System and Network Administration

ASIA PACIFIC UNIVERSITY OF TECHNOLOGY & INNOVATION

Security Policies

& Host Security

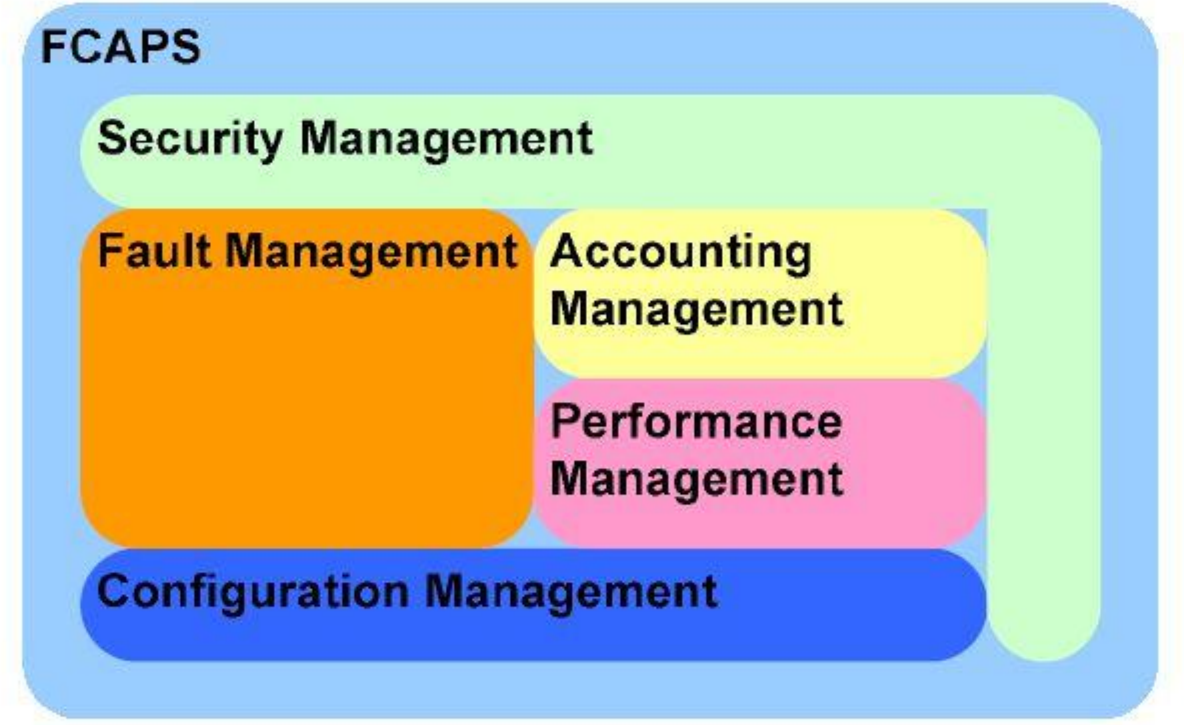
Secure Systems

1. Security policy
   - **What needs to be protected**
   - **Kinds / level of protection**
   - **Responsibilities**
   - **Auditing policy**
2. Security environment
   - **Physical environment**
   - **Physical security**
   - **Hardware, operating system**
   - **firewalls, etc**
3. Security mechanisms
   - **cryptography**
   - **authentication**
   - **security protocols**
4. Monitoring and auditing procedures
   - **monitor access**
   - **audit trails**
   - **feedback on failures, security breaches**
   - **containment & recovery**

A Philosophy

- System Administration is about
  - Putting together a network of computers
  - Getting them to run some applications
  - Keeping them running in a dynamic world
- System Administration is as much about technology as it is about user behaviour
- System Administration requires constant monitoring and rapid response to problems

The OSI Network Management Model

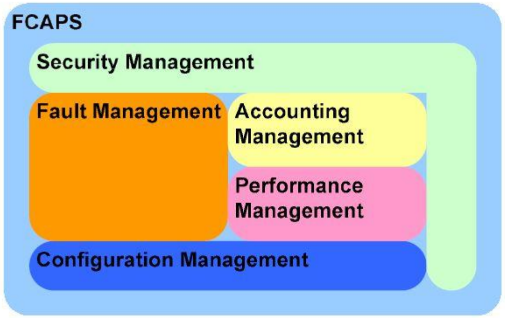


Aimed at standardizing management systems – not necessarily at standardizing manager behavior

Network Configuration Management
10 Sep 2007 - https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.html

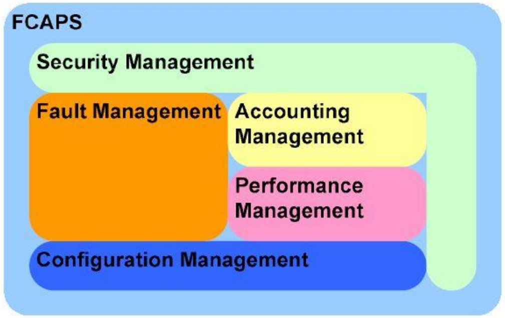
FCAPS: Fault Management

- Detect faults, or abnormal operation of network
- Isolate (the cause of the) fault, and
- Correct the problem, in order to return to a normal/functional state



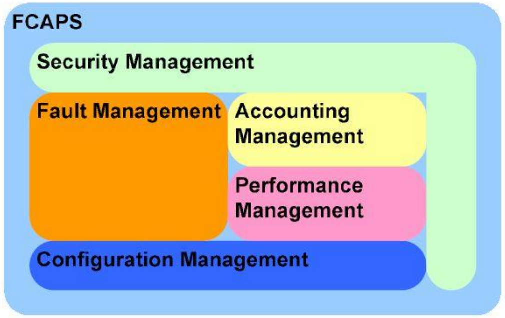
FCAPS: Configuration Management

- Network structure
  - design or functional requirements, geography or building requirements, network engineering constraints
- Network architecture
  - Network segmentation, addressing
  - Name resolution, Directories
  - Start-up of services and software
- Network policy
  - User rights and responsibilities
  - Application limits and responsibilities
  - Security and privacy



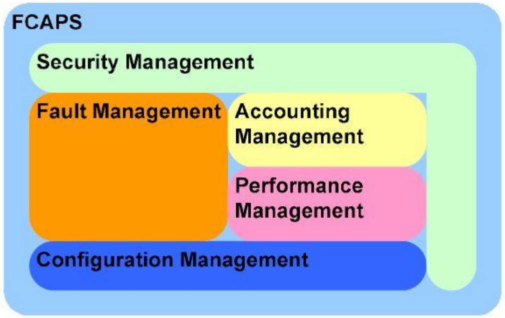
FCAPS: Accounting Management

- Establish how to charge users for the utilization of managed objects or resources on the network,
- Establish auditing of utilization for purposes of intrusion detection.



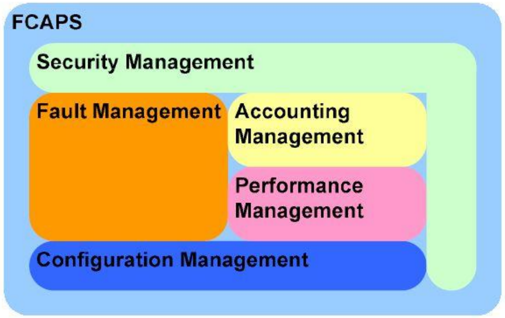
FCAPS: Performance Management

- Monitor and evaluate the behaviour of managed objects
- Evaluate the effectiveness of communication activities
- Evaluate if performance targets are being met, e.g., speed, efficiency, maximizing bandwidth or channel capacity, minimization of data loss during communications, avoidance or resolution of traffic congestion, throughput.



FCAPS: Security Management

- Implement security policies
  - Protect managed objects from misuse, sabotage, unauthorized access
- Ensuring data integrity
- Analysing security state of network
- Administering firewalls, web security, VPN (virtual private networks)
- Intrusion detection



Q
&
A

Policy Based Network Management

- from policy to implementation, e.g., for configuration management
- Policy = A clear expression of goals and responses
  - Prepares for possible errors or problems
  - Documents Intent and Procedure
- Necessary in medium to large organisations or where many administrators co-operate
- Helps to align system operation with organisational objectives

Security Management

- The ***security policy*** defines what information is to be protected and from whom
- **Security policy applies to resources** under control of the enterprise
- ***Security mechanisms*** implement aspects of the **security policy**, and their **effectiveness** must be monitored

Security Policy

- Strict control over access to system configuration files
- Control privileges
  - Users should only have access to the services that they have been specifically authorised to use and any access by remote users or connections to remote computer systems must be authenticated.
- Encrypted communication channels
  - Close telnet and ftp ports – use ssh
- Monitor system use and performance
- Track reports of attacks and vulnerabilities
- Test and evaluate failure modes
  - Avoid single point of failure

Security Management

- **Security policy applies to resources** under control of the enterprise; ***acceptable use policy* applies to people and interfaces.**
- ***Security procedures*** implement aspects of the **acceptable use policy**, and **compliance** must be monitored

Acceptable Use Policy

Should include at least:

- An **access policy** - defines access rights and privileges
- An **accountability policy** - defines the responsibilities of users, operating staff, and management
- An **authentication policy** - establishes trust via something the user knows, has, or is
- A **privacy policy** - defines reasonable expectation of monitoring of email, access to user files, etc
- A **technology policy** - guidelines for purchasing, configuring, and auditing computer systems

Acceptable Use Policy

Acceptable use policy should specify

- Applications that are run on networks PCs and restrict the downloading of unknown application from internet or other sites.
- Users connect only permitted computers or other devices to the LAN interfaces in their offices.
  - “BYOD” (Bring Your Own Device) needs to be dealt with
  - e.g.,** wireless@apu v, Staff@apu
- Encourage users to log out their session when not in use.

Security Policy needs to include steps to minimise social issues

- user education
- clearly stated policy on disclosing information over the phone

Security Policy

The implications are:

- implementing the acceptable use policy is essentially a management issue;
- implementing the security policy is more of a technical issue;
- security policy implementation mechanisms must provide information necessary for enforcement of the acceptable use policy.
- Monitoring effectiveness of mechanisms and compliance with policies (accountability) requires keeping track of activity (audit trails)

RedHat 9 Security Guide

- p.46 securing portmap
- p.49 securing nfs
- p.50 securing web
- p.54 sendmail (a postfix alternative)
- p.55 nmap
- p.65, 75-77, 97- firewalls

Q
&
A

Network Policy

- Segmentation
  - Subnet addressing
  - Logical to physical address mapping (VLANs?)
  - Port Blocking? Different on each subnet?
  - Blocking at Firewall or Router?
- Address configuration
  - Static /etc/hosts, DHCP
- Name Resolution
  - DNS, WINS
- Directory Services

Applications Policy

- SMTP
  - Name aliases (eg Chris.Freeman@monash.edu.au)
  - File size and type limitations for attachments
  - SPAM filtering
  - Virus checking
- HTTP
  - Content & Style guides, plagiarism, authorisation?
  - CGI / Modules allowed?
    (eg Apache mod_perl, mod_ssl)
  - Load Limiting

Resource Sharing Policy

- File Systems
  - Common/Shared directories? Read-only?
- Backups
  - Global or Local?
  - Image or File?
  - Archival or Incremental?
- Printing
  - Personal printing? Page count quotas?
  - Colour vs Monochrome

User Account Policy

- formal user registration and deregistration procedure for granting access
- allocation of passwords controlled through a formal management process.
- a formal process conducted at regular intervals to review users' access rights.
- policies and procedures governing use of mobile computing and teleworking facilities.

Password Issues

- No passwords
- Easily guessed
- Password aging
- Login shells
- Access to encrypted passwords
- Group logins – Shared accounts
- Root privileges

Non-Technical aspects of Security

- Otherwise impenetrable systems can still be compromised using “Social Engineering”.
- An unwary user may be tricked into revealing the keys to sensitive information ***(“Phishing”)***
  - Phone call from bogus SysAdmin who needs info to repair or install
  - Bogus Market survey with questions that reveal enough info to be able to guess passwords or key information
  - Discarded documents with account numbers or other pertinent data

Non-Technical aspects of Security

- Bragging
  - Misguided users bragging about how good their system is, are actually giving information away.
  - Egotistical crackers may over emphasize their success to provoke a situation where more information is revealed.

- Security Policy needs to include steps to minimise these social issues
  - user education
  - clearly stated policy on disclosing information over the phone
  - Check Lists

Password Security

- Passwords
  - Consistent use of Strong Passwords
  - UP, low, Num, # - _ + ~
  - Prevent brute force and dictionary attacks
- Force users to change their password
  - Set an expiration date
  - Be sure to send plenty of warnings
  - **Expect complaints!**
- Combat Password Sniffing
  - telnet, ftp etc use plaintext passwords that are visible to protocol analysers
  - Use SSH/SSL

Try out **`pwgen`**

What are the likely consequences? (simple, written down)

Q
&
A

RedHat 9 Security Guide

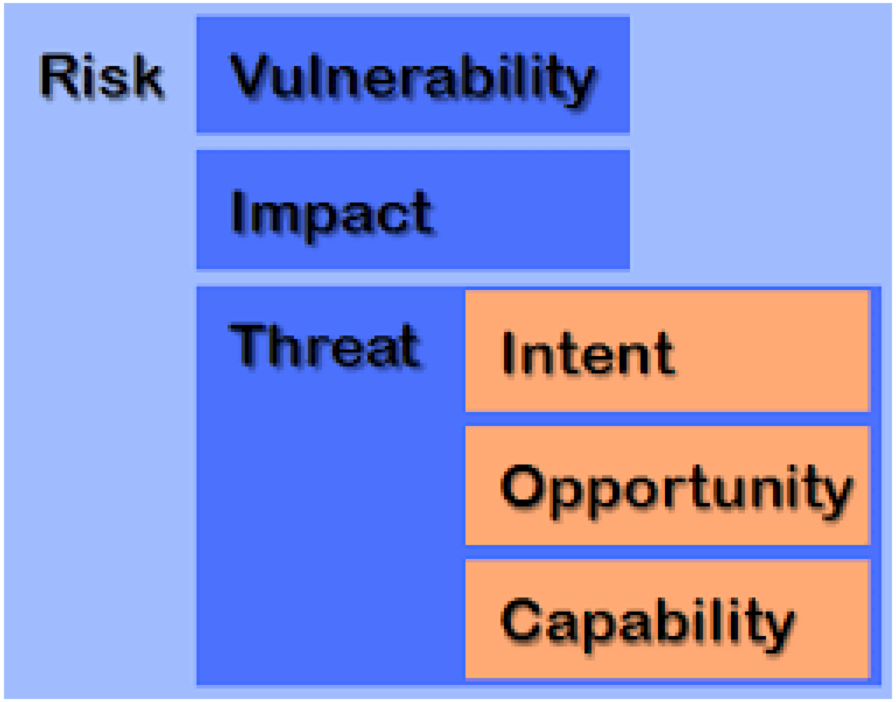
- 8. Vulnerability Assessment
- 8.1. Thinking Like the Enemy
- 8.2. Defining Assessment and Testing
- 8.3. Evaluating the Tools

- 10. Incident Response
- 10.1. Defining Incident Response
- 10.2. Creating an Incident Response Plan
- 10.3. Implementing the Incident Response Plan
- 10.4. Investigating the Incident
- 10.5. Restoring and Recovering Resources
- 10.6. Reporting the Incident

- Appendix A. Common Exploits and Attacks

Intruder prevention

- White hat hackers (penetration testing)
  - Scanning
  - Vulnerability analysis
  - System update/patch



Risk

Vulnerability

Impact

Threat

Intent

Opportunity

Capability

Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions

- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
  - Choose mitigation strategies
  - Build solutions based on the strategies

Intrusion Lifecycle

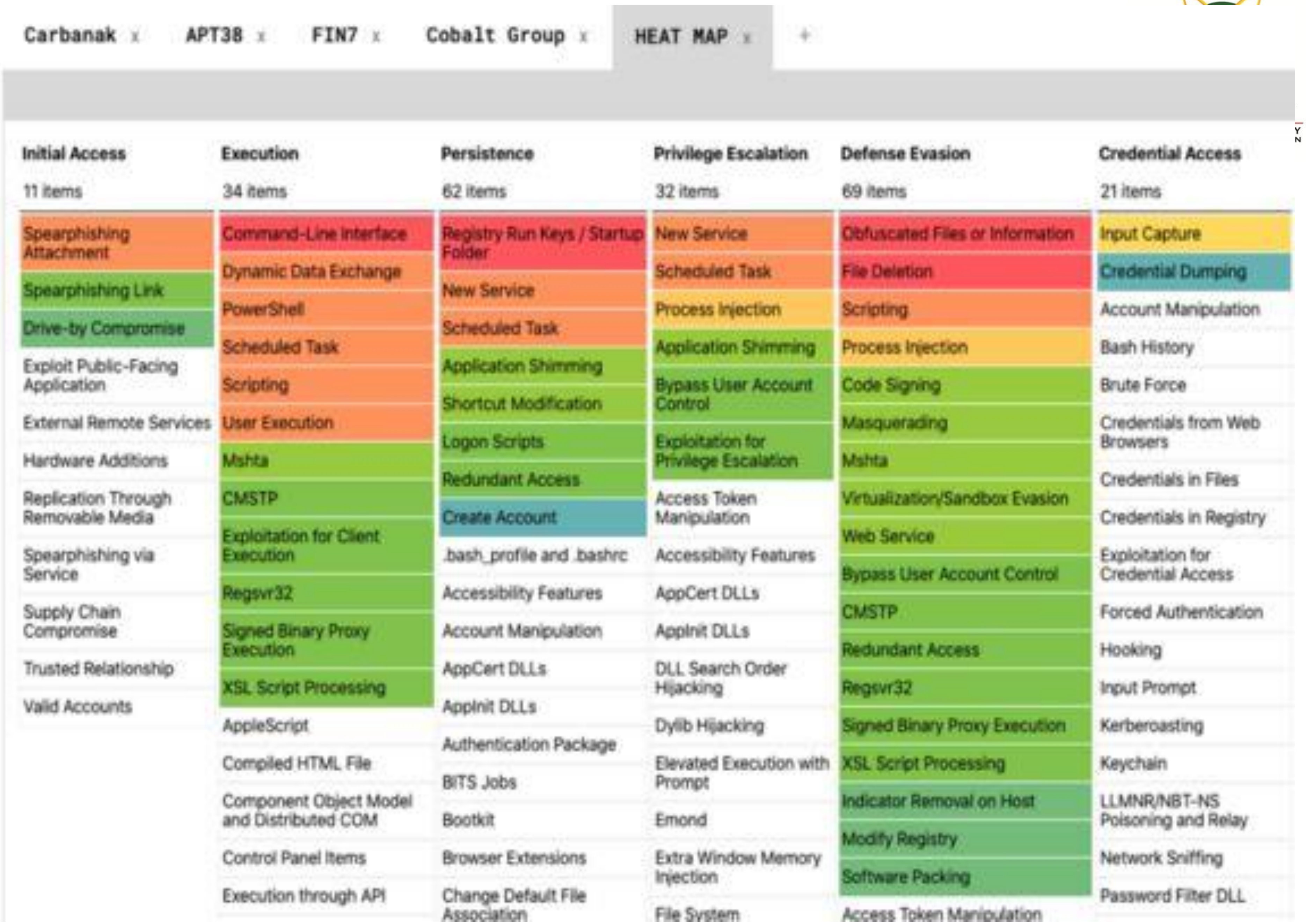
Phase	Technique	Description
1	**Reconnaissance**	- Gather as much info about targets as possible. - Required to craft an attack.
2	**Initial exploitation**	- Gain access to network or hosts, obtain credentials, etc.
3	**Privilege escalation**	- Gain greater control over systems. - Can do more damage with higher privileges.
4	**Pivoting**	- Compromise a central host. - Spread to other hosts and network segments.
5	**Persistence**	- Maintaining access is an important goal. - Avoiding discovery, erasing traces of activity

https://attack.mitre.org/#

- The MITRE Corporation, a not-for-profit org, released the ATT&CK Framework in 2015, for the private sector, governments, the cybersecurity product and service community, and the general public.
- ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. The framework is a matrix of intrusion techniques.
- The ATT&CK Framework is essentially the attacker's playbook — how they get in your system, how they move, what they do, what their end goals are, and how it impacts your system. ATT&CK maps and indexes virtually everything regarding an intrusion from both the attack and defense sides.

MITRE ATT&CK Framework

- The ATT&CK Matrix is composed of tactics, techniques, and procedures, otherwise known as TTP. Following the columns, or tactics, from left to right, shows steps an attacker would typically follow when attacking your organization.
- Multiple techniques can be employed to accomplish the same tactic, and depending on the attacker's main objective, not all 12 tactics need to be employed.
- The aggregate of techniques used during an attack is known as the behavior profile — the procedure the attacker followed to accomplish their ultimate goal by attacking your system.
- Each of the 220+ techniques on the ATT&CK matrix has a page that includes a brief summary of the adversarial technique, procedure examples, mitigations for detecting and defending against each of these attacks.



Initial Access

11 items

- Spearphishing Attachment
- Spearphishing Link
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Replication Through Removable Media
- Spearphishing via Service
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

34 items

- Command-Line Interface
- Dynamic Data Exchange
- PowerShell
- Scheduled Task
- Scripting
- User Execution
- Mshta
- CMSTP
- Exploitation for Client Execution
- Regsvr32
- Signed Binary Proxy Execution
- XSL Script Processing
- AppleScript
- Compiled HTML File
- Component Object Model and Distributed COM
- Control Panel Items
- Execution through API

Persistence

62 items

- Registry Run Keys / Startup Folder
- New Service
- Scheduled Task
- Application Shimming
- Shortcut Modification
- Logon Scripts
- Redundant Access
- Create Account
- .bash_profile and .bashrc
- Accessibility Features
- Account Manipulation
- AppCert DLLs
- AppInit DLLs
- Authentication Package
- BITS Jobs
- Bootkit
- Browser Extensions
- Change Default File Association

Privilege Escalation

32 items

- New Service
- Scheduled Task
- Process Injection
- Application Shimming
- Bypass User Account Control
- Exploitation for Privilege Escalation
- Access Token Manipulation
- Accessibility Features
- AppCert DLLs
- AppInit DLLs
- DLL Search Order Hijacking
- Dylib Hijacking
- Elevated Execution with Prompt
- Emond
- Extra Window Memory Injection
- File System

Defense Evasion

69 items

- Obfuscated Files or Information
- File Deletion
- Scripting
- Process Injection
- Code Signing
- Masquerading
- Mshta
- Virtualization/Sandbox Evasion
- Web Service
- Bypass User Account Control
- CMSTP
- Redundant Access
- Regsvr32
- Signed Binary Proxy Execution
- XSL Script Processing
- Indicator Removal on Host
- Modify Registry
- Software Packing
- Access Token Manipulation

Credential Access

21 items

- Input Capture
- Credential Dumping
- Account Manipulation
- Bash History
- Brute Force
- Credentials from Web Browsers
- Credentials in Files
- Credentials in Registry
- Exploitation for Credential Access
- Forced Authentication
- Hooking
- Input Prompt
- Kerberoasting
- Keychain
- LLMNR/NBT-NS Poisoning and Relay
- Network Sniffing
- Password Filter DLL

https://attack.mitre.org/matrices/enterprise/#

- Initial Access — techniques that use various entry vectors to gain an initial foothold within a network (e.g., T1192 Spearphishing Link)
- Execution — techniques that result in running attacker-controlled code on a local or remote system (e.g., T1086 PowerShell)
- Persistence — techniques used to maintain persistent access to a system (e.g., T1037 Logon Scripts)
- Privilege Escalation — techniques used to gain higher-level privileges on a system or network (e.g., T1055 Process Injection)
- Defense Evasion — techniques used to avoid detection (e.g., T1073 DLL Side-Loading)
- Credential Access — techniques for stealing credentials such as account names and passwords (e.g., T1208 Kerberoasting)

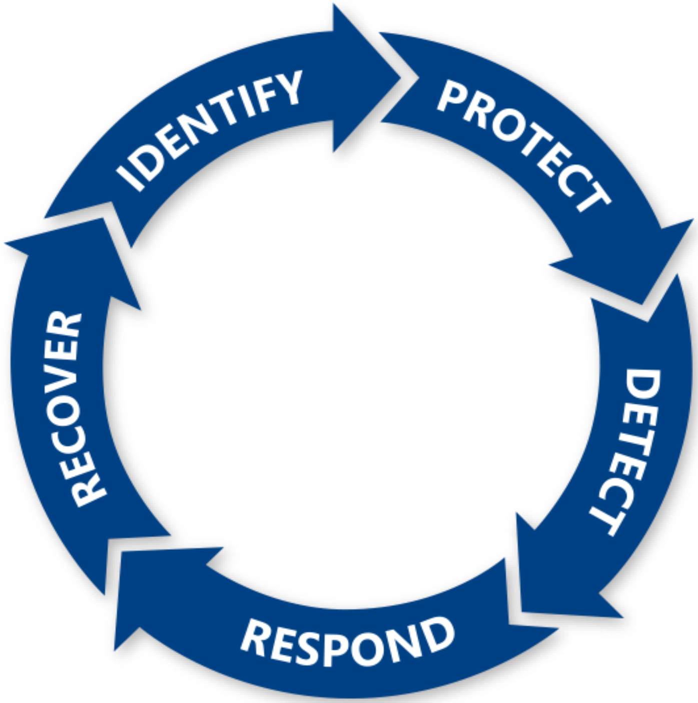
https://attack.mitre.org/matrices/enterprise/#

- Discovery — techniques used to gain knowledge about the system and internal network (e.g., T1040 Network Sniffing)
- Lateral Movement — techniques used to enter and control remote systems on a network from the already compromised host (e.g., T1097 Pass the Ticket) Attackers typically have to pivot through multiple machines (usually the weakest link in the chain of machines) to ultimately reach their end objective.
- Collection — techniques used to gather information relevant to following through on the attacker's objectives (e.g., T1056 Input Capture)
- Command & Control — techniques attackers may use to communicate with systems under their control, often disguised to look like normal HTTP traffic (e.g., T1172 Domain Fronting)
- Exfiltration — techniques used to steal data from your network (e.g., T1002 Data Compressed)

Q
&
A

NIST Cybersecurity Framework

1. Identify high-value assets
2. Protect against known and unknown threats
3. Detect attacks
4. Respond to suspicious activity
5. Recover from breach



A cycle of Continuous Improvement

Vulnerability Assessment

- A vulnerability assessment is an internal audit of your network and system security

- If you were to perform a vulnerability assessment of your home, you would check each door to see if they are shut and locked, and check every window, making sure that they shut completely and latch correctly.

- This same concept applies to systems, networks, and electronic data. Malicious users are the thieves and vandals of your data. Focus on their tools, mentality, and motivations, and you can then react swiftly to their actions.

Network Scanners and Analysis Tools

Network Tool	Description
Packet analyzer	• Monitors wireless or wired network communications. • Captures traffic data. • Can be used to gather information by examining packet contents.
Protocol analyzer	• Uses data captured by packet analyzer. • Identifies protocols and applications used by traffic. • Can reveal malicious traffic using specific vectors.
Network enumerator	• Identifies logical topology of a network to reveal connection pathways. • Provides high-level overview of network architecture.

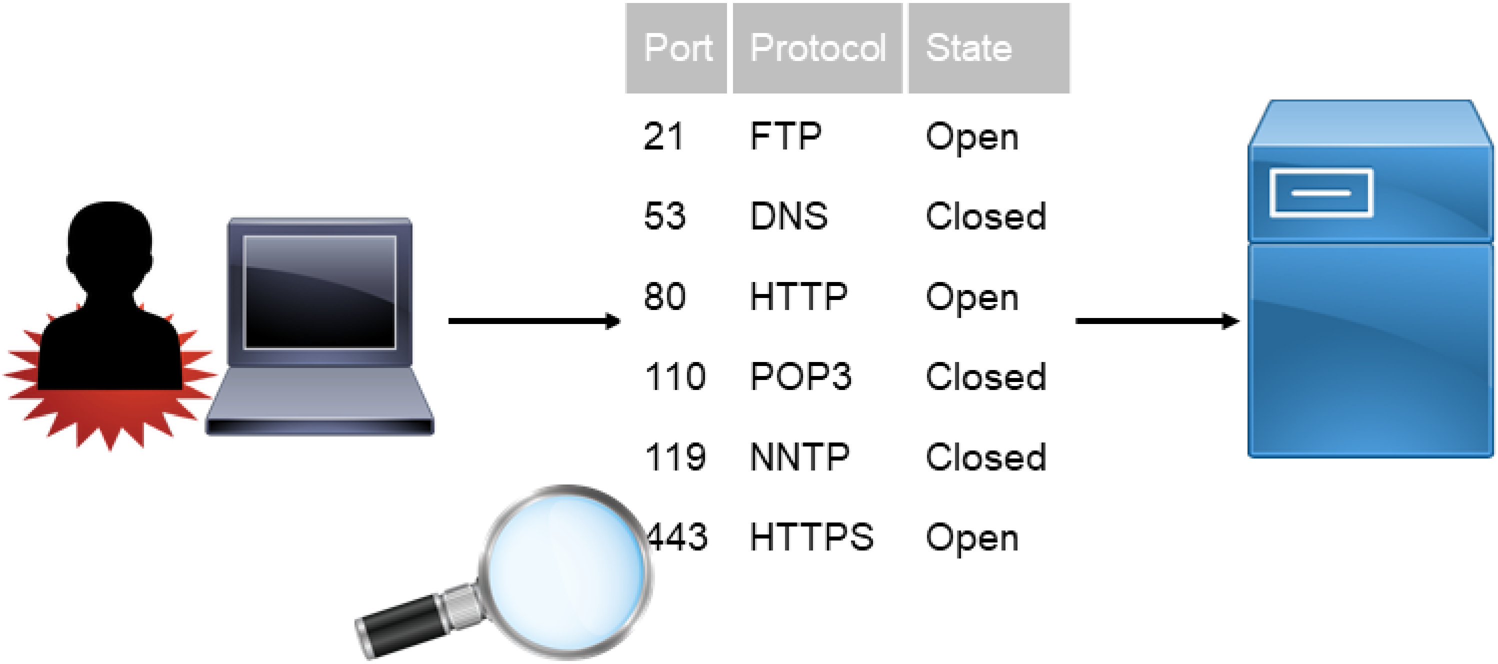
Port Scanning Attacks

Port: An endpoint of a logical connection that host computers use to connect to processes or services on other hosts.

Port scanning attack: A network-based attack where an attacker scans computers and other devices to see which ports are listening, in an attempt to find a way to gain unauthorized access.

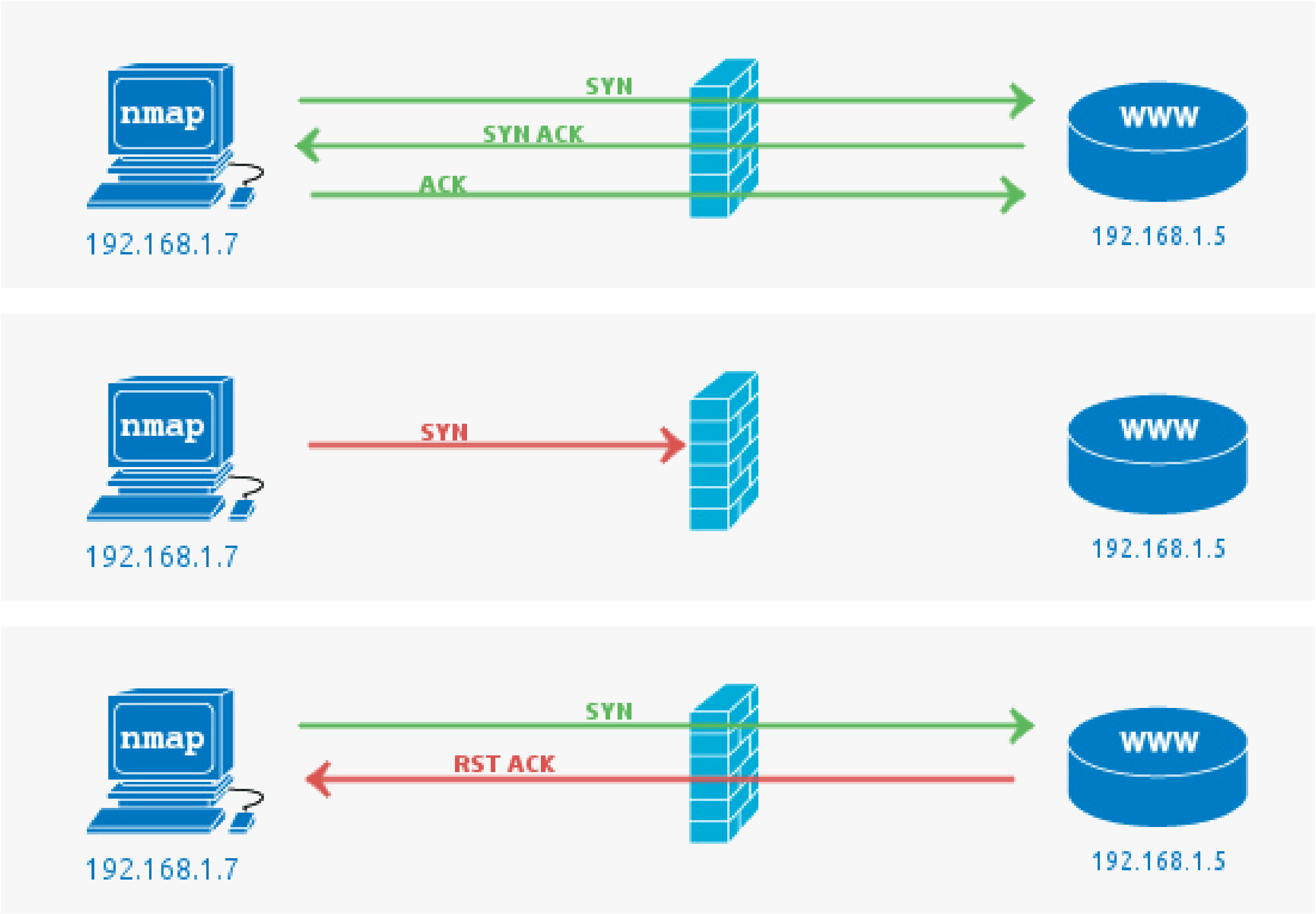
- TCP and UDP ports scanned.
- Active services scanned.
- Can be automated.
- Likely to occur, whether you're aware of it or not.

Port Scanning Attacks (Cont.)



Port	Protocol	State
21	FTP	Open
53	DNS	Closed
80	HTTP	Open
110	POP3	Closed
119	NNTP	Closed
443	HTTPS	Open

https://hackertarget.com/nmap-tutorial/



open

filtered

closed

nmap

- nmap ("Network Mapper") is a utility for network discovery and security auditing.
- It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Port scanning: hping

- The standard hping behaviors are encapsulated into a scanning algorithm.
  - for example to perform a SYN scan you just specify the -S option
  - you can change the TCP windows size, TTL, control the IP fragmentation as usual, and so on.
- Unlike most scanners, hping shows some interesting info about received packets, the IP ID, TCP win, TTL, and so on,
- Don't forget to look at this additional information when you perform a scan! Sometimes they reveal interesting details.

Q&A
dreamstime.com

Vulnerability Assessment Tools

Tool Type	Implement To
Vulnerability scanner	Assess systems, networks, and apps for weaknesses.
Port scanner	Assess current state of all ports on a network.
Protocol analyzer /packet sniffer	Assess traffic and what it reveals about contents and protocols being used.
Fingerprinting tools	Identify a target's OS information and running services.
Network enumerator	Map logical structure of network and identify rogue systems.
Password cracker	Recover secret passwords from stored or transmitted data.
Backup utilities	Create copies of scanned data.

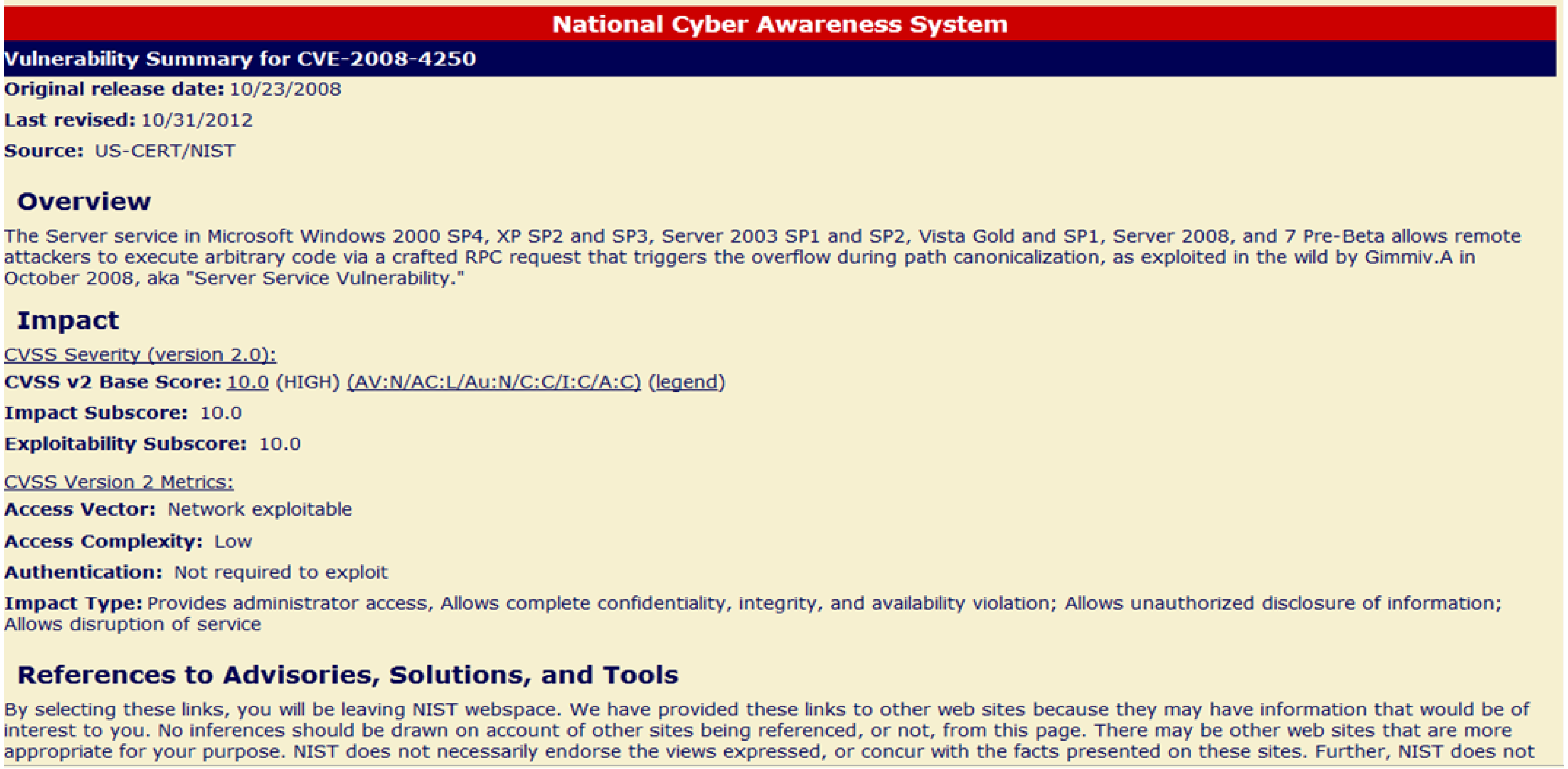
- Checklist
  - List of Hosts
  - List of type and versions of OS used
  - List of services provided
  - List of patches applied & non-standard software

- Test for weak passwords (*crack, satan, john the ripper*)*
- Ensure latest security patches are applied
- Evaluate trust relationships between hosts
- Monitor processes: watch for unusual or excessive process spawning
- Check file system for suspicious files
- Use a port scanner to find vulnerabilities*

Try it first – before someone tries it on you

Vulnerability Tracking

- [Common Vulnerability & Exposures (CVE)]
- Sample: CVE-2008-4250



National Cyber Awareness System

Vulnerability Summary for CVE-2008-4250

Original release date: 10/23/2008

Last revised: 10/31/2012

Source: US-CERT/NIST

Overview

The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka "Server Service Vulnerability."

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not

Q
&
A
dreamstime.com

Attack!

- Don’t panic
- Determine the appropriate level of response
- Gather tracking information
- Assess degree of exposure

- Pull the plug
- Devise recovery plan
- Communicate the recovery plan
- Implement the recovery plan
- Report the incident

Security Specialists

- Plan
- Lead
- Follow up

Vulnerability Assessment
Incident Response

System Administrators

- Participate
- Implement
- Execute

Incident Response

How will you respond to Incidents of **misuse** (malicious or abusive activity inside the network) or **intrusion** (breaches from the outside) ?

The incident response plan needs to cover four key activities:

1. Immediate action
2. Investigation
3. Restoration of resources
4. Reporting the incident to proper channels

Incident Response

- An incident response must be decisive and executed quickly.
  - Reacting quickly may minimize the impact of resource unavailability and the potential damage caused by system compromise.
- There is little room for error in most cases.
  - By staging practice emergencies and measuring response times, it is possible to develop a methodology that fosters speed and accuracy.
  - This is often referred to as “white-hat” or “ethical” hacking

Incident Response

- The incident response plan needs input from legal counsel, to alert technical and managerial staff to the legal ramifications of breaches
  - the hazards of leaking a client's personal, medical, or financial records for example, and the importance of restoring service in mission-critical environments such as hospitals and banks.

Can a person be fired if their weak password caused the disclosure of credit card numbers in our database of ecommerce customers?

Or should the system administrator who allowed the user to have a weak password be fired?

Q&A
dreamstime.com