If you don't have these controls in place yet, then don't worry. Cyber security is a marathon, not a sprint.

Hydra is **a parallelized network login cracker built in various operating systems like Kali Linux, Parrot and other major penetration testing environments**. Hydra works by using different approaches to perform brute-force attacks in order to guess the right username and password combination.

What is Hydra tool used for?

Hydra is a pre-installed tool in Kali Linux used **to brute-force username and password to different services such as ftp, ssh, telnet, MS-SQL, etc**

Nmap, the acronym for Network Mapper, is **an open-source security auditing and network scanning software designed by Gordon Lyon**. It is developed in such a way that it can quickly analyze massive networks as well as single hosts

1. Ping sweep: A simple Nmap scan that pings all accessible IP addresses to see which ones reply to ICMP (Internet Control Message Protocol). This Ping Sweep is great for people that need to know the quantity of IP addresses.
2. SYN Scan: It sends an SYN message through TCP to all target ports. If the system receives an acknowledgment back, a port has been opened. No answer indicates a closed or unavailable port.
3. TCP Scan: Like SYN scan, it uses the TCP layer to send packets to all ports. The distinction is that the acknowledgment packets complete the connection. The logs may readily locate the TCP scan and use additional computing power.
4. Idle Scan: This scan is used to see whether any malicious assaults are planned on a network. Nmap scans are relocated away from a port to look for malware. However, the external host should be assigned an IP address and a port.
5. RPC Scan: Hackers use Remote Procedure Calls (RPC) to render systems vulnerable to viral assaults. It is recommended to periodically scan a network for RPC commands, as these procedures may run on the system and gather data.
6. Windows Scan: When SYN packets are issued, the program searches the ports for acknowledgment packets. This scan detects any irregularities in the received ACK packets and helps identify which ports are malfunctioning.
7. Bounce Scan: This scan checks the File Transfer Protocol layer's security. FTP levels seldom accept packets, and if they do, they may be forwarded to an internal layer to access inside computers. Bounce scan evaluates the same flaw and determines if your FTP layer is vulnerable.

8. UDP Scan: This scan is mainly effective in Windows to see if the UDP layer is vulnerable. It is not always crucial to acquire a response from the UDP layer, but it is helpful to know whether any Trojan assaults are active.

9. FIN Scan: Like SYN Scan, the system that sends the packets receives a largely TCP FIN packet response. The system sending an RST packet is a false alarm, and users should not be concerned.

10. NULL Scan: This scan is beneficial for systems other than Windows that can readily detect packet types and react with TCP or NULL answers. Windows can't utilize NULL scans since they don't always work.

What Is Wireshark Used For?

Wireshark has many uses, including troubleshooting networks that have performance issues. Cybersecurity professionals often use Wireshark to **trace connections, view the contents of suspect network transactions and identify bursts of network traffic.**

What is Wireshark Used For?

Packet analysis software like Wireshark is used by entities that must remain informed about the state of security of their network, as such, the software is commonly used by governments, schools, and technology businesses.

Common Wireshark use cases include:

- Identify the cause of a slow internet connection
- Investigating lost data packets
- Troubleshooting latency issues
- Detecting malicious network activity
- Identify unauthorized data exfiltration
- Analyzing bandwidth usage
- Tracing voice over Internet (VoIP) calls over the network
- Intercepting Man-in-the-Middle (MITM) attacks

How to Use Wireshark

Before following a Wireshark tutorial, it's important to understand how networking systems work.

The OSI model (Open Systems Interconnection Model) is a framework that represents how network traffic is transferred and displayed to an end-user. It's comprised of 7 layers

- **Application (Layer 7)** - Displays the graphical User Interface (UI) - what the end-user sees
- **Presentation (Layer 6)** - Formats data to achieve effective communication between networked applications
- **Session Layer (Layer 5)** - Ensures connections between end-points are continuous and uninterrupted.
- **Transports Layer (Layer 4)** - Proxy servers and firewalls reside on this layer. Ensures error-free data transfer between each endpoint by processing TCP and UDP protocols. At this layer, Wireshark can be used to analyze TCP traffic between two IP addresses
- **Network Layer (Layer 3)** - Ensures routing data for routers residing on this network are error-free.
- **Data Link Layer (Layer 2)** - Identifies physical servers through two sub-layers, Media Access Control (MAC), and Logical Link Control (LLC).
- **Physical Layer (Layer 1)** - Comprised of all the physical hardware that processes network activity

To use correctly use Wireshark, you must be aware of the different proctors being processed at each OSI layer. This will help you decide which layer should be analyzed for each specific diagnostic requirement.

Here's a run-through of the protocols being processed at each OSI layer:

- **Application (Layer 7)** - SMTP, HTTP, FTP, POP3, SNMP
- **Presentation (Layer 6)** - MPEG, ASCH, SSL, TLS
- **Session Layer (Layer 5)** - NetBIOS, SAP
- **Transports Layer (Layer 4)** - TCP, UDP
- **Network Layer (Layer 3)** - IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
- **Data Link Layer (Layer 2)** - RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
- **Physical Layer (Layer 1)** - RS232, 100BaseTX, ISDN, 11.

- John the Ripper is a popular open source password cracking tool that combines several different cracking programs and runs in both brute force and dictionary attack modes.

- John the Ripper is often used in the enterprise to detect weak passwords that could put network security at risk, as well as other administrative purposes. The software can run a wide variety of password-cracking techniques against the

various user accounts on each operating system and can be scripted to run locally or remotely.

- Originally developed for Unix-derived systems, John the Ripper is available for most common platforms. The free and open source (FOSS) version is generally distributed as source code. A commercial version, John the Ripper Pro, is a more user-friendly version distributed as native code for a given system.

Wapiti tool

Wapiti is **an open source tool that scans web applications for multiple vulnerabilities including data base injections, file disclosures, cross site scripting, command execution attacks, XXE injection, and CRLF injection.** The database injection includes SQL, XPath, PHP, ASP, and JSP injections

Wapiti works with the following types of vulnerabilities:

- file expansion (local and remote, fopen, readfile);
- injection (PHP / JSP / ASP / SQL injection and XPath injection);
- XSS (Cross Site Scripting) (reflected and persistent);
- detection and execution of commands (eval(), system(), passtru());
- CRLF injection (split HTTP responses, session fixation);
- XXE (XML External Entity) embedding;
- SSRF (Server Side Request Forgery);
- use of known potentially dangerous files (thanks to the Nikto database);
- weak .htaccess configurations that can be bypassed;

- the presence of backup files that reveal confidential information (disclosure of the source code);
- Shellshock;
- open redirects;
- non-standard HTTP methods that can be allowed (PUT)

Autopsy. Autopsy® is **a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools**. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

Description

Autopsy is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).

The Sleuth Kit and Autopsy are both Open Source and run on UNIX platforms (you can use Cygwin to run them both on Windows). As Autopsy is HTML-based, you can connect to the Autopsy server from any platform using an HTML browser. Autopsy provides a "File Manager"-like interface and shows details about deleted data and file system structures.

Analysis Modes

- A dead analysis occurs when a dedicated analysis system is used to examine the data from a suspect system. In this case, Autopsy and The Sleuth Kit are run in a trusted environment, typically in a lab. Autopsy and TSK support raw, Expert Witness, and AFF file formats.
- A live analysis occurs when the suspect system is being analyzed while it is running. In this case, Autopsy and The Sleuth Kit are run from a CD in an untrusted environment. This is frequently used during incident response while the incident is being confirmed. After it is confirmed, the system can be acquired and a dead analysis performed.

Evidence Search Techniques

- File Listing: Analyze the files and directories, including the names of deleted files and files with Unicode-based names. (screenshot)
- File Content: The contents of files can be viewed in raw, hex, or the ASCII strings can be extracted. When data is interpreted, Autopsy sanitizes it to prevent damage to the local analysis system. Autopsy does not use any client-side scripting languages. (screenshot) (Sleuth Kit Informer #1)
- Hash Databases: Lookup unknown files in a hash database to quickly identify it as good or bad. Autopsy uses the NIST National Software Reference Library (NSRL) and user created databases of known good and known bad files. (screenshot)
- File Type Sorting: Sort the files based on their internal signatures to identify files of a known type. Autopsy can also extract only graphic images (including thumbnails). The extension of the file will also be compared to the file type to identify files that may have had their extension changed to hide them. (screenshot)
- Timeline of File Activity: In some cases, having a timeline of file activity can help identify areas of a file system that may contain evidence. Autopsy can create timelines that contain entries for the Modified, Access, and Change (MAC) times of both allocated and unallocated files. (screenshot)
- Keyword Search: Keyword searches of the file system image can be performed using ASCII strings and grep regular expressions. Searches can be performed on either the full file system image or just the unallocated space. An index file can be created for faster searches. Strings that are frequently searched for can be easily configured into Autopsy for automated searching. (screenshot)
- Meta Data Analysis: Meta Data structures contain the details about files and directories. Autopsy allows you to view the details of any meta data structure in the file system. This is useful for recovering deleted content. Autopsy will search the directories to identify the full path of the file that has allocated the structure. (screenshot)
- Data Unit Analysis: Data Units are where the file content is stored. Autopsy allows you to view the contents of any data unit in a variety of formats including ASCII, hexdump, and strings. The file type is also given and Autopsy will search the meta data structures to identify which has allocated the data unit. (screenshot)
- Image Details: File system details can be viewed, including on-disk layout and times of activity. This mode provides information that is useful during data recovery. (screenshot)

Case Management

- Case Management: Investigations are organized by *cases*, which can contain one or more *hosts*. Each host is configured to have its own time zone setting and clock skew so that the times shown are the same as the original user would have

seen. Each host can contain one or more file system images to analyze. (screenshot) (Sleuth Kit Informer #2)

- Event Sequencer: Time-based events can be added from file activity or IDS and firewall logs. Autopsy sorts the events so that the sequence of incident events can be more easily determined. (screenshot)
- Notes: Notes can be saved on a per-host and per-investigator basis. These allow you to make quick notes about files and structures. The original location can be easily recalled with the click of a button when the notes are later reviewed. All notes are stored in an ASCII file. (screenshot)
- Image Integrity: It is crucial to ensure that files are not modified during analysis. Autopsy, by default, will generate an MD5 value for all files that are imported or created. The integrity of any file that Autopsy uses can be validated at any time. (screenshot)
- Reports: Autopsy can create ASCII reports for files and other file system structures. This enables you to quickly make consistent data sheets during the investigation.
- Logging: Audit logs are created on a case, host, and investigator level so that actions can be easily recalled. The exact Sleuth Kit commands that are executed are also logged.
- Open Design: The code of Autopsy is open source and all files that it uses are in a raw format. All configuration files are in ASCII text and cases are organized by directories. This makes it easy to export the data and archive it. It also does not restrict you from using other tools that may solve the specific problem more appropriately.
- Client Server Model: Autopsy is HTML-based and therefore you do not have to be on the same system as the file system images. This allows multiple investigators to use the same server and connect from their personal systems.

Autopsy is written in Perl and runs on the same UNIX platforms as The Sleuth Kit:

- Linux
- Mac OS X
- Open & FreeBSD
- Solaris
- Cygwin (you cannot use the win32 executables that can be downloaded from this site, you must build in Cygwin)

- What Is Metasploit, and How Does It Work?

- Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

- The various tools, libraries, user interfaces, and modules of Metasploit allow a user to configure an exploit module, pair with a payload, point at a target, and launch at the target system. Metasploit's large and extensive database houses hundreds of exploits and several payload options.

What Is the Purpose of Metasploit?

Metasploit is a powerful tool used by network security professionals to do penetration tests, by system administrators to test patch installations, by product vendors to implement regression testing, and by security engineers across industries. The purpose of Metasploit is to help users identify where they are most likely to face attacks by hackers and proactively mend those weaknesses before exploitation by hackers.

Who Uses Metasploit?

With the wide range of applications and open-source availability that Metasploit offers, the framework is used by professionals in development, security, and operations to hackers. The framework is popular with hackers and easily available, making it an easy to install, reliable tool for security professionals to be familiar with even if they don't need to use it.

Metasploit Uses and Benefits

Metasploit provides you with varied use cases, and its benefits include:

- Open Source and Actively Developed – Metasploit is preferred to other highly paid penetration testing tools because it allows accessing its source code and adding specific custom modules.
- Ease of Use – it is easy to use Metasploit while conducting a large network penetration test. Metasploit conducts automated tests on all systems in order to exploit the vulnerability.
- Easy Switching Between Payloads – the set payload command allows easy, quick access to switch payloads. It becomes easy to change the meterpreter or shell-based access into a specific operation.
- Cleaner Exits – Metasploit allows a clean exit from the target system it has compromised.

- Friendly GUI Environment – friendly GUI and third-party interfaces facilitate the penetrate testing project.

What Tools Are Used in Metasploit?

Metasploit tools make penetration testing work faster and smoother for security pros and hackers. Some of the main tools are Aircrack, Metasploit unleashed, Wireshark, Ettercap, Netsparker, Kali, etc.

Metasploitable 2

Its is a test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine (VM) is compatible with VMWare, VirtualBox, and other common virtualization platforms.

What is Cyber Security?

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim's device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

Dridex malware

In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global **Dridex malware attack**. This malicious campaign affected the public, government, infrastructure and business worldwide.

Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.

In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

Romance scams

In February 2020, the FBI warned U.S. citizens to be aware of confidence fraud that cybercriminals commit using dating sites, chat rooms and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data.

The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million.

Emotet malware

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.
Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

Update your software and operating system: This means you benefit from the latest security patches.
Use anti-virus software: Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
Use strong passwords: Ensure your passwords are not easily guessable.
Do not open email attachments from unknown senders: These could be infected with malware.
Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.
Avoid using unsecure WiFi networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.