Pen Test Report for DVWA in a Virtual Environment

Samiha Najah[1] and Mohammed Mujeebuddin[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

Business operations are now more digitalized and hence more exposed to technological risks such as hacking exploitation. Penetration testing helps organizations to estimate their security posture through the testing of network, computer systems, or Web applications to identify any existing vulnerabilities that a hacker can exploit. In this article, we aim to demonstrate a practical implementation of Penetration Testing in a virtual environment which was configured for learning purposes. The process involves the following phases: Reconnaissance, Scanning, Enumeration, Vulnerability Assessment, Gaining Access, and recommendation of the countermeasures. The results demonstrated several existing vulnerabilities such as Missing Encryption of Sensitive Data, Improper Certificate Validation and Windows Bluetooth driver elevation of privilege. At the end of the report, several countermeasures have been recommended in order to enhance the security posture of the studied environment.

Introduction

Cybersecurity has drastically emerged in recent years making it an important concern these days for organization and businesses as it helps in protecting sensitive information and systems from accessing, using, disclosing, interrupting, altering, or destructing by unauthorized parties. As the use of technology is increasing, the risk of cyber-attacks is simultaneously increasing making it important for organizations and business to secure their systems and applications. A study conducted at Ponemon Institute in 2015 surveyed 350 organizations from 11 different countries that had experienced data breaches. The results proved that nearly half of said breaches (47%) were the effect of a malicious attack and the rest happened because of system glitches and human errors (Vaultes, 2020). This increasing demand of risk and vulnerability assessment gives rise to penetration testing. Penetration Testing is a technique that simulates an attack from a malicious source, for ensuring that flaws or vulnerabilities in networked environments, web applications, and physical premises are known about and can be fixed before they are exploited in a real attack (Tang, 2014).

The detection of vulnerabilities is one of the most significant advantages of penetration testing. Systems that have vulnerabilities can be attacked by intruders for obtaining unauthorized access or do harm. Automated vulnerability scanners are effective for spotting known flaws, but they can be unable to identify undiscovered or specially created flaws. On the other side, penetration testing simulates an assault from a hostile source and can identify weaknesses that other security measures might miss. Analysis of security measures is also a key advantage of penetration testing. Security measures like firewalls, intrusion detection systems, and antivirus software are heavily invested in by organizations. Without routine testing, it is challenging to determine how well these measures are working and whether they are offering the anticipated degree of safety. Penetration testing mimics an attack and offers information on how well the current security measures are working. Additionally, penetration testing can enhance incident response. Organizations may test their incident response plans and procedures by simulating an attack to make sure they are ready to act swiftly and efficiently in the event of a genuine assault.

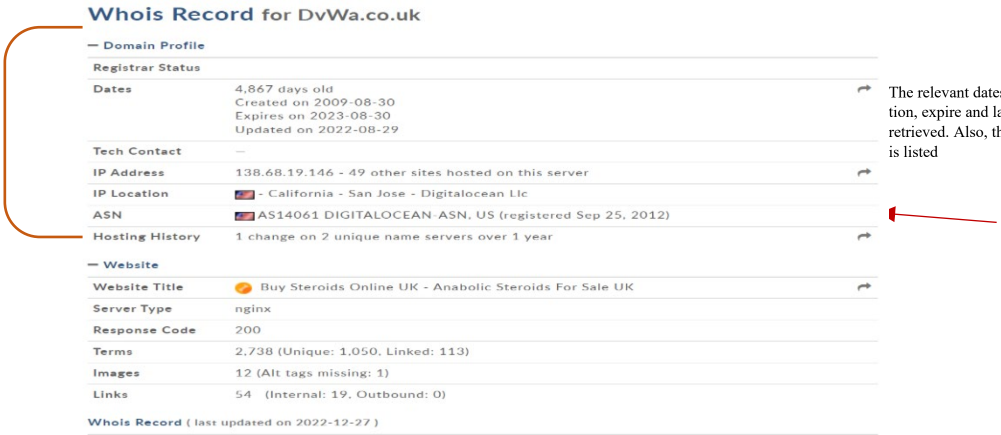
This Report is based on an assignment for the Module "Ethical Hacking". This module provides hands-on practice in choosing and using appropriate tools and techniques as well as the most recent ethical hacking and penetration testing approaches. It helps in analyzing and understanding the core concepts of ethical hacking including the steps of performing penetration testing. The Report aims to:

- To Study several approaches and steps of performing Penetration Testing
- To Perform Footprinting of Publicly available information using multiple techniques
- To Execute the Scanning phase by utilizing multiple tools and techniques
- To Accomplish enumeration by using multiple techniques to retrieve usernames, network shares etc.
- To Identify the vulnerabilities in the network, server and web application being tested and to link them with the Vulnerability Scoring Systems and Databases.
- To Recommend security solutions for protecting against known risks and vulnerabilities.

The Report Comprises of 8 Sections, Section 1 – Introduction, provides an initial understanding of the Report but describing the concept of penetration testing. Section 2 – Footprinting, analyzes and describes different Footprinting techniques and identifies several vulnerabilities. Section 3 – Scanning, examines different scanning tools and techniques and identifies certain key vulnerabilities. Section 4 – Enumeration, evaluates various techniques and tools used to perform enumeration of usernames, network shares, groups etc. Section 5 – Gaining Access, provides understanding of different tools and techniques used for gaining access. Section 6 – Vulnerability Scoring Systems and databases, links the found vulnerabilities in section 2,3 and 4 to Vulnerabilities listed in the Vulnerability scoring Systems and Databases. Section 7 – Security Solutions, recommendations of several security solutions for known risks and vulnerabilities. Section 8 – Conclusion, provides an overall understanding and summary of the penetration testing conducted.

Performing Foot Printing: Domain Tools Who IS Lookup

Whois is a tool that is used around the world as it provides record listing which helps in identifying the owner of the domain and their contact information. Its record contains valid information of a group or company (Domaintools, 2022). Mainly it provides details of the registrant, the name of the servers, recent updates made and the expiry date information. This information can be useful in conducting Footprinting and reconnaissance by collecting information prior to conducting an attack (Domaintools, 2022).



Whois Record for DvWa.co.uk

— Domain Profile

Registrar Status	
Dates	4,867 days old Created on 2009-08-30 Expires on 2023-08-30 Updated on 2022-08-29
Tech Contact	–
IP Address	138.68.19.146 - 49 other sites hosted on this server
IP Location	- California - San Jose - Digitalocean Llc
ASN	AS14061 DIGITALOCEAN-ASN, US (registered Sep 25, 2012)
Hosting History	1 change on 2 unique name servers over 1 year

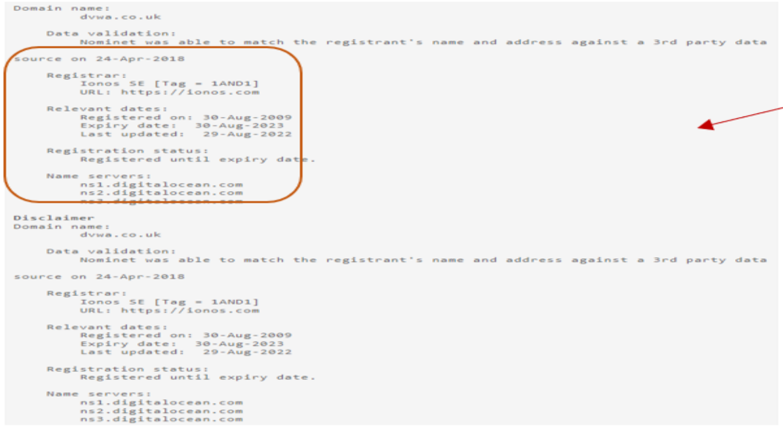
— Website

Website Title	Buy Steroids Online UK - Anabolic Steroids For Sale UK
Server Type	nginx
Response Code	200
Terms	2,738 (Unique: 1,050, Linked: 113)
Images	12 (Alt tags missing: 1)
Links	54 (Internal: 19, Outbound: 0)

Whois Record (last updated on 2022-12-27)

The relevant dates such as registration, expire and last updated dates are retrieved. Also, the name of the server is listed

The IP address and the location of the domain is retrieved.



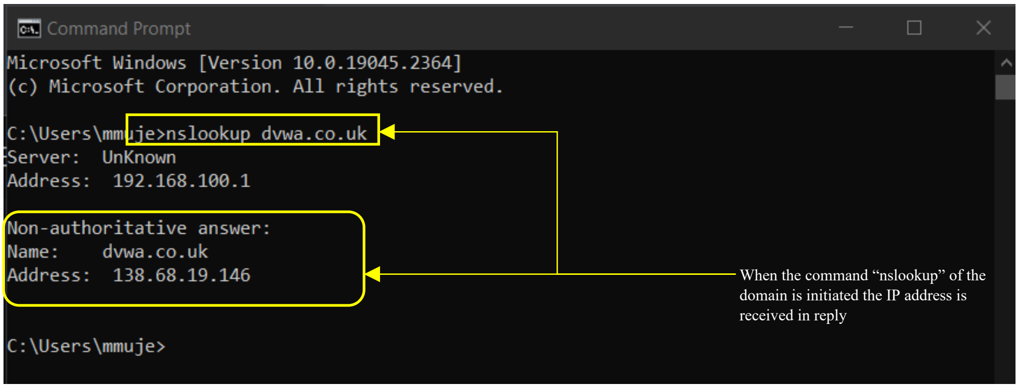
```
Domain name:
        dvwa.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data
source on 24-Apr-2018

    Registrar:
        Ionos SE [Tag = 1AND1]
        URL: https://ionos.com

    Relevant dates:
        Registered on: 30-Aug-2009
        Expiry date:  30-Aug-2023
        Last updated:  29-Aug-2022

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.digitalocean.com
        ns2.digitalocean.com
        ns3.digitalocean.com

Disclaimer
Domain name:
        dvwa.co.uk

    Data validation:
        Nominet was able to match the registrant's name and address against a 3rd party data
source on 24-Apr-2018

    Registrar:
        Ionos SE [Tag = 1AND1]
        URL: https://ionos.com

    Relevant dates:
        Registered on: 30-Aug-2009
        Expiry date:  30-Aug-2023
        Last updated:  29-Aug-2022

    Registration status:
        Registered until expiry date.

    Name servers:
        ns1.digitalocean.com
        ns2.digitalocean.com
        ns3.digitalocean.com
```

The relevant dates such as registration, expire and last updated dates are retrieved. Also, the names of the server is listed

Figure 1. Who is record

NsLookUp

Nslookup is a command-line tool that helps in finding the IP address or DNS record of a specific hostname. It also permits reverse DNS lookup through inputting the IP addresses of the corresponding domains. It is a very useful tool to gather valid information of the host before conducting attacks. It helps in the Footprinting and reconnaissance phase of ethical hacking.



```
Microsoft Windows [Version 10.0.19045.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mmuje>nslookup dvwa.co.uk
Server:  UnKnown
Address:  192.168.100.1

Non-authoritative answer:
Name:    dvwa.co.uk
Address:  138.68.19.146

C:\Users\mmuje>
```

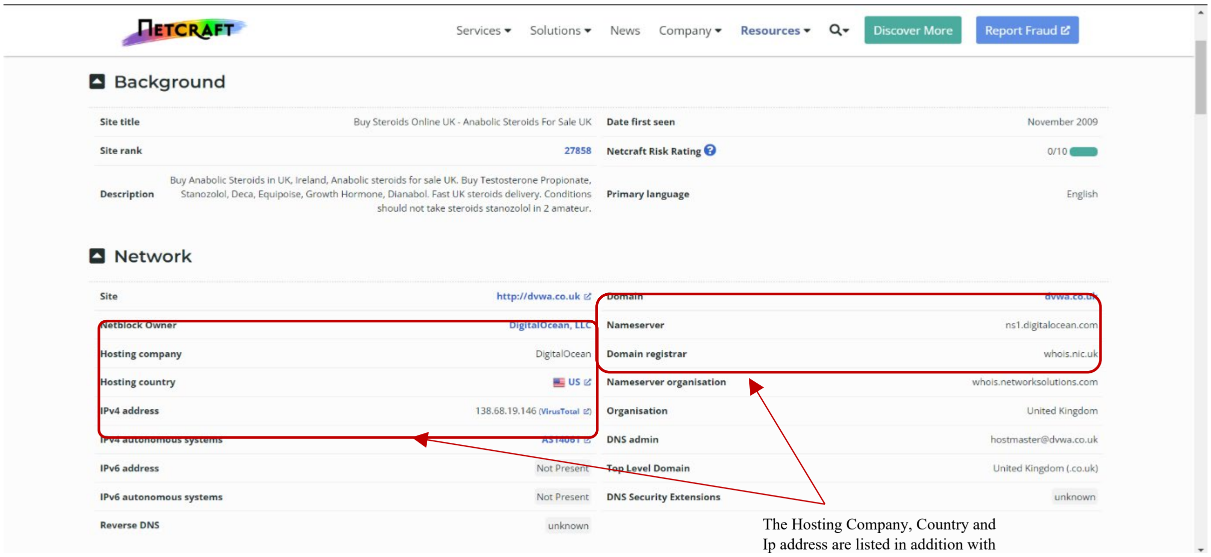
When the command "nslookup" of the domain is initiated the IP address is received in reply

Figure 2. NS look up command

As seen, the command Nslookup helped in getting the IP address for the domain dvwa.co.uk. The Known IP address can provide various possibilities for conducting attacks.

Netcraft

Netcraft is an online-tool used for gathering information as it provides detailed data on the web server through point-to-point data on what is running on the server along with IP address, Whois information, server-side technologies and much more. The information collected can be utilized for finding a valid testing methodology and to help in characterizing the attack surface.



Background

Site title	Buy Steroids Online UK - Anabolic Steroids For Sale UK	Date first seen	November 2009
Site rank	27858	Netcraft Risk Rating	0/10
Description	Buy Anabolic Steroids in UK, Ireland, Anabolic steroids for sale UK. Buy Testosterone Propionate, Stanozolol, Deca, Equipoise, Growth Hormone, Dianabol. Fast UK steroids delivery. Conditions should not take steroids stanozolol in 2 amateur.	Primary language	English

Network

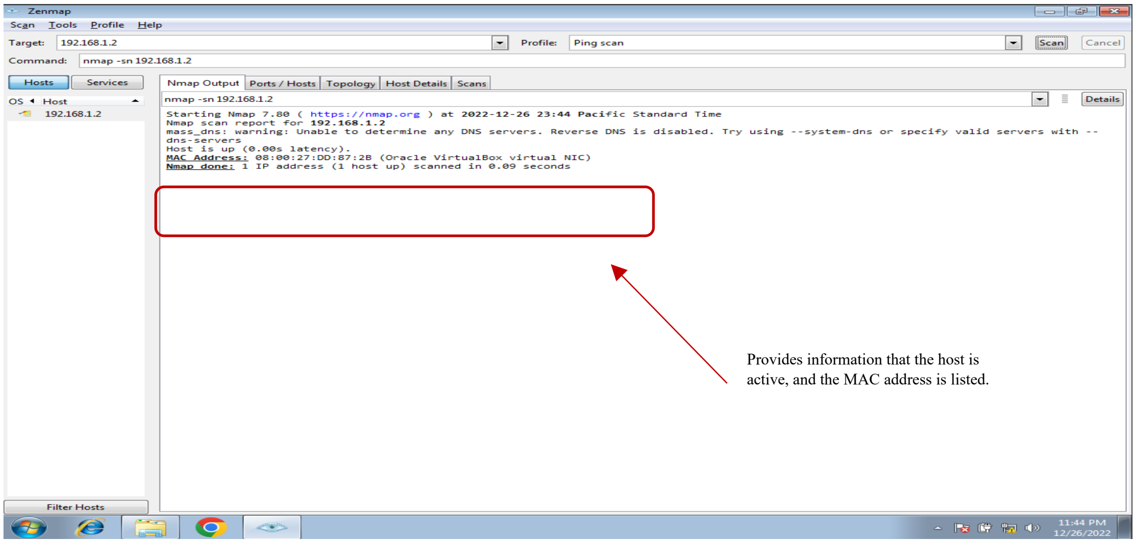
Site	http://dvwa.co.uk	Domain	dvwa.co.uk
Netblock Owner	DigitalOcean, LLC	Nameserver	ns1.digitalocean.com
Hosting company	DigitalOcean	Domain registrar	whois.nic.uk
Hosting country	US	Nameserver organisation	whois.networksolutions.com
IPv4 address	138.68.19.146 (VirusTotal)	Organisation	United Kingdom
IPv4 autonomous systems	AS14061	DNS admin	hostmaster@dvwa.co.uk
IPv6 address	Not Present	Top Level Domain	United Kingdom (.co.uk)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	unknown		

The Hosting Company, Country and
Ip address are listed in addition with
the name of server.

Figure 3. Net craft tool command

Scanning Techniques

Zenmap is a well-known official Nmap security scanner GUI which supports Linux, windows, MAC OS etc. It is a free and Open-source software which allows an interactive creation of Nmap command lines. It allows us to save the scan results and to view them later (Nmap, 2022). The Scope of using this tool was to identify the open ports and OS version that can be vulnerable to attacks.



Target: 192.168.1.2

Profile: Ping scan

Command: nmap -sn 192.168.1.2

192.168.1.2

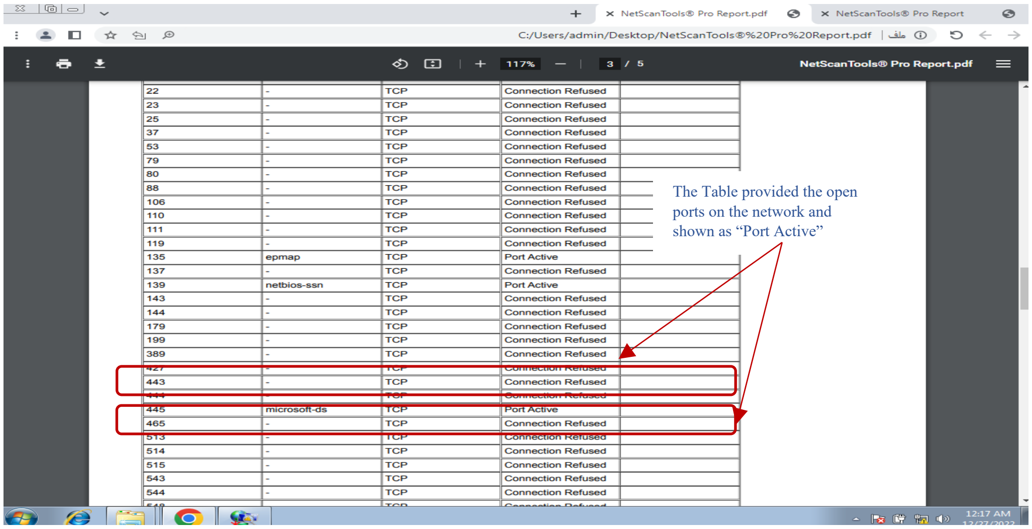
nmap -sn 192.168.1.2

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-26 23:44 Pacific Standard Time
Nmap scan report for 192.168.1.2
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --
dns-servers
Host is up (0.00s latency).
MAC Address: 08:00:27:DD:87:2B (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Provides information that the host is
active, and the MAC address is listed.

Figure 4. Zen map output tool

In the above figure, a ping scan is initiated to verify if the host is active or down. The ping scan provided the result as host is up and provided the MAC address of the Host. After the Ping Scan was successful and the host was active, an intense scan was initiated which helped in discovering the open ports that can be vulnerable. Mostly the TCP ports were open. The tool provided the MAC address and also the OS running on the system that is Windows 7 version 8.1. The distance of the device is 1 hop, and the name of the device is "EH-PC" while the domain is "WORKGROUP." The Report provides the details on the services of the Open Ports such as 135 for epmap, 445 for Microsoft-ds etc.


NetScanTools® Pro Report.pdf
NetScanTools® Pro Report
C:/Users/admin/Desktop/NetScanTools®%20Pro%20Report.pdf
117%
3 / 5
NetScanTools® Pro Report.pdf
12:17 AM

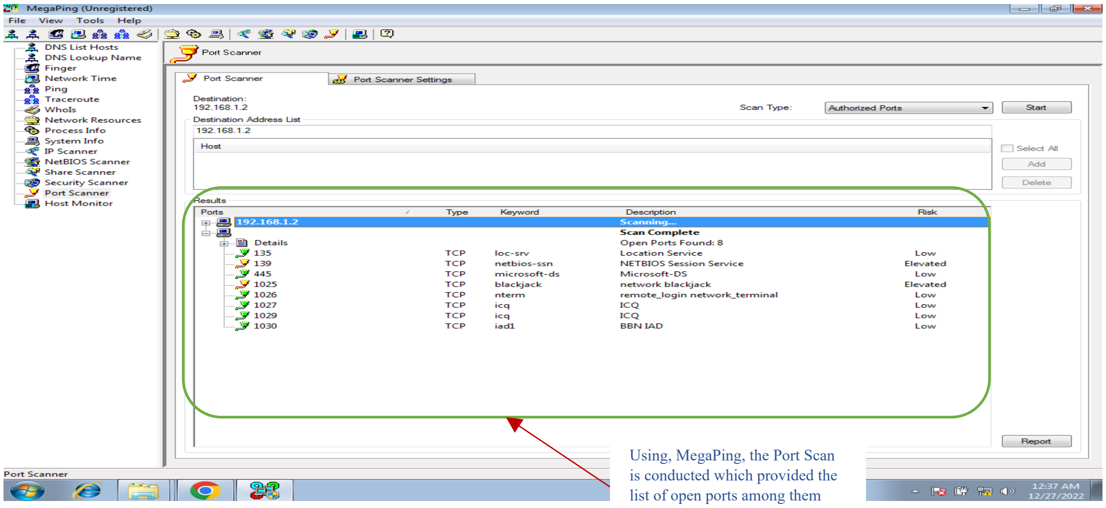
22	-	TCP	Connection Refused	
23	-	TCP	Connection Refused	
25	-	TCP	Connection Refused	
37	-	TCP	Connection Refused	
53	-	TCP	Connection Refused	
79	-	TCP	Connection Refused	
80	-	TCP	Connection Refused	
88	-	TCP	Connection Refused	
106	-	TCP	Connection Refused	
110	-	TCP	Connection Refused	
111	-	TCP	Connection Refused	
119	-	TCP	Connection Refused	
135	epmap	TCP	Port Active	
137	-	TCP	Connection Refused	
139	netbios-ssn	TCP	Port Active	
143	-	TCP	Connection Refused	
144	-	TCP	Connection Refused	
179	-	TCP	Connection Refused	
199	-	TCP	Connection Refused	
389	-	TCP	Connection Refused	
427	-	TCP	Connection Refused	
443	-	TCP	Connection Refused	
444	-	TCP	Connection Refused	
445	microsoft-ds	TCP	Port Active	
465	-	TCP	Connection Refused	
513	-	TCP	Connection Refused	
514	-	TCP	Connection Refused	
515	-	TCP	Connection Refused	
543	-	TCP	Connection Refused	
544	-	TCP	Connection Refused	
548		TCP	Connection Refused	

The Table provided the open ports on the network and shown as "Port Active"

Figure 5. Workgroup domain

Mega Ping

Mega Ping is a network utility that includes a variety of tools for diagnosing and troubleshooting network issues. It can perform a variety of tasks such as ping, traceroute, domain name resolution, and more. It is mainly designed to help pen testers monitor and maintain their networks. Some of the features of Mega Ping include Network monitoring, Traceroute, DNS lookup, Port scanning and Ping. In the Figure below, the IP address is provided for scanning open ports. MegaPing provided all the open ports, the type identified was TCP and simultaneously their risk level is provided.



Destination:
192.168.1.2

Scan Type: Authorized Ports

Destination Address List
192.168.1.2

Host

Results

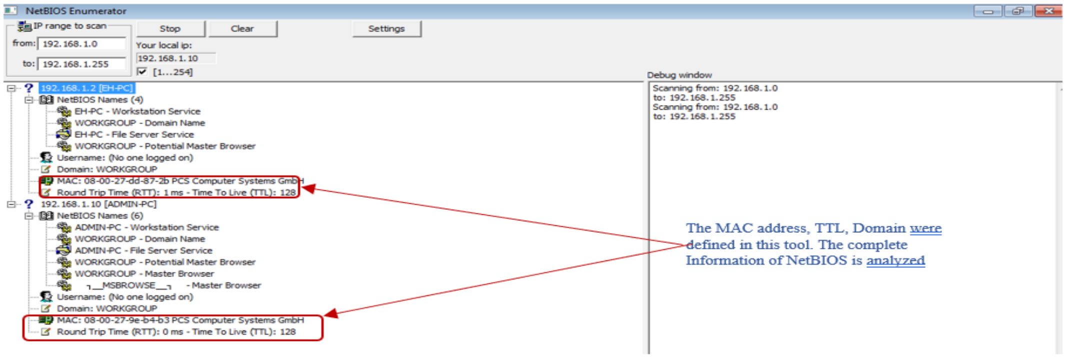
```
Ports                 Type   Keyword         Description                          Risk
192.168.1.2                                  Scanning...
                                             Scan Complete
   Details                                   Open Ports Found: 8
   135                TCP    loc-srv         Location Service                     Low
   139                TCP    netbios-ssn     NETBIOS Session Service              Elevated
   445                TCP    microsoft-ds    Microsoft-DS                         Low
   1025               TCP    blackjack       network blackjack                    Elevated
   1026               TCP    nterm           remote_login network_terminal        Low
   1027               TCP    icq             ICQ                                  Low
   1029               TCP    icq             ICQ                                  Low
   1030               TCP    iad1            BBN IAD                              Low
```

Using, MegaPing, the Port Scan is conducted which provided the list of open ports among them were mainly TCP ports

Figure 6. Mega ping network

Enumeration Techniques

NetBIOS Enumerator can scan a network and identify devices that are using NetBIOS, including the device name, IP address, and other information. This can be useful for pen testers who need to identify and detect NetBIOS-enabled devices on the network. NetBIOS Enumerator is typically used in conjunction with other network management tools, such as network scanners or protocol analyzers. It may be included as a feature in these types of tools, or it may be available as a standalone tool. The Tool provided a list of details on the devices within the IP range, it provided the Hostname, domain name, MAC address, TTL etc. This information can cause harm to the network if the attacker tries to initiate an attack.



from: 192.168.1.0
to: 192.168.1.255
Your local ip: 192.168.1.10
☑ [1...254]

```
192.168.1.2 [EH-PC]
  NetBIOS Names (4)
    EH-PC - Workstation Service
    WORKGROUP - Domain Name
    EH-PC - File Server Service
    WORKGROUP - Potential Master Browser
  Username: (No one logged on)
  Domain: WORKGROUP
  MAC: 08-00-27-dd-87-2b PCS Computer Systems GmbH
  Round Trip Time (RTT): 1 ms - Time To Live (TTL): 128
192.168.1.10 [ADMIN-PC]
  NetBIOS Names (6)
    ADMIN-PC - Workstation Service
    WORKGROUP - Domain Name
    ADMIN-PC - File Server Service
    WORKGROUP - Potential Master Browser
    WORKGROUP - Master Browser
    ┐__MSBROWSE__┐    - Master Browser
  Username: (No one logged on)
  Domain: WORKGROUP
  MAC: 08-00-27-9e-b4-b3 PCS Computer Systems GmbH
  Round Trip Time (RTT): 0 ms - Time To Live (TTL): 128
```

```
Scanning from: 192.168.1.0
to: 192.168.1.255
Scanning from: 192.168.1.0
to: 192.168.1.255
```

The MAC address, TTL, Domain were defined in this tool. The complete Information of NetBIOS is analyzed

Figure 7. Enumeration technique example

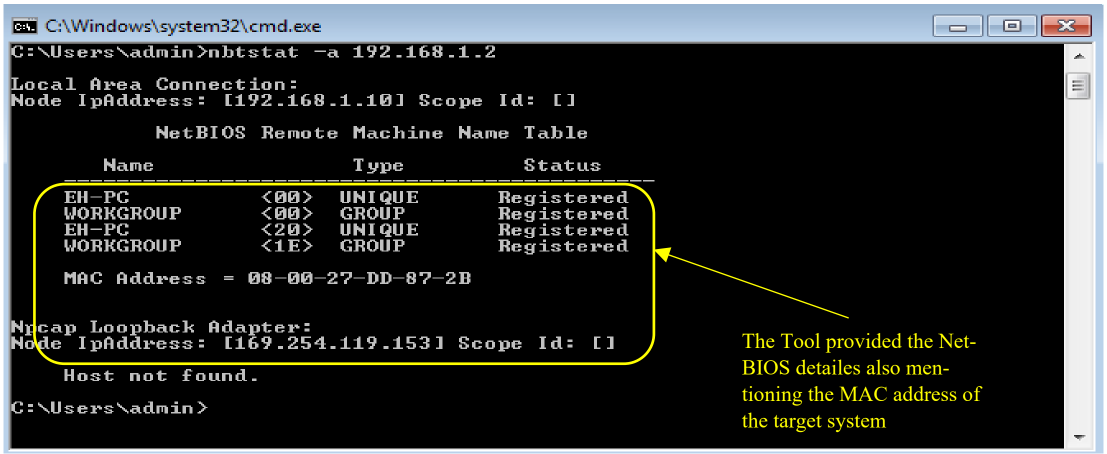
Nbtstat

Nbtstat is a command-line tool that is used to display statistics and information about the NetBIOS over TCP/IP (NBT) protocol on a Windows computer. NBT is a networking protocol that was commonly used in the early days of networking to share resources such as files and printers. It is still used today in some older systems but has largely been replaced by newer protocols such as TCP/IP.

The nbtstat tool can be used to display a variety of information about the NBT protocol, including:

- The NetBIOS name table of a computer, which lists the NetBIOS names that are registered on the computer and their associated IP addresses.
- The NetBIOS name cache of a computer, which lists the NetBIOS names that the computer has recently resolved to IP addresses.
- The NetBIOS sessions that are active on the computer
- The NetBIOS names that conflict with other names on the network

Nbtstat is a useful tool for network administrators, Penetration testing experts and IT professionals who need to troubleshoot issues with the NBT protocol or identify devices that are using NBT on their network. For using nbtstat, it is required to enter the appropriate command and arguments at the command prompt. For example, "nbtstat -n" command can be used for displaying the NetBIOS name table of a computer, or the "nbtstat -a [ip address]" command is used for displaying information about a specific NetBIOS name as performed on the below figure.



```
C:\Users\admin>nbtstat -a 192.168.1.2

Local Area Connection:
Node IpAddress: [192.168.1.10] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    EH-PC          <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    EH-PC          <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered

    MAC Address = 08-00-27-DD-87-2B


Npcap Loopback Adapter:
Node IpAddress: [169.254.119.153] Scope Id: []
    Host not found.

C:\Users\admin>
```

The Tool provided the NetBIOS detailes also mentioning the MAC address of the target system

Figure 8. Command window

Vulnerabilities Found from Foot Printing, Scanning and Enumeration

1. In the Footprinting Phase, the tool Netcraft provided that the site is not HTTPS site, and it is not SSL/TLS validated.
2. In the Scanning Phase, the open ports were identified. Among them Port 135 is open. The inbound Connection in Port 135 TCP is not blocked. As Microsoft DCOM service runs on user's computer, it uses port 135 (ManageEngine, 2022). Port 135 exposes where DCOM services can be found on the machine. Hackers can use tools such as "epdump" which can immediately identify every DCOM-related service running on hosting computer. Therefore, it is recommended that port 135 must not be exposed to the internet and should be blocked (ManageEngine, 2022).
3. Port 445 is recommended to be blocked as it is not safe to publicly expose, and it would help in preventing internal spreading of ransomware.
4. The OS was discovered to be Windows 7, There are several vulnerabilities that can be identified and exploited when using windows 7, as defined in CVE vulnerability assessment scoring system.

Vulnerability Scoring Systems and Databases

Vulnerability scoring systems and databases are tools that are used to assess the risk and impact of vulnerabilities in software and systems. These tools typically assign a numerical score to each vulnerability, based on factors such as the potential impact of the vulnerability, the likelihood of exploitation, and the ease of exploitation (Cyber, 2022). The score is then used to prioritize the vulnerabilities that need to be addressed, with higher scores indicating a greater level of risk and the need for more urgent action (Cyber, 2022).

There are several different vulnerability scoring systems and databases that are used in the industry, including the Common Vulnerability Scoring System (CVSS), the Common Weakness Enumeration (CWE) etc.

Vulnerability scoring systems and databases are an important tool for organizations to use when managing the security of their systems and networks (Cyber, 2022). By using these tools, organizations can identify and prioritize vulnerabilities that need to be addressed and take appropriate steps to mitigate the risks associated with those vulnerabilities.

CWE-311: Missing Encryption of Sensitive Data & CWE-295: Improper Certificate Validation (Common Weakness Enumeration – CWE)

CWE-311 and CWE-295 were appropriate records for the SSL/TLS not validated vulnerability. CWE-311 helps in understanding that the lack of proper data encryption passes up the guarantees of confidentiality, integrity and accountability. When the web application does not utilize a secured channel like SSL for exchanging sensitive information, it is highly possible for an attacker who has access to the network to sniff packets from the connection and uncover the data. CWE-295 mentions that if the certificate is malicious and invalid it would allow the attacker to spoof a trusted entity by interfering in the communication path between the host and client. Therefore, the domain dvwa.co.uk is vulnerable and can be exploited by attacks such as MITM.

CVE-2002-1561: RPC Component (Common Vulnerability Enumeration-CVE)

The RPC Component in windows 200, windows NT allows remote attackers to cause a denial of service through a malformed packet to the RPC Endpoint Mapper at TCP port 135 triggering a null pointer deference (CVE, 2022). Also, the ME vulnerability Manager Plus (ManageEngine, 2022), makes it a requirement to block port 135 as Port 135 exposes where DCOM services can be found on the machine. Hackers can use tools such as “epdump” which can immediately identify every DCOM-related service running on a hosting computer.

CVE-2022-44675: Windows Bluetooth Driver Elevation of Privilege Vulnerability CVE-2022-44670367: Windows SSTP Vulnerability

There are various vulnerabilities associated with windows 7. As the OS was discovered the vulnerabilities listed in the CVE are all associated with it. These vulnerabilities can be exploited by certain attacks that are based on OS discovery.

Security Solutions for Risks and Vulnerabilities

Banner Grabbing is a technique that is utilized by attackers and security teams for obtaining information about the computer systems and services that run on open ports. The host provides a text that displays the type and version of the software running on the system or the server, providing the attackers an advantage in cyber-attacks (GeeksforGeeks, 2022).

There are several countermeasures that help in avoiding banner grabbing. These include,

- For avoiding banner grabbing attacks, organizations must disable their banners on shady affiliate websites which are associated with known hacker forums where malicious tools are sold (GeeksforGeeks, 2022).
- Turning off all unnecessary and unused services that are running on the network hosts to limit information disclosure. (Mutune, 2021)
- Organizations must patch the Softwares which they use that includes antivirus programs and OS (GeeksforGeeks, 2022).
- Restrict access to services on the network and alternatively changing the Server Signature line to serversignature off in the httpd.config file. (Mutune, 2021).

IP Spoofing

IP spoofing mainly refers to creating IP packets with false source IP addresses to impersonate another system. IP Spoofing provides hackers with the ability to conduct malicious action such as DDoS attacks on target system or surrounding infrastructure without getting detected (Kaspersky, 2022). There are several countermeasures to prevent IP spoofing such as,

- Organizations must use VPN to hide their IP address and visit only secured sites which use HTTPS protocol and implement strong password policies (Kaspersky, 2022).
- Organizations can protect their network by using a firewall for securing the systems from unauthorized IP Packets, fake source IP addresses and suspicious traffic.
- Using robust verification methods to protect from IP spoofing (Kaspersky, 2022).
- Deploying packet filtering for detecting inconsistencies such as outgoing packets with source IP addresses which do not match those on the organizations network.

Enumeration

Enumeration is described as way of extracting information such as usernames, hostnames, network resources, shares and services from a system. In Enumeration, the hacker builds an active connection to the system and performs directed queries for gaining further information about the target. The information that is gathered is utilized for identifying the weaknesses in the system security that would help the hacker to exploit the system (Greycampus, 2022). There are several security countermeasures to block enumeration. These include (Upguard, 2021),

- To prevent reverse DNS sweeping (enumeration attack) from working, make sure that private hostnames aren't linked to IP addresses in the DNS zone files of publicly accessible DNS servers (etutorials, 2021).
- Configuring SMTP servers to either reject emails from unidentified senders or to send replies without internal IP addresses or host information (etutorials, 2021).
- Configuring each name server to prevent the transmission of DNS zones to untrusted hosts (etutorials, 2021).
- There must be a multi-factor authentication mechanism. As authentication is requested with each login attempt, the attackers will not have access to any server responses until they submit a correct authentication token first.
- Using CAPTCHA in all forms helps in effectively blocking automated enumeration attacks.
- There needs to be a limit set for the login attempts made. When the login process is blocked after several failed attempts from the same IP address then it would not be possible for an attacker to conduct enumeration attacks
- Use WAF which is a web application firewall that helps in blocking suspicious login attempts that is coming from single IP address.

Social Engineering

Social Engineering refers to a broad range of malicious activities that are performed through human interactions. It is basically considered an art of convincing people to reveal confidential information. It takes place when people are unaware of the valuable information to which they have access and are careless about protecting it. It mainly deals with psychological manipulations (Imperva, 2019). There are several security countermeasures that help in blocking social engineering attacks (Imperva, 2019).

- It is Highly important to spread awareness in the society and community by providing free training sessions.
- It is necessary to periodically change passwords as this would reduce the possibility of social engineering attacks.
- Blocking accounts after several failed password attempts. This will stop the attacker from trying different combinations of passwords.

- It is important for organizations to employ security personals and issue identity cards for their employees.
- Do not attempt to open emails and attachments from suspicious sources.

Conclusion

In conclusion, learning penetration testing in a virtual environment provides a safe and effective way for beginners to gain hands-on experience in the field of cybersecurity. Using virtual machines and simulated networks, students can learn and practice various techniques such as Footprinting, scanning, and enumeration, without the risk of causing damage to real systems. Foot printing allows individuals to gather information about a target system, which is a crucial first step in any penetration testing engagement. Scanning involves the use of tools to identify open ports, services, and vulnerabilities that can be exploited. Enumeration involves the process of gathering information about users, shares, and other resources within a network. In general, the use of virtual environments for learning penetration testing offers numerous benefits, including flexibility, scalability, and cost-effectiveness. Students can practice and develop their skills in a safe and controlled environment, and instructors can easily monitor their progress and provide feedback. As cybersecurity threats continue to evolve, it is imperative that we equip the next generation of professionals with the skills and knowledge needed to protect our digital assets.

References

Vaultes. (2020). Why penetration testing is important. https://www.vaultes.com/why-penetration-testing-is-important/#:~:text=The%20main%20reason%20penetration%20tests,security%20policies%20are%20genuinely%20effective.

Tang, A. (2014). A Guide to Penetration Testing. Network Security, 2014(8), 8–11. https://doi.org/10.1016/s1353-4858(14)70079-0

Panda Security. (2022). What is a man-in-the-middle (MITM) attack? definition and prevention. https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/

Invicti. (2022). Cookie not marked as secure. https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/cookie-not-marked-as-secure/

Invicti. (2022). Insecure Transportation Security Protocol Supported. https://www.invicti.com/eb-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/

Alfaro, J. G., & Arribas, G. N. (2009). A Survey on Cross-Site Scripting Attacks. https://doi.org/10.48550/arXiv.0905.4850

Krasniqi, G., & Bejtullahu, V. (2018). Vulnerability assessment and penetration testing: Case study on web application security. 2018 UBT International Conference. https://doi.org/10.33107/ubt-ic.2018.213

Kareem, F. Q., Ameen, S. Y., Salih, A. A., Ahmed, D. M., Kak, S. F., Yasin, H. M., Ibrahim, I. M., Ahmed, A. M., Rashid, Z. N., & Omar, N. (2021). SQL Injection Attacks Prevention System Technology: Review. Asian Journal of Research in Computer Science, 13–32. https://doi.org/10.9734/ajrcos/2021/v10i330242

Invicti. (2022). Internal Server Error. https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/internal-server-error/

Invicti. (2022). Missing X-Frame-Options Header. https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-x-frame-options-header/

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. International Journal of Computer Applications, 182(33), 27–29. https://doi.org/10.5120/ijca2018918286

Tal, L. (2019). 84% of all websites are impacted by jQuery XSS Vulnerabilities. Medium.
https://lirantal.medium.com/84-of-all-websites-are-impacted-by-jquery-xss-vulnerabilities-snyk-4c73a935ab11

CWE. (2022). CWE-550: Server-generated Error Message Containing Sensitive Information.
https://cwe.mitre.org/data/definitions/550.html

Yari, I. A. (2016). Vulnerability Assessment of Web Applications and Recommendations for Actions: Penetration Testing Report. Friedrich-Alexander-University of Erlangen-Nürnberg.
https://doi.org/10.13140/RG.2.2.16548.40323

Varshney, G., Misra, M., & Atrey, P. (2017). Browshing a new way of phishing using a malicious browser extension. 2017 Innovations in Power and Advanced Computing Technologies (i-PACT).
https://doi.org/10.1109/ipact.2017.8245147

Tanwar, R., Choudhury, T., Zamani, M., & Gupta, S. (2021). Information security and optimization (1st ed.).
Namecheap. (2022). What is ModSecurity and why do we need it?.
https://www.namecheap.com/support/knowledgebase/article.aspx/9542/22/what-is-modsecurity-and-why-do-we-need-it/

Sheldon, R. (2022). 12 best patch management software and Tools for 2023. Enterprise Desktop.
https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools

nmap. (2022). Zenmap - Official cross-platform nmap security scanner GUI. Retrieved from
https://nmap.org/zenmap/
ManageEngine. (2022).
.
Cyber. (2022). What is vulnerability scoring system and Databases. https://www.xmcyber.com/glossary/what-is-common-vulnerability-scoring-system/

CVE. (2022). Vulnerability details : CVE-2002-1561. https://www.cvedetails.com/cve/CVE-2002-1561/

Mutune, G. (2021). Banner grabbing. https://cyberexperts.com/encyclopedia/banner-grabbing/

GeeksforGeeks. (2022). What is banner grabbing? https://www.geeksforgeeks.org/what-is-banner-grabbing/

Kaspersky. (2022). IP spoofing: How it works and how to prevent it. https://www.kaspersky.com/resource-center/threats/ip-spoofing

Greycampus. (2022). Enumeration and its types. Ethical Hacking.
https://www.greycampus.com/opencampus/ethical-hacking/enumeration-and-its-types

Upguard. (2021). What is an enumeration attack? how they work + prevention tips.
https://www.upguard.com/blog/what-is-an-enumeration-attack

Imperva. (2019). What is Social Engineering: Attack Techniques & Prevention Methods.
https://www.imperva.com/learn/application-security/social-engineering-attack/