

MIS 4596

Managing Enterprise Cybersecurity

Malware Analysis

Unit #22

Agenda

- Computer virus
- Malicious software
- Proliferation of malware
- Malware components
- Anti-malware components
- Best practices for protection
- Milestone 4 instructions

Virus

Virus: attached to a file

1986

Brain virus

an F-Secure Production

BRAIN

Malicious Software (Malware)

Malware enables unauthorized access to networks for purposes of theft, sabotage, or espionage

- There are many types of malware, many cyberattacks use a combination of several types to achieve their goals
 - Obtain sensitive information (login credentials, credit card data, Social Security numbers, ...)
 - Gain unauthorized access to systems
 - Carry out a profit-oriented scheme
- Usually introduced into a network through phishing, attachments, downloads, or may gain access through social engineering or flash drives
- Manual attacks on information systems are less common than the used to be
 - >95% of all compromises use email as the main attack vector

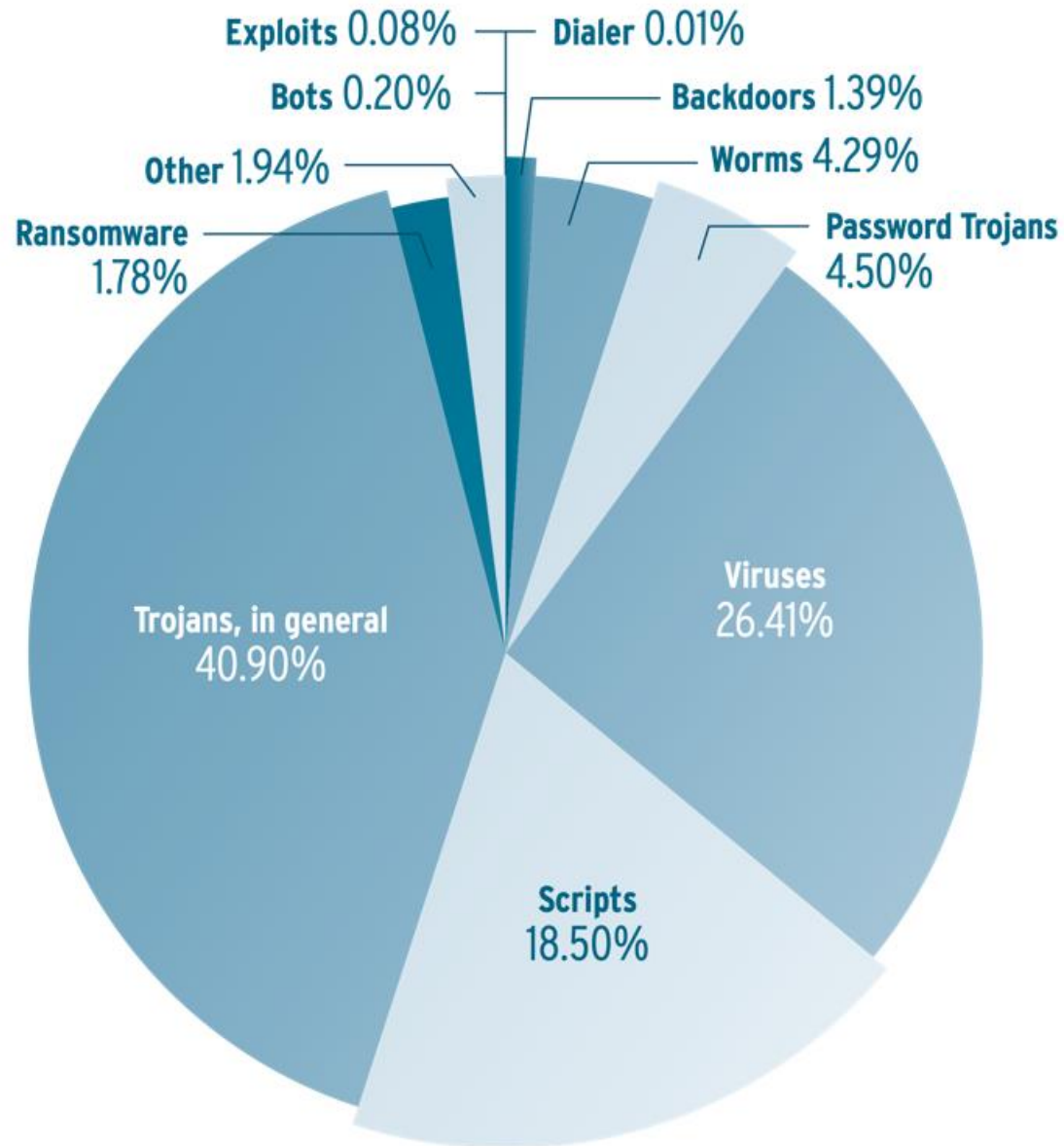


Types of malware

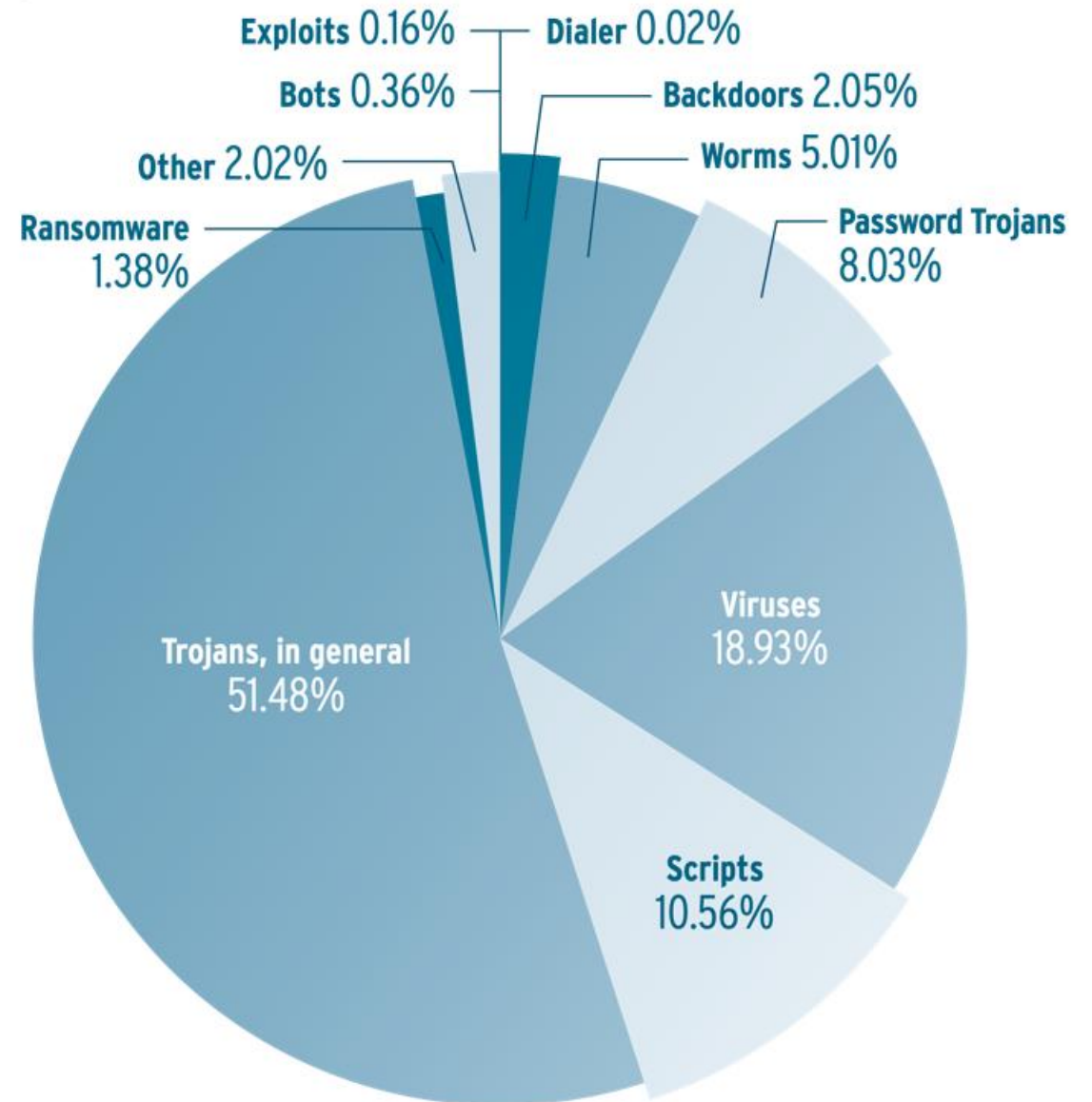
Type	What It Does	Real-World Example
Ransomware	disables victim's access to data until ransom is paid	RYUK
Fileless Malware	makes changes to files that are native to the OS	Astaroth
Spyware	collects user activity data without their knowledge	DarkHotel
Adware	serves unwanted advertisements	Fireball
Trojans	disguises itself as desirable code	Emotet
Worms	spreads through a network by replicating itself	Stuxnet
Rootkits	gives hackers remote control of a victim's device	Zacinlo
Keyloggers	monitors users' keystrokes	Olympic Vision
Bots	launches a broad flood of attacks	Echobot
Mobile Malware	infects mobile devices	Triada

<https://www.crowdstrike.com/epp-101/types-of-malware/>

Distribution of malware under Windows 2017



Q1 2018



Ransomware

- Software that uses encryption to disable a target's access to its data until a ransom is paid
 - The victim organization is rendered partially or totally unable to operate until it pays
 - There is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly

```
Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
wowsmith123456@posteo.net. Your personal installation key:

zRNagE-CDBMfc-pD5A14-vFd5d2-14mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.
Key: _
```

In 2019 the city of Baltimore was hit by a type of ransomware named RobbinHood which was distributed using the National Security Agency's Eternal Blue hacking tool

- The attack halted all city activities, including tax collection, property transfers, and government email for weeks, and cost the city more than \$18 million
- The same type of malware was used against the city of Atlanta in 2018, resulting in costs of \$17 million

Fileless Malware

- Does not install anything initially, instead, it makes changes to files that are native to the operating system, such as PowerShell
 - Because the operating system recognizes the edited files as legitimate, a fileless attack is not caught by antivirus software
 - Because these attacks are stealthy, they are up to 10 times more successful than traditional malware attacks

Astaroth is a fileless malware

- When users downloaded the file, a Windows Management Instrumentation (WMI) tool was launched, along with a number of other legitimate Windows tools
- These tools downloaded additional code that was executed only in memory, leaving no evidence that could be detected by vulnerability scanners
- Then the attacker downloaded and ran a Trojan that stole credentials and uploaded them to a remote server

Malware proliferation is directly related to profit hackers can make without being caught

Money making schemes include:

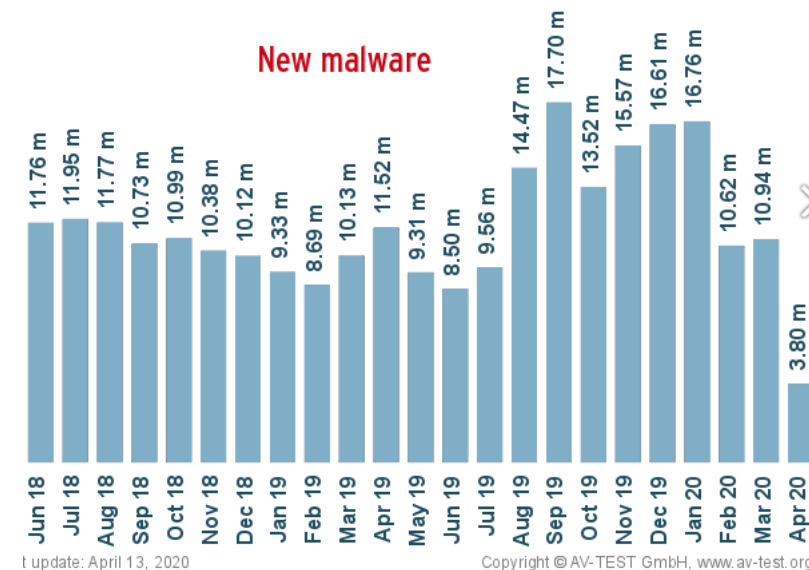
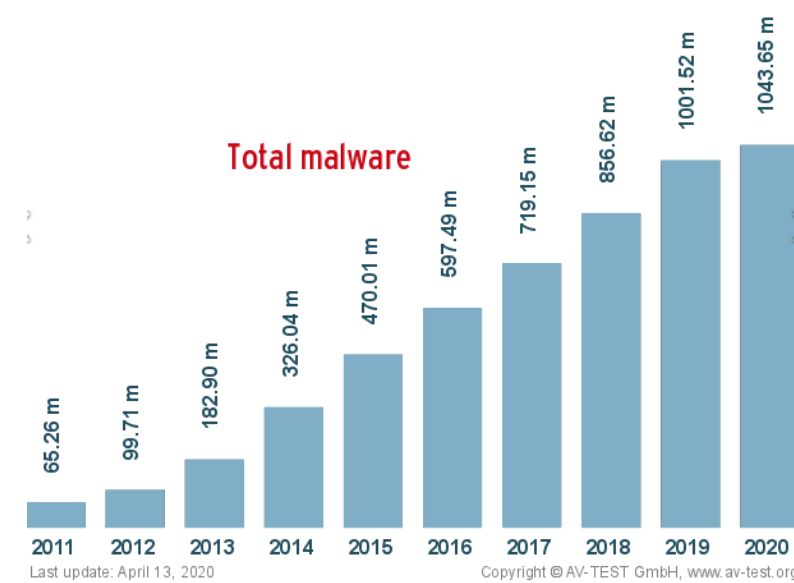
- Compromising systems with botnets for later use in:
 - Distributed denial of service (DDoS) attacks
 - Spam distribution
- Ransomware encrypting users' files with keys that are only given after users pay a ransom
- Spyware collects personal data for resale
- Redirecting web traffic pointing people to a specific product for purchase
- Installing key loggers, which collect financial information for reuse
- Carrying out phishing attacks, fraudulent activities, identity theft, and information warfare

Malware is increasing

AVTest reports over 350,000 new malware and potentially unwanted applications identified each day

Main reasons types malware is increasing in quantity and potency:

- Homogenous computer environments (Windows, MacOS, Android, iOS) – 1 piece of malware will work on many/most devices
- Everything is becoming a computer capable of being compromised (phones, TVs, game consoles, power grids, medical devices,...)
- More people and companies store all their data in digital format
- Many accounts are configured with too much privilege (i.e. root/administrator access)
- More people who do not understand technology are using it for sensitive purposes (i.e. e-commerce, online banking, ...)



Malware Components

Malware typically has 6 common elements

1. Insertion – Installs itself on the victim's computer
2. Replication – Copies itself and spreads to other victims
3. Avoidance – Uses methods to avoid being detected
4. Trigger – An event initiates its payload execution
5. Payload - Carries out its function (i.e. exploits a vulnerability to provide access, deletes files, encrypts files, installs a backdoor, ...)
6. Eradication – Removes itself after its payload is executed

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Signature-based malware detection

Anti-malware software scans files, e-mail, other data and **compares** them **to a database of signatures** created by the anti-malware vendor

- A malware signature is a sequence of code extracted from the virus that is used to identify the virus
- Can only identify previously identified malware
- Updates to the signatures must be downloaded and applied frequently
- Cannot detect 0-day attacks

Signature-based malware detection avoidance

Polymorphic virus has the capability to change its own code to produce thousands of varied operational versions of itself

- Can use different encryption techniques
- Can vary the sequence of their instructions
 - Combining noise or bogus instructions with the useful instructions
 - Using a mutation engine and a random-number generator to change the sequence of their instructions

Multi-part virus distributes its components to different parts of the system

Integrity-based malware detection

- Calculates and stores a hash for each component of the system: operating system files, application files, configuration files, ...
- Each new scan of the system calculates a hash for each component and compares it with the stored hash to detect differences
- Detected differences send alerts and are flagged as suspect for further analysis



Heuristic-based malware detection

Analyzes the overall structure of the malicious code, evaluating

- Coded logic, instructions, functions and modules
- Data types and structures

Assesses likelihood that the code is malicious by accumulating a scored rating of “suspiciousness”

- Increases as it finds more potentially malicious attributes
- Compared to a threshold, which when crossed the detector identifies the software as malware and the protections are activated

2 types of heuristic malware detection methods

1. Static analysis – Reviewing code without running it
2. Dynamic analysis – Reviewing code as it is running

Behavior-based malware detection

Allows suspicious code to execute within the unprotected operating system, and watches its interaction with the operating system components looking for suspicious activities:

- Writing to Run keys in the Windows Registry or startup files
- Opening, deleting, or modifying files
- Modifying executable logic
- Creating or modifying macros and scripts
- Scripting e-mail messages to send executable code
- Connecting to network shares or resources
- Formatting a hard drive or writing to the boot sector

Anti-malware software components

Detection techniques

- Signature-based
- Integrity-based
- Heuristic-based
- Behavior-based

Proactive techniques able to detect new malware (i.e. 0-day attacks)

Protection techniques

- Quarantine the file
- Clean the file
- Roll-back to prior version of the file
- Warn the user
- Log the event

Best practices against malware attacks

User Education

Training users on best practices can go a long way in protecting an organization

- How to avoid malware
 - Don't download and run unknown software
 - Don't blindly insert "found media" into your computer
- How to identify potential malware
 - Phishing emails
 - Unexpected applications/processes running on a system

<https://www.rapid7.com/fundamentals/malware-attacks/>

Best practices against malware attacks

Use Reputable Anti-Virus (A/V) Software

- When installed, a suitable A/V solution will detect (and remove) any existing malware on a system, as well as monitor for and mitigate potential malware installation or activity while the system is running. It'll be important to keep it up-to-date with the vendor's latest definitions/signatures.

Ensure Your Network is Secure

- Control access to systems on the organization's network
- Use of proven technology and methodologies—such as using a firewall, IPS, IDS
- Remote access only through VPN—will help minimize the attack “surface” your organization exposes

Regular Website Security Audits

- Scan the organization's websites regularly for vulnerabilities
 - Software with known bugs and server/service/application misconfiguration
 - Detect if known malware has been installed

Create Regular, Verified Backups

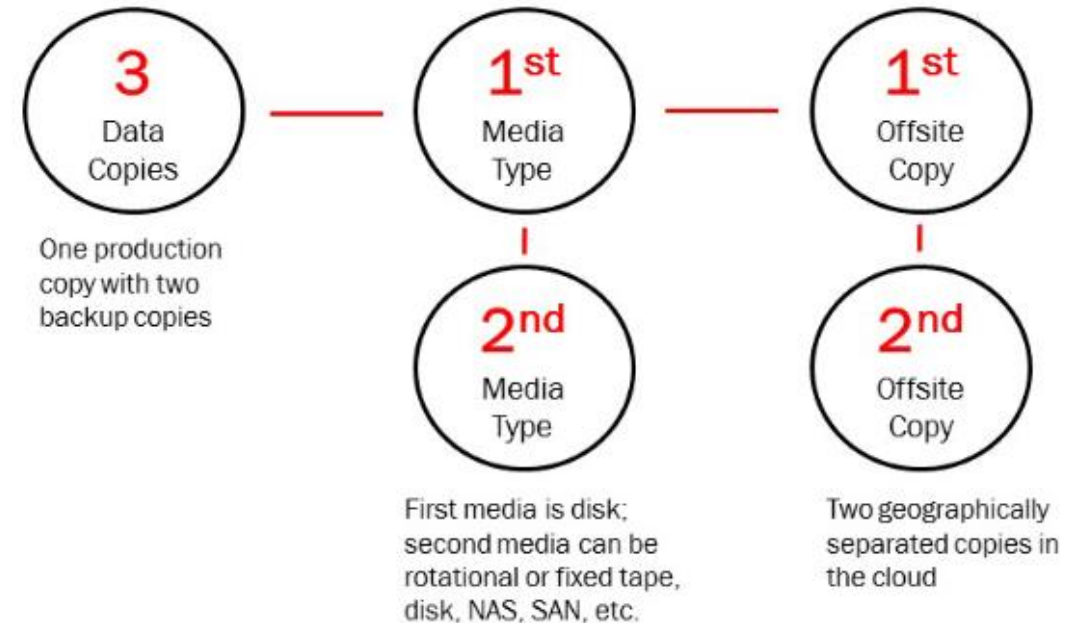
- Have regular (i.e. current and automated) offline backup
- Make sure they are verified to be happening on the expected regular basis and are usable for restore operations
 - Old, outdated backups are less valuable than recent ones
 - Backups that don't restore properly are of no value

Mitigation – Backup Best Practice

Three-Two-One rule

- Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

Maersk had 50 copies of their mission critical software and corresponding data – all in the same format, all on the network



Agenda

- ✓ Computer virus
- ✓ Malicious software
- ✓ Proliferation of malware
- ✓ Malware components
- ✓ Anti-malware components
- ✓ Best practices for protection
- Milestone 4 instructions

Milestone 4 instructions

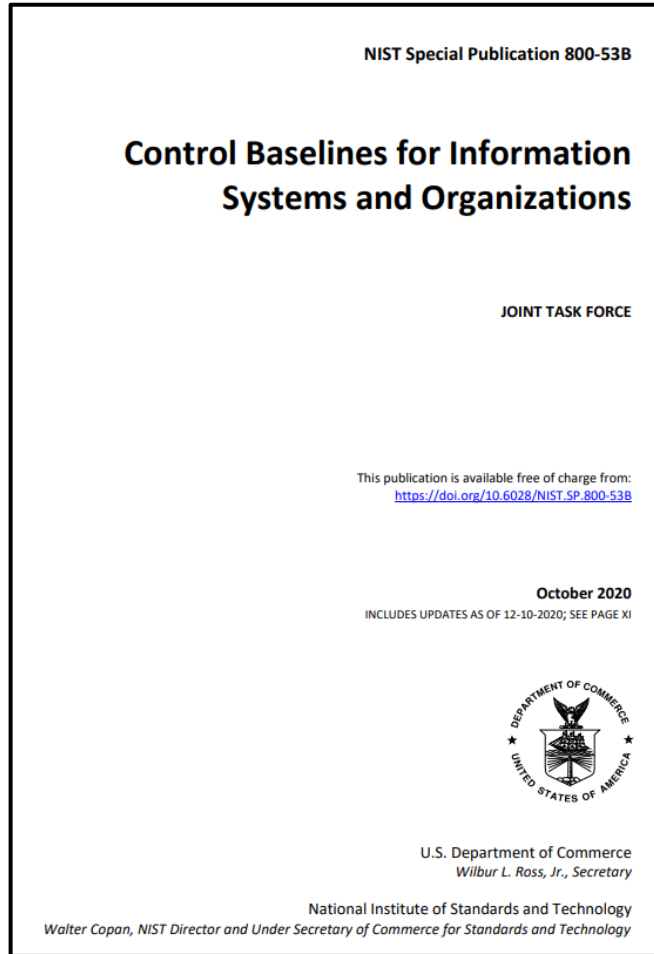
Your assignment is to transform your Milestone 3 penetration test and vulnerability identification report into a vulnerability identification and security mitigation and control report

As before, your report is for senior managers of the company who owns and depends on financial management information stored on and processed within the server you examined in your penetration test

Be sure your report:

1. Clearly identifies the level of concern the managers should have for confidentiality, integrity, and availability of the financial information on the server and the potential impact on the business' assets, operations, and people should the information and information system be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction
2. Identifies the vulnerabilities you found during your penetration test
3. Recommends information security controls for mitigating each of the vulnerabilities you found

Finding Controls to Mitigate Vulnerabilities



https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

password

1/3

3.7 IDENTIFICATION AND AUTHENTICATION FAMILY

Table 3-7 provides a summary of the controls and control enhancements assigned to the Identification and Authentication Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-1	Policy and Procedures		x	x	x
IA-2	Identification and Authentication (Organizational Users)		x	x	x
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS		x	x	x
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS		x	x	x
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1)(2).			
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION				x
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE				
IA-2(7)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(8)	ACCESS TO ACCOUNTS — REPLAY RESISTANT		x	x	x
IA-2(9)	NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT	W: Incorporated into IA-2(8).			
IA-2(10)	SINGLE SIGN-ON				
IA-2(11)	REMOTE ACCESS — SEPARATE DEVICE	W: Incorporated into IA-2(6).			
IA-2(12)	ACCEPTANCE OF PIV CREDENTIALS		x	x	x
IA-2(13)	OUT-OF-BAND AUTHENTICATION				
IA-3	Device Identification and Authentication			x	x
IA-3(1)	CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION				
IA-3(2)	CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION	W: Incorporated into IA-3(1).			
IA-3(3)	DYNAMIC ADDRESS ALLOCATION				
IA-3(4)	DEVICE ATTESTATION				
IA-4	Identifier Management		x	x	x
IA-4(1)	PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS				
IA-4(2)	SUPERVISOR AUTHORIZATION	W: Incorporated into IA-12(1).			
IA-4(3)	MULTIPLE FORMS OF CERTIFICATION	W: Incorporated into IA-12(2).			
IA-4(4)	IDENTIFY USER STATUS			x	x
IA-4(5)	DYNAMIC MANAGEMENT				
IA-4(6)	CROSS-ORGANIZATION MANAGEMENT				
IA-4(7)	IN-PERSON REGISTRATION	W: Incorporated into IA-12(4).			
IA-4(8)	PAIRWISE PSEUDONYMOUS IDENTIFIERS				
IA-4(9)	ATTRIBUTE MAINTENANCE AND PROTECTION				
IA-5	Authenticator Management		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x

This publication is available free of charge from: <https://doi.org/10.6028/NIST.SP.800-53B>

IA-5	Authenticator Management		x	x	x
IA-5(1)	PASSWORD-BASED AUTHENTICATION		x	x	x

Example of Control to Mitigate a Vulnerability...

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage system authenticators by:

- a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
- b. Establishing initial authenticator content for any authenticators issued by the organization;
- c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
- e. Changing default authenticators prior to first use;
- f. Changing or refreshing authenticators [*Assignment: organization-defined time period by authenticator type*] or when [*Assignment: organization-defined events*] occur;
- g. Protecting authenticator content from unauthorized disclosure and modification;
- h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and
- i. Changing authenticators for group or role accounts when membership to those accounts changes.

Discussion: Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements for authenticator content contain specific criteria or characteristics (e.g., minimum password length). Developers may deliver system components with factory default authentication credentials (i.e., passwords) to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant risk. The requirement to protect individual authenticators may be implemented via control [PL-4](#) or [PS-6](#) for authenticators in the possession of individuals and by controls [AC-3](#), [AC-6](#), and [SC-28](#) for authenticators stored in organizational systems, including passwords stored in hashed or encrypted formats or files containing encrypted or hashed passwords accessible with administrator privileges.

Control Enhancements:

(1) AUTHENTICATOR MANAGEMENT | [PASSWORD-BASED AUTHENTICATION](#)

For password-based authentication:

- (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [*Assignment: organization-defined frequency*] and when organizational passwords are suspected to have been compromised directly or indirectly;
- (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
- (c) Transmit passwords only over cryptographically-protected channels;
- (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash;
- (e) Require immediate selection of a new password upon account recovery;
- (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;
- (g) Employ automated tools to assist the user in selecting strong password authenticators; and
- (h) Enforce the following composition and complexity rules: [*Assignment: organization-defined composition and complexity rules*].

Discussion: Password-based authentication applies to passwords regardless of whether they are used in single-factor or multi-factor authentication. Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten. Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Related Controls: [IA-6](#).

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

September 2020

INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

Read and understand what this control is about, identify the basic information you need for your report

Search NIST SP 800-53 for additional controls

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

f 492



Page view

Multi-factor

24/25

NIST SP 800-53, REV. 5

SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

TABLE C-7: IDENTIFICATION AND AUTHENTICATION FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	IMPLEMENTED BY	ASSURANCE
IA-1	Policy and Procedures	o	√
IA-2	Identification and Authentication (Organizational Users)	o/s	
IA-2(1)	MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS	s	
IA-2(2)	MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS	s	
IA-2(3)	LOCAL ACCESS TO PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(1).	
IA-2(4)	LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS	W: Incorporated into IA-2(2).	
IA-2(5)	INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION	o/s	
IA-2(6)	ACCESS TO ACCOUNTS — SEPARATE DEVICE	s	

This pu

Research controls, study the details, then identify the control and summarize briefly in your report

[IA-2](#) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Discussion: Organizations can satisfy the identification and authentication requirements by complying with the requirements in [\[HSPD 12\]](#). Organizational users include employees or individuals who organizations consider to have an equivalent status to employees (e.g., contractors and guest researchers). Unique identification and authentication of users applies to all accesses other than those that are explicitly identified in [AC-14](#) and that occur through the authorized use of group authenticators without individual authentication. Since processes execute on behalf of groups and roles, organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity.

Organizations employ passwords, physical authenticators, or biometrics to authenticate user identities or, in the case of **multi-factor** authentication, some combination thereof. Access to organizational systems is defined as either local access or network access. Local access is any access to organizational systems by users or processes acting on behalf of users, where access is obtained through direct connections without the use of networks. Network access is access to organizational systems by users (or processes acting on behalf of users) where access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. Internal networks include local area networks and wide area networks.

The use of encrypted virtual private networks for network connections between organization-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks with respect to protecting the confidentiality and integrity of information traversing the network. Identification and authentication requirements for non-organizational users are described in [IA-8](#).

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | [MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS](#)

Implement **multi-factor authentication for access to privileged accounts.**

Discussion: **Multi-factor** authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). **Multi-factor** authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using **multi-factor** options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

(2) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | [MULTI-FACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS](#)

Implement **multi-factor authentication for access to non-privileged accounts.**

Discussion: **Multi-factor** authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). **Multi-factor** authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card. In addition to authenticating users at the system level, organizations may also employ authentication mechanisms at the application level, at their discretion, to provide increased information security. Regardless of the type of access (i.e., local, network, remote), non-privileged accounts are authenticated using **multi-factor** options appropriate for the level of risk. Organizations can provide additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.


What other types of controls can you think of to research and include in your report to mitigate the vulnerabilities you found...

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
<u>AC</u>	Access Control	<u>PE</u>	Physical and Environmental Protection
<u>AT</u>	Awareness and Training	<u>PL</u>	Planning
<u>AU</u>	Audit and Accountability	<u>PM</u>	Program Management
<u>CA</u>	Assessment, Authorization, and Monitoring	<u>PS</u>	Personnel Security
<u>CM</u>	Configuration Management	<u>PT</u>	PII Processing and Transparency
<u>CP</u>	Contingency Planning	<u>RA</u>	Risk Assessment
<u>IA</u>	Identification and Authentication	<u>SA</u>	System and Services Acquisition
<u>IR</u>	Incident Response	<u>SC</u>	System and Communications Protection
<u>MA</u>	Maintenance	<u>SI</u>	System and Information Integrity
<u>MP</u>	Media Protection	<u>SR</u>	Supply Chain Risk Management

Research controls, study the details, then identify the control and summarize briefly in your report

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES



ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Control:

- a. Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and
- b. Define system access authorizations to support separation of duties.

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties. Separation of duties is enforced through the account management activities in [AC-2](#), access control mechanisms in [AC-3](#), and identity management activities in [IA-2](#), [IA-4](#), and [IA-12](#).

Related Controls: [AC-2](#), [AC-3](#), [AC-6](#), [AU-9](#), [CM-5](#), [CM-11](#), [CP-9](#), [IA-2](#), [IA-4](#), [IA-5](#), [IA-12](#), [MA-3](#), [MA-5](#), [PS-2](#), [SA-8](#), [SA-17](#).

Control Enhancements: None.

References: None.

-6 LEAST PRIVILEGE

Control: Employ the principle of **least privilege**, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Discussion: Organizations employ **least privilege** for specific duties and systems. The principle of **least privilege** is also applied to system processes, ensuring that the processes have access to systems and operate at privilege levels no higher than necessary to accomplish organizational missions or business functions. Organizations consider the creation of additional processes, roles, and accounts as necessary to achieve **least privilege**. Organizations apply **least privilege** to the development, implementation, and operation of organizational systems.

Related Controls: [AC-2](#), [AC-3](#), [AC-5](#), [AC-16](#), [CM-5](#), [CM-11](#), [PL-2](#), [PM-12](#), [SA-8](#), [SA-15](#), [SA-17](#), [SC-38](#).

Control Enhancements:

(1) LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS

Authorize access for [Assignment: organization-defined individuals or roles] to:

- (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and
- (b) [Assignment: organization-defined security-relevant information].

Next time

Malware-Ransomware Case Study:

“CYBERATTACK: The Maersk Global Supply-Chain Meltdown”

Agenda

- ✓ Computer Virus
- ✓ Malicious software
- ✓ Proliferation of malware
- ✓ Malware components
- ✓ Anti-malware components
- ✓ Best practices for protection
- ✓ Milestone 4 instructions
- ✓ Next time...