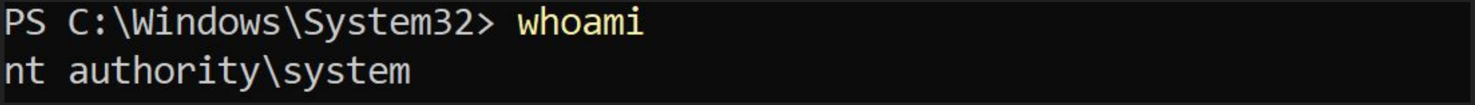
Cybersecurity and Ethical Hacking

Neel Bhavsar



```
PS C:\Windows\System32> whoami
nt authority\system
```

- BITS Hyderabad 2019 Graduate, Bronze Medalist
- Offensive Security Student
  - OSCP | OSCE | OSWP
  - Mantra is to “Try Harder”
- Software Developer @Microsoft
  - Always looking for something to learn
  - MTA - Security, Networking, Server Admin
- Hobbies : Yoga, Cooking, Swimming, Computers (Of course)
- Twitter : @3vilbuff3r

```
[root@archlinux ~/cybersec-talk]# cat agenda
```

- Stories, Random chats and interactions
- How something gets hacked? : A 1000 ft View
- Let's hack this box?
- Questions
- Your perspectives, feedback and more resources

@N got hacked!

- How I Lost My $50,000 Twitter Username - Naoki Hiroshima
- $50,000 handle
- Simple called up the paypal guys and asked for last 4 digits of the credit card
- Brute forced the first 2 digits on GoDaddy to hijack GoDaddy, DNS and MX servers.
- Hiroshima had to give up on the username handle.

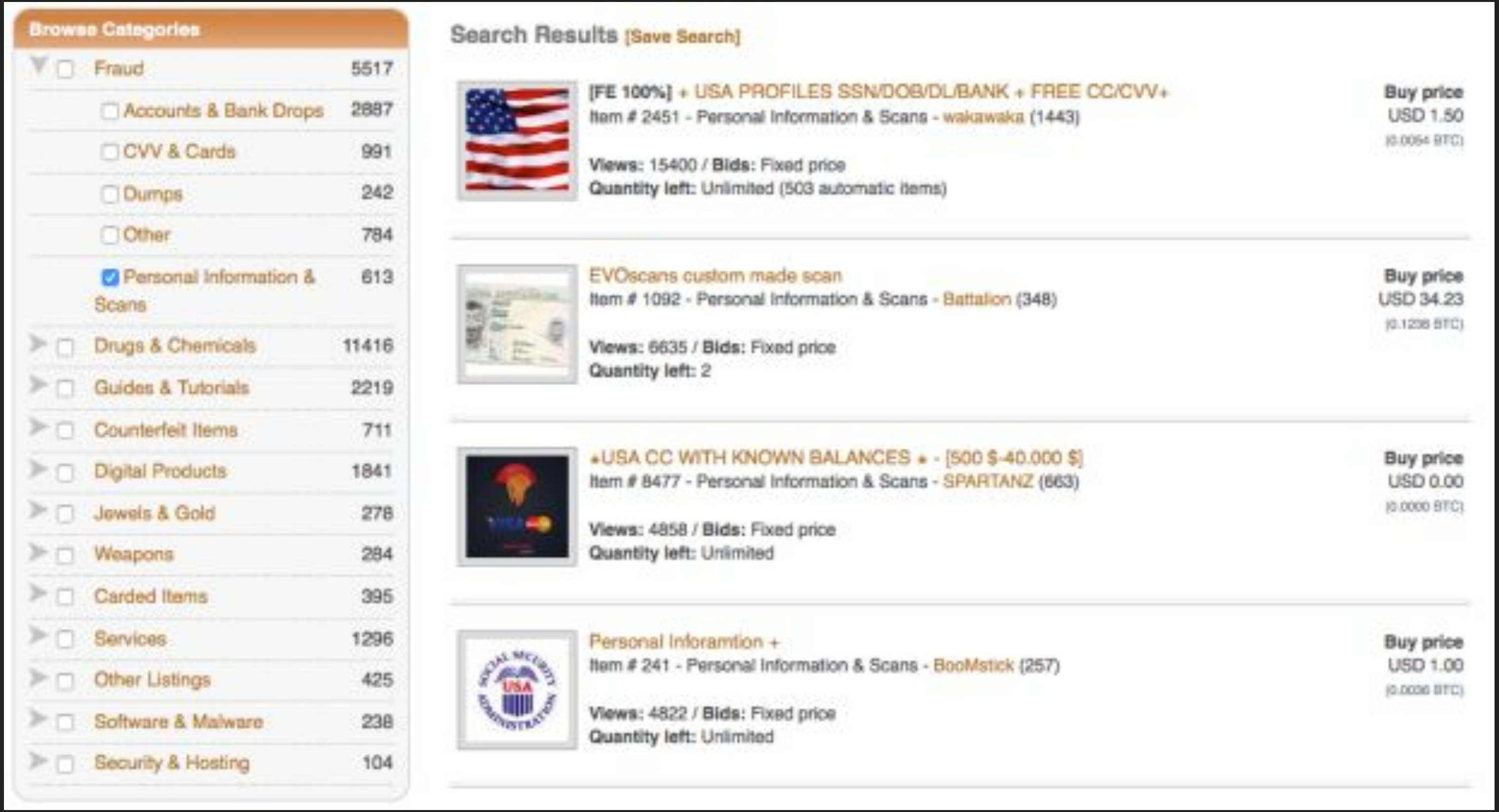
I don’t own a server. Why do I care?

- I have got nothing to hide!!
- Use facebook / instagram / snapchat?
- Snapchat was involved in a big data breach in 2014
- Recently an Indian Researcher was awarded $30,000 bounty for finding a logical flaw in password reset function in instagram
- Every damn application on your phone asks for your personal data and most of them don’t know how to handle sensitive data.

Data leaks : Leaking phone numbers, emails ..

- It’s just a phone number.
- Is it?
- Where do you get your bank OTP
- 2 factor authentication challenges
- Bank account transaction messages
- Password reset codes from facebook, twitter?
- The more detailed profile .. bigger price for selling it!

Yes, people are sold! : Identity markets



Browse Categories

□ Fraud	5517
□ Accounts & Bank Drops	2887
□ CVV & Cards	991
□ Dumps	242
□ Other	784
☑ Personal Information & Scans	613
□ Drugs & Chemicals	11416
□ Guides & Tutorials	2219
□ Counterfeit Items	711
□ Digital Products	1841
□ Jewels & Gold	278
□ Weapons	284
□ Carded Items	395
□ Services	1296
□ Other Listings	425
□ Software & Malware	238
□ Security & Hosting	104

Search Results [Save Search]

[FE 100%] + USA PROFILES SSN/DOB/DL/BANK + FREE CC/CVV+
Item # 2451 - Personal Information & Scans - wakawaka (1443)
Views: 15400 / **Bids:** Fixed price
Quantity left: Unlimited (503 automatic items)
Buy price USD 1.50 (0.0054 BTC)

EVOscans custom made scan
Item # 1092 - Personal Information & Scans - Battalion (348)
Views: 6635 / **Bids:** Fixed price
Quantity left: 2
Buy price USD 34.23 (0.1238 BTC)

+USA CC WITH KNOWN BALANCES + - [500 $-40.000 $]
Item # 8477 - Personal Information & Scans - SPARTANZ (663)
Views: 4858 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 0.00 (0.0000 BTC)

Personal Inforamtion +
Item # 241 - Personal Information & Scans - BooMstick (257)
Views: 4822 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 1.00 (0.0036 BTC)

So what is cybersecurity anyway?

- Cisco
    - Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.
- What’s included?
    - Computers
    - Networks
    - Power Grids
    - Mobiles
    - IoT
    - The Cloud

And Ethical Hacking?

- Ethical -- Hacking
- Legal, with good intentions and with written permission
- Hats
  - White hats
  - Black hats
  - Gray hats
- What do they do?
  - Try find vulnerabilities before the bad guys do
  - Patch them ALL
- Red team / Blue team

Careers in Cybersecurity

- Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021
- There is a zero-percent unemployment rate in cybersecurity and the opportunities in this field are endless
- Roles
    - Security Architect
    - Vulnerability researcher
    - Penetration Tester
    - Threat analyst
    - Cyber security manager
    - Legal

```
[root@archlinux ~/cybersec-talk]# cat how-to █
```

- Reconnaissance
- Active Scanning
- Service identification
- Exploitation
- Post exploitation
- Privilege escalation
- Covering your tracks!

DISCLAIMER

- This knowledge is for educational purposes only
- Only attack the lab machines and nothing outside the scope
- I will not be responsible for the damage caused

Reconnaissance

- Doing your research
  - Domains
    - www.victim.com, ftp.victim.com, internal.victim.com
  - IP ranges
    - 63.35.124.32-80
  - People and their pets
  - Affiliations
    - Has ties with ABC company
    - Uses ‘wordpress’ to host their internal blogging website.
    - Uses kaspersky antivirus in all company computers
  - Locations

Active Scanning

- In reconnaissance we never touch the target directly
- Probing the target
  - Interacting with the servers
- Port scanning
  - TCP/UDP
  - Nmap
  - OS fingerprinting
- Vulnerability Scanning
  - Bulk scan for publicly disclosed vulnerabilities

Service Identification

- What is the role of the server in the network
- What services are running?
  - http
  - dns
- Any out of date services?
  - shodan
- Public exploits
  - exploit-db
- Source code review and 0-day exploits

Exploitation

- Finding and modifying publicly available exploits
- Exploit development and 0-day exploits
- Owning the target

Post Exploitation

- Look around, what you see? Anything that you did not have access from outside
- Password gathering and cracking
- Monitoring user activities, taking photos, keyloggers
- Persistence - Creating hidden service
- Pivoting - Going deeper into the network

Privilege escalation

- What’s the fun if you’re not the *root*
- OS Exploits - Are you using older versions of the operating systems?
- Configuration errors - Running processes as root,
- Permission errors - Not following Principle of Least Privilege

Covering your tracks!

- Remove traces of exploits
- Clean up logs
  - or better yet remove only your activities
- Bypassing anti-viruses

Demo...

What are your perspectives? Feedback?

- Love it? Hate it? What did you like? What you didn’t?
- How can we make it better?
- What else would you like to include?

Where can I learn more?

- Vulnerable machine images : Vulnhub.com
- Vulnerable machine labs (free and paid) : Hackthebox.eu
- Challenges and learning references : Rootme.org
- Step by step self learn : overthewire.org
- Certifications and Training : https://www.offensive-security.com
- Books
  - Kali Linux Revealed
  - Hacking : art of exploitation
  - Hacking Exposed
  - Fun read : Ghost in the wires, Kevin Mitnick
  - Smart girl’s guide to privacy

References and Thanks to

- https://cybersecurityventures.com/jobs/
- https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd
- https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- https://www.vulnhub.com/
- @DCAU7 for the base image of the vulnerable machine used in the demo

Thank You