Getting Started with Cyber Security Domain

KNOW YOUR SPEAKER

Veshraj Ghimire

Associate Cyber Security Engineer
@Vairav Technology

Part-Time Bug Bounty Hunter

CEH(practical), eJPT, eWPTxV2

Topics to be covered

- Introduction
- Career Paths
- Getting started
- Career Progression
- Certifications
- Fun Game
- Q&A

Introduction

What really is cybersecurity?

- Practice of **protecting** computer systems, networks, software, and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

Why cybersecurity in today's date?

- Digital Revolution
- Rise in Cybercrime
- Privacy Concerns and Data Protection

Growing Demand for Cybersecurity Professionals

- With increase in risks, the opportunity as a cyber professional increases
- Lucrative Job Market

Career paths

Red Team

- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

Blue Team

- Defensive Security
- Infrastructure Protection
- Damage Control
- Incident Response
- Operational Security
- Threat Hunting
- Digital Forensics

OPPORTUNITIES IN OFFENSIVE SECURITY

Penetration tester

- Also known as ethical hacker
- Responsible for assessing and identifying vulnerabilities
- Use different methodologies to find out potential issues and help them remediate

Red teamer

- Conducts simulated real-world cyber attacks on organization
- Use various attack techniques, such as social engineering, network exploitation, and physical security breaches, to identify weaknesses and help organizations enhance their security defenses

Exploit Developer

- Create and design software exploits to take advantage of vulnerabilities in systems or applications
- Develop code or techniques that can be used for penetration testing, vulnerability research, or offensive security purposes.

Bug bounty hunter

- Cybersecurity professionals who actively search for security vulnerabilities in systems, applications, or websites.
- Participate in bug bounty programs, which are initiatives offered by organizations to reward individuals for responsibly disclosing vulnerabilities.

Opportunities in Defensive Security

Security Operations Center (SOC) Analyst

- responsible for monitoring and analyzing security events and alerts in real-time
- Investigate potential security incidents, triage alerts, and respond to threats to maintain the security and integrity of an organization's digital assets.

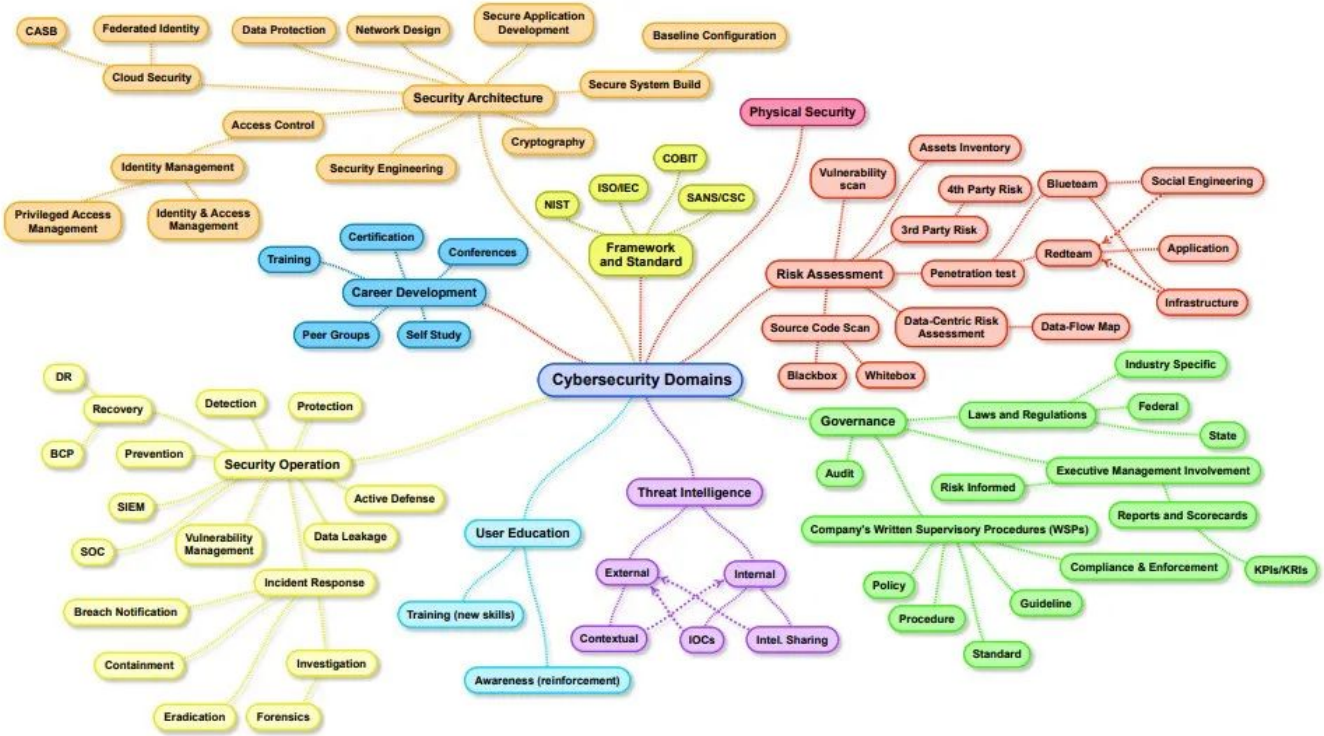
Incident responder

- Detect and respond to cybersecurity incidents promptly.
- Investigate security breaches and develop strategies to prevent future attacks
- Minimizing the impact of security incidents and restoring normal operations.

Security Compliance Analyst

- Ensure that an organization's security practices align with industry regulations and standards.
- Assess and monitor compliance with frameworks like ISO 27001, NIST, or GDPR, and work to ensure that security controls are implemented effectively.

Not limited!


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Physical Security
Framework and Standard
NIST
ISO/IEC
COBIT
SANS/CSC
Career Development
Training
Certification
Conferences
Peer Groups
Self Study
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Redteam
Social Engineering
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Risk Informed
Executive Management Involvement
Company's Written Supervisory Procedures (WSPs)
Reports and Scorecards
KPIs/KRIs
Compliance & Enforcement
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Prevention
Detection
Protection
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

So how to get started?

Understanding how internet works

- Networking Fundamentals
- How Webserver works
- Ports and protocols, different network services, OSI Layer and TCP/IP Layer, HTTP requests, HTTP request methods, HTTP responses, DNS, IPv4 and IPv6

Learning to code

- Not mandatory to be able to build a good looking application, but need to learn up to the point where you can solve different problems with JavaScript and a backend technology like PHP, Python or Node.js
- Learn a SQL and a NoSQL database technology
- Learn C,C++ and rust for reverse engineering/Binary Exploitation

Learning practically

- Hackthebox
- TryHackme
- Portswigger Web Academy
- Picoctf
- PentesterLab
- Over the Wire,etc

Connecting with like minded peoples

- Networking,support,quick better understanding

Join cyber security communities:

- Pentester Nepal
- r/cybersecurity

Staying up to date

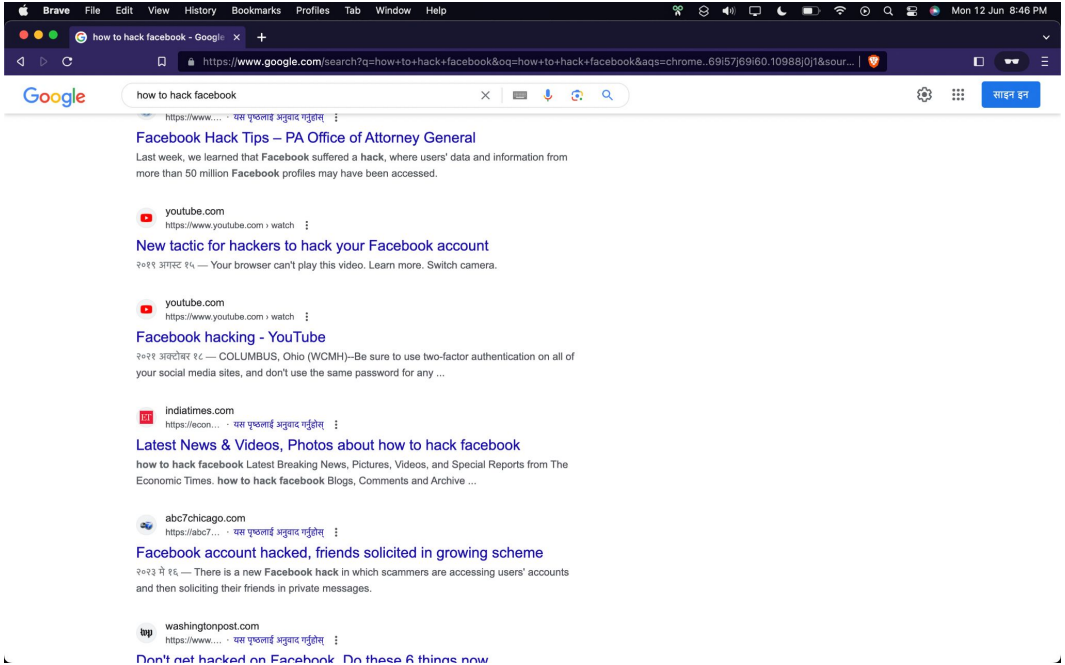
- Follow hashtags, professionals on twitter
- Read blogs regularly
- Spend time on researching about latest vulnerabilities found by other researchers

Career progression

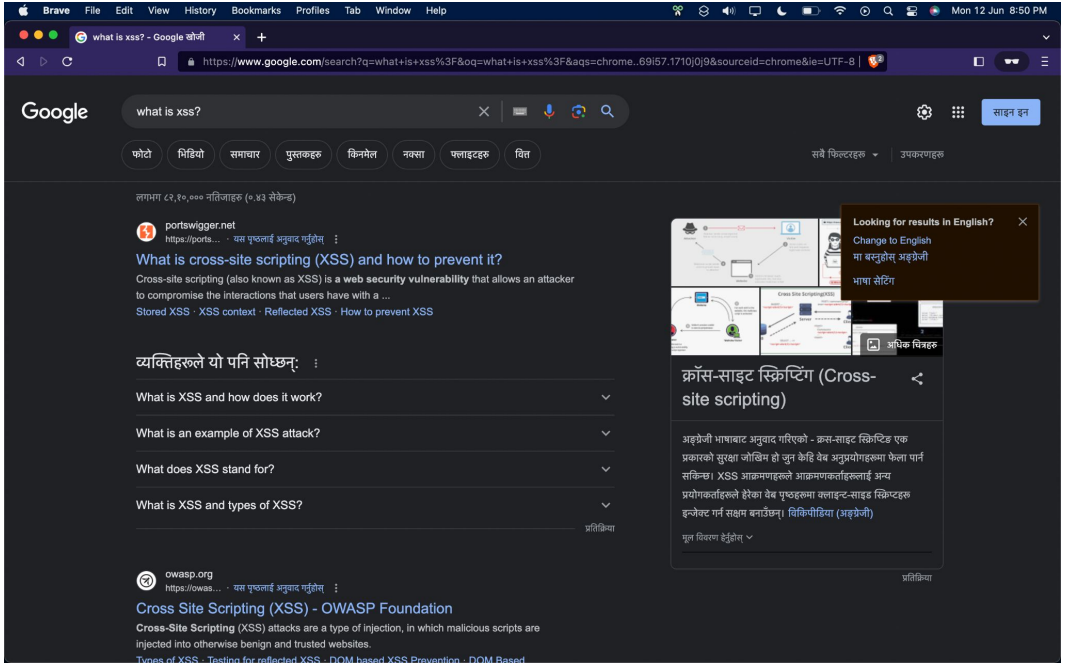
Learn to google!!

Get curious and keep searching

How not to use google ❌



How to use google ✅

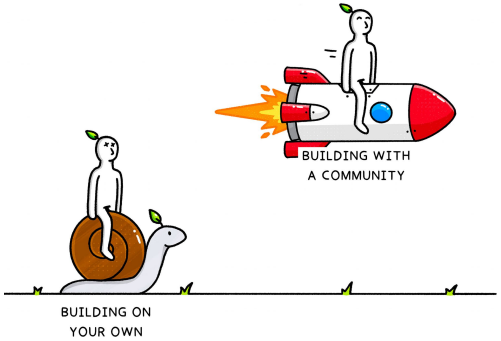


Specialize in specific area

- Deep Expertise: Helps you to become a subject matter expert, which can lead to increased recognition and credibility within your industry
- Competitive Advantage: When seeking career advancement opportunities or pursuing higher-level positions.

Contribute to the community

- Builds a Strong Professional Network
- Personal and Professional Growth
- Makes a Positive Impact



Consistency is the key!

- Schedule things
- Don’t try to finish everything in a single day
- Rome wasn’t built in a day, Good thing takes time

Obtain Advance certifications

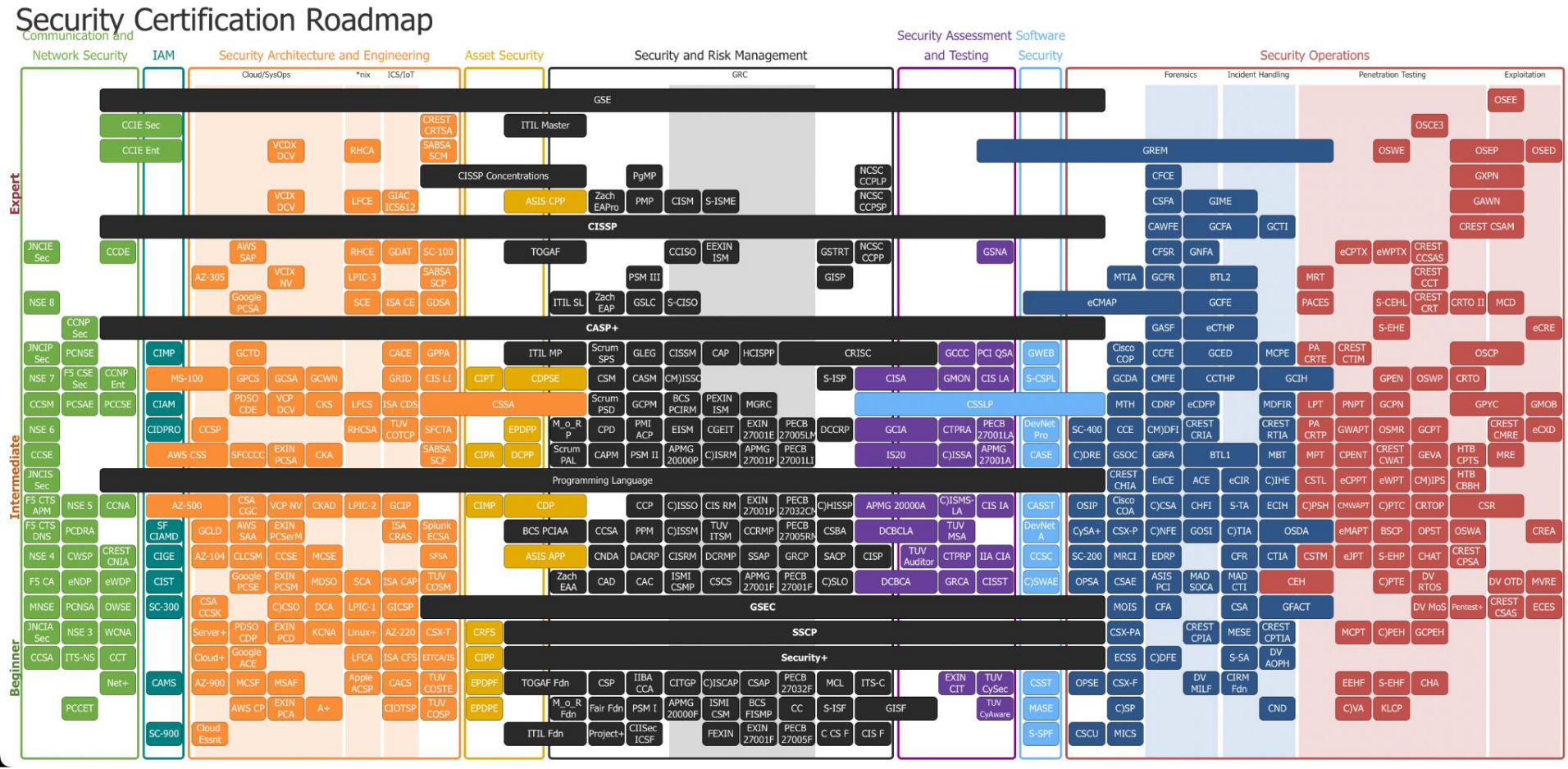
- Increased Career Opportunities
- Enhanced Knowledge and Skills
- Industry Recognition and Credibility

Certifications

Popular certifications

- CISSP
- CISA
- Security+
- CEH
- CISM
- GSEC
- SSCP
- OSCP

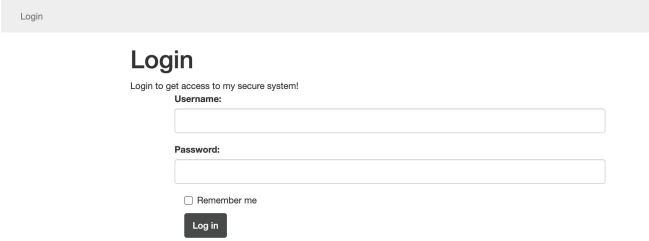
Source: https://www.coursera.org/articles/popular-cybersecurity-certifications



Source: https://pauljerimy.com/security-certification-roadmap/

FUN GAME

Spot the vulnerability #1



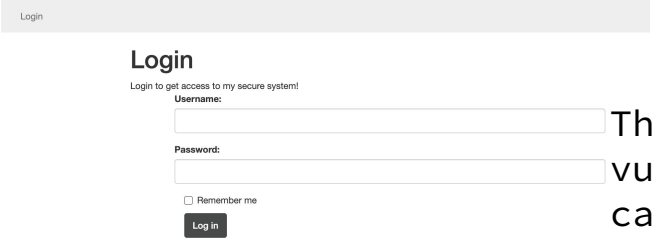

```
1  SELECT * FROM user WHERE login='[USER]' and password='[PASSWORD]';
```

Where: **[USER]** and **[PASSWORD]** are the values you submitted.

The logic behind the authentication is:

- if the query returns at least one result, you're in
- if the query returns no result, you have not provided a valid username and password.

Spot the vulnerability #1



This type of vulnerability is called SQL injection

Username: 'or 1=1 #

How?

```
1  SELECT * FROM user WHERE login='[USER]' and password='[PASSWORD]';
```

Where: **[USER]** and **[PASSWORD]** are the values you submitted.

The logic behind the authentication is:

- if the query returns at least one result, you're in
- if the query returns no result, you have not provided a valid username and password.

Our goal is to make the query return at least one result. To do so we are going to inject a condition that is always true: **1=1**. To do that, we are going to:

- Break outside of the single quote to be able to inject SQL using a single quote.
- Add a **OR** keyword to make sure the comparison is always true.
- Add our always true comparison: **1=1**
- Comment out the remaining query using **--** (the space at the end matters) or **#**.

Spot the vulnerability #2

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

Spot the vulnerability #2

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }

}
?>
```

This type of issue is called command injection where attacker can execute his arbitrary command on host.

Ping for FREE

Enter an IP address below:

127.0.0.1; ls -la /root submit

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.042 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.012/0.023/0.042/0.013 ms
total 76
drwxr-xr-x 13 root root 4096 Jul  2 08:04 .
drwxr-xr-x 21 root root 4096 May 22  2018 ..
-rw-------  1 root root  324 Jul  2 08:04 .Xauthority
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history -> /dev/null
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
drwx------  3 root root 4096 May 20  2012 .config
drwx------  2 root root 4096 May 20  2012 .filezilla
drwxr-xr-x  5 root root 4096 Jul  2 08:04 .fluxbox
drwx------  2 root root 4096 May 20  2012 .gconf
drwx------  2 root root 4096 May 20  2012 .gconfd
drwxr-xr-x  2 root root 4096 May 20  2012 .gstreamer-0.10
drwx------  4 root root 4096 May 20  2012 .mozilla
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
drwx------  5 root root 4096 May 20  2012 .purple
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4096 May 20  2012 .ssh
drwx------  2 root root 4096 Jul  2 08:04 .vnc
drwxr-xr-x  2 root root 4096 May 20  2012 Desktop
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
-rw-r--r--  1 root root  138 Jul  2 08:04 vnc.log
```

Thank you!

VeshrajGhimire

GhimireVeshraj