THE NORTHCAP UNIVERSITY

Exploitation of multiple targets using Armitage

30 YEARS OF EXCELLENCE

NAAC Accredited

Exploiting multiple targets with Armitage

THE NORTHCAP UNIVERSITY

- Armitage inbuilt Kali Linux tool
- **GUI interface** in favor of the Metasploit console (CLI).
- It also **allows you to test multiple targets** at the same time —**up to 512 targets** at once.

YEARS OF EXCELLENCE

NAAC Accredited

Exploiting multiple targets with Armitage

THE NORTHCAP UNIVERSITY

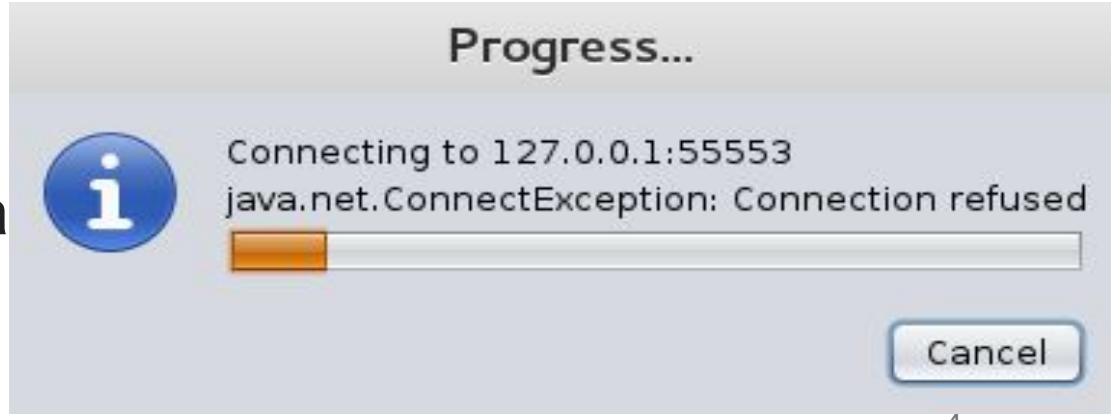
1. To start Armitage, ensure that the **database** and Metasploit **services** are started using
   - **Service postgresql start**
   - **Service metasploit start**

2. Start Armitage
   - **Armitage**
   - Accept the defaults for the rest of the Armitage scre

Exploiting multiple targets with Armitage

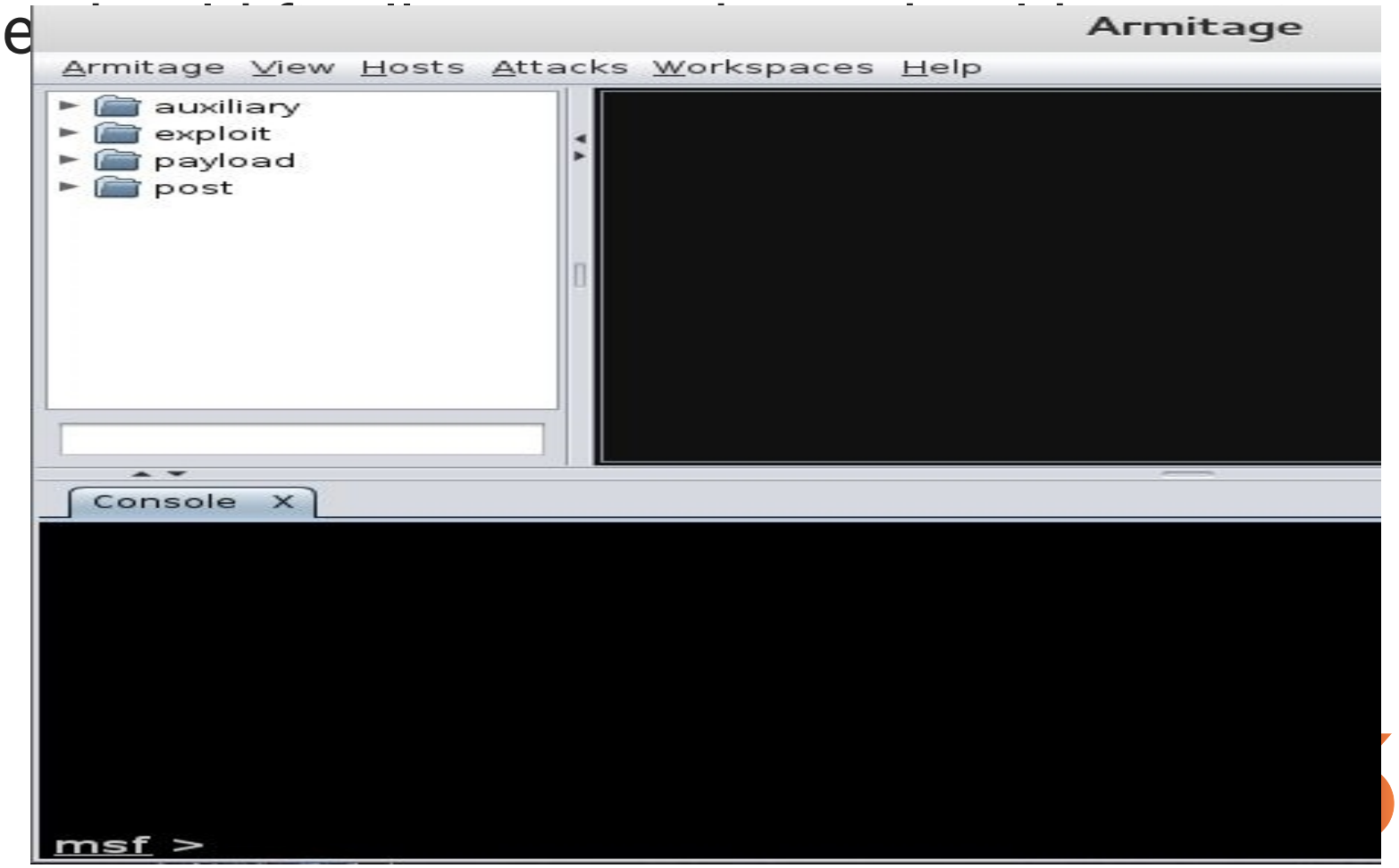
2. Start Meta

3. Starting the connection
   - Metasploit RPC server starts in the ba



Exploiting multiple targets with Armitage

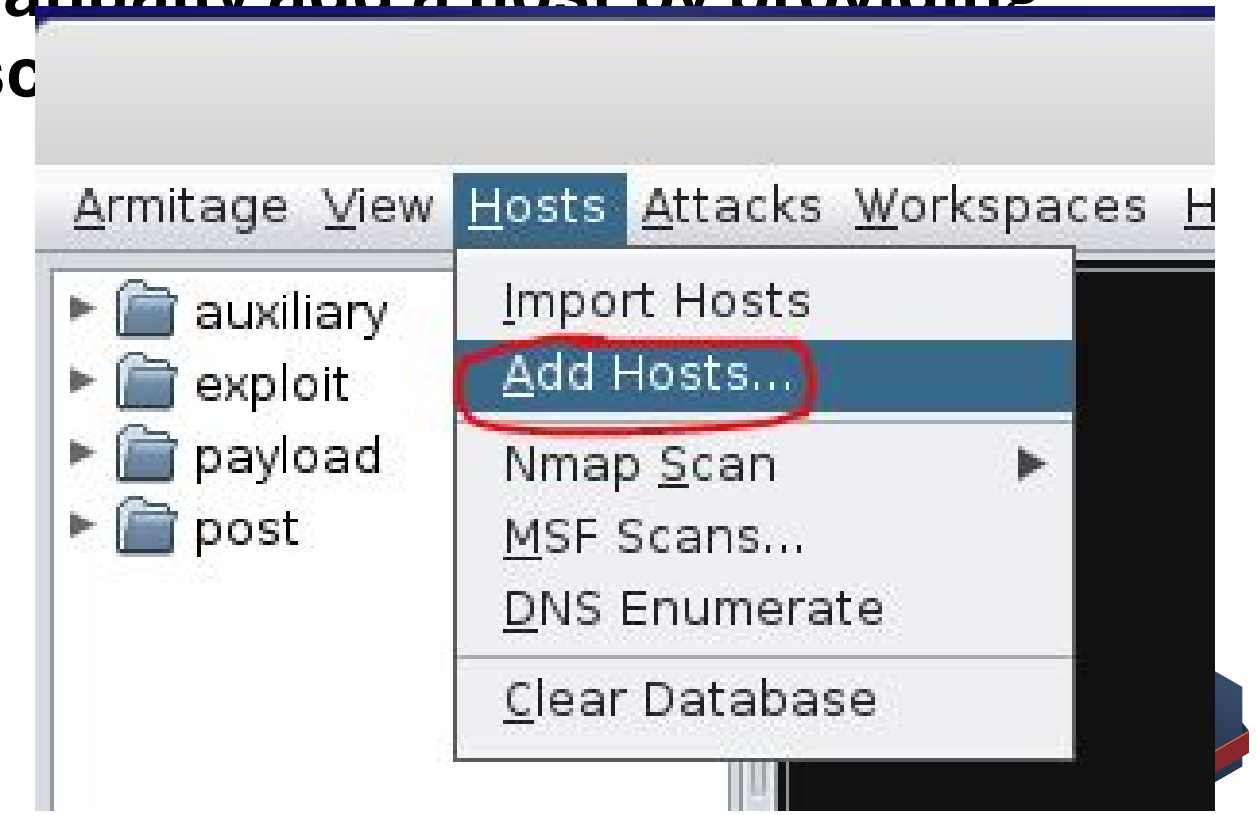
4. Armitage



Exploiting multiple targets with Armitage

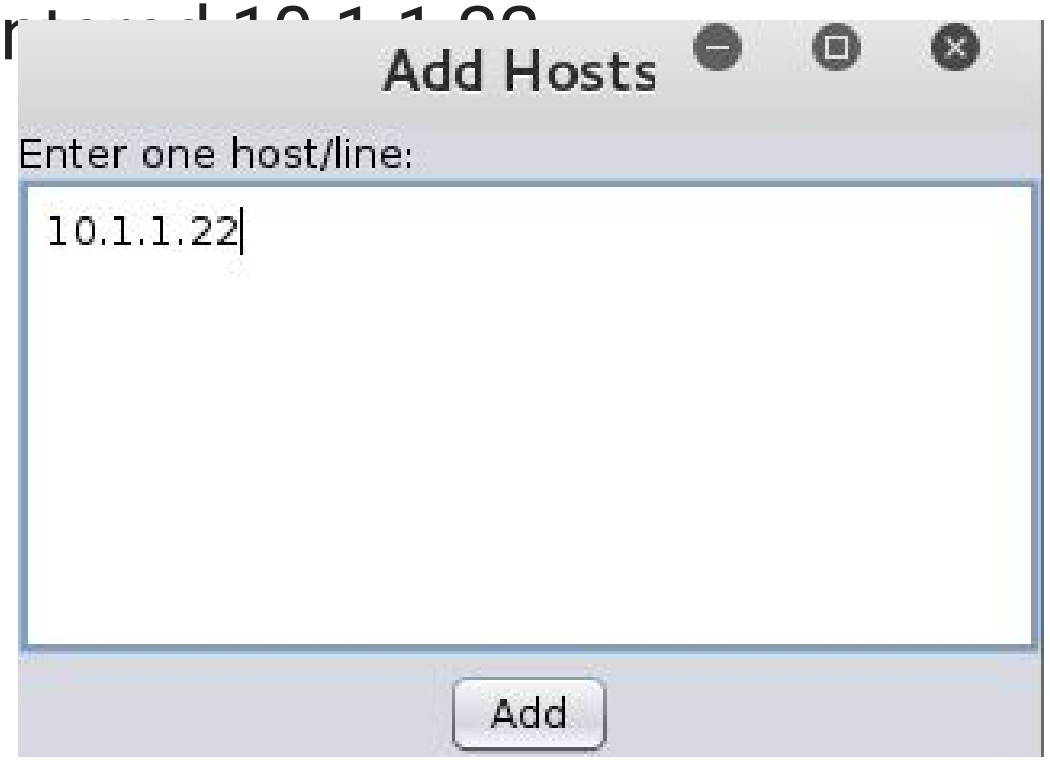
4. Choose the target (host or range of IP addresses) to attack:

- To discover available targets, **manually add a host by providing IP address** or select an **nmap sc** menu bar.
- Select “Add Hosts…”:



Exploiting multiple targets with Armitage

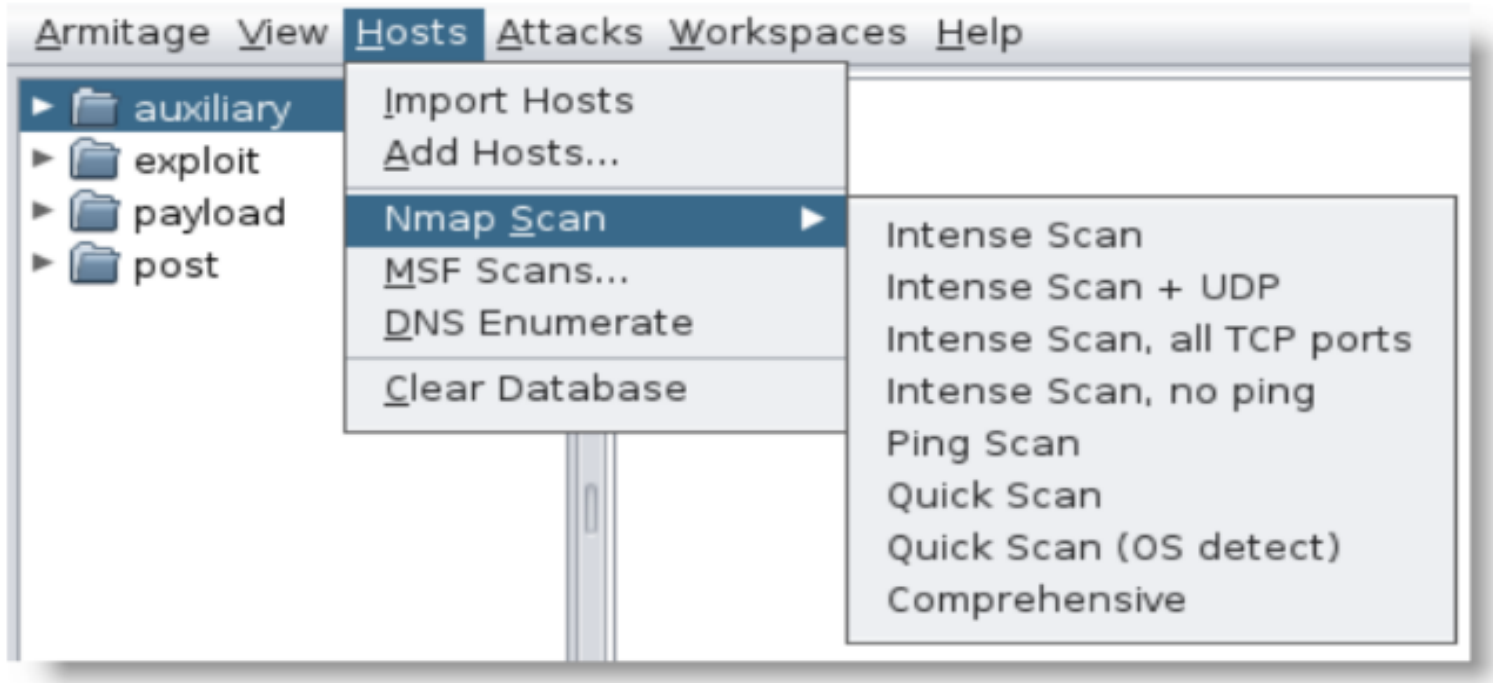
Enter the target (hosts) IP addresses, then click Add. In this example we en



Exploiting multiple targets with Armitage

- Armitage can also enumerate targets using MSF auxiliary commands

4. Nmap scan using Artii

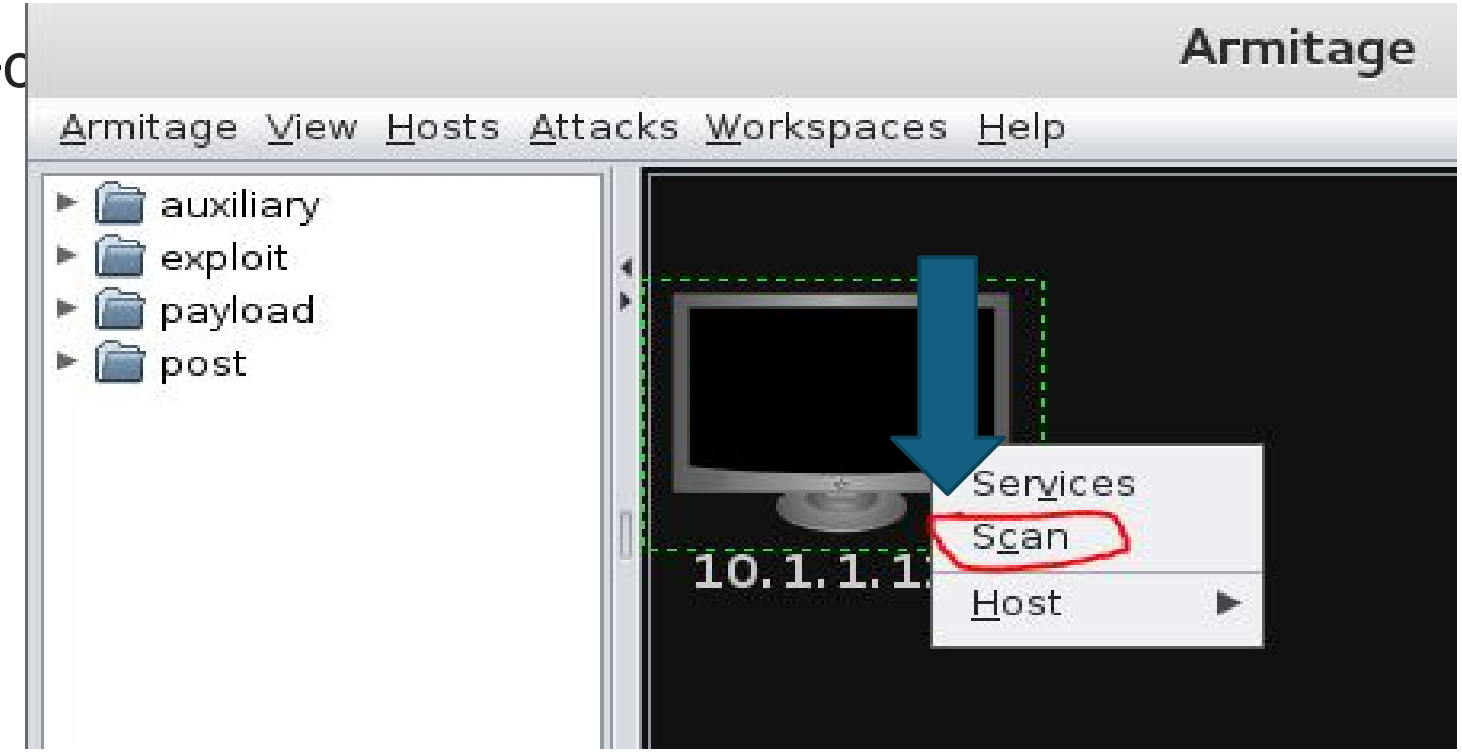


Once you have identified
can **select specific modu**

Exploiting multiple targets with Armitage

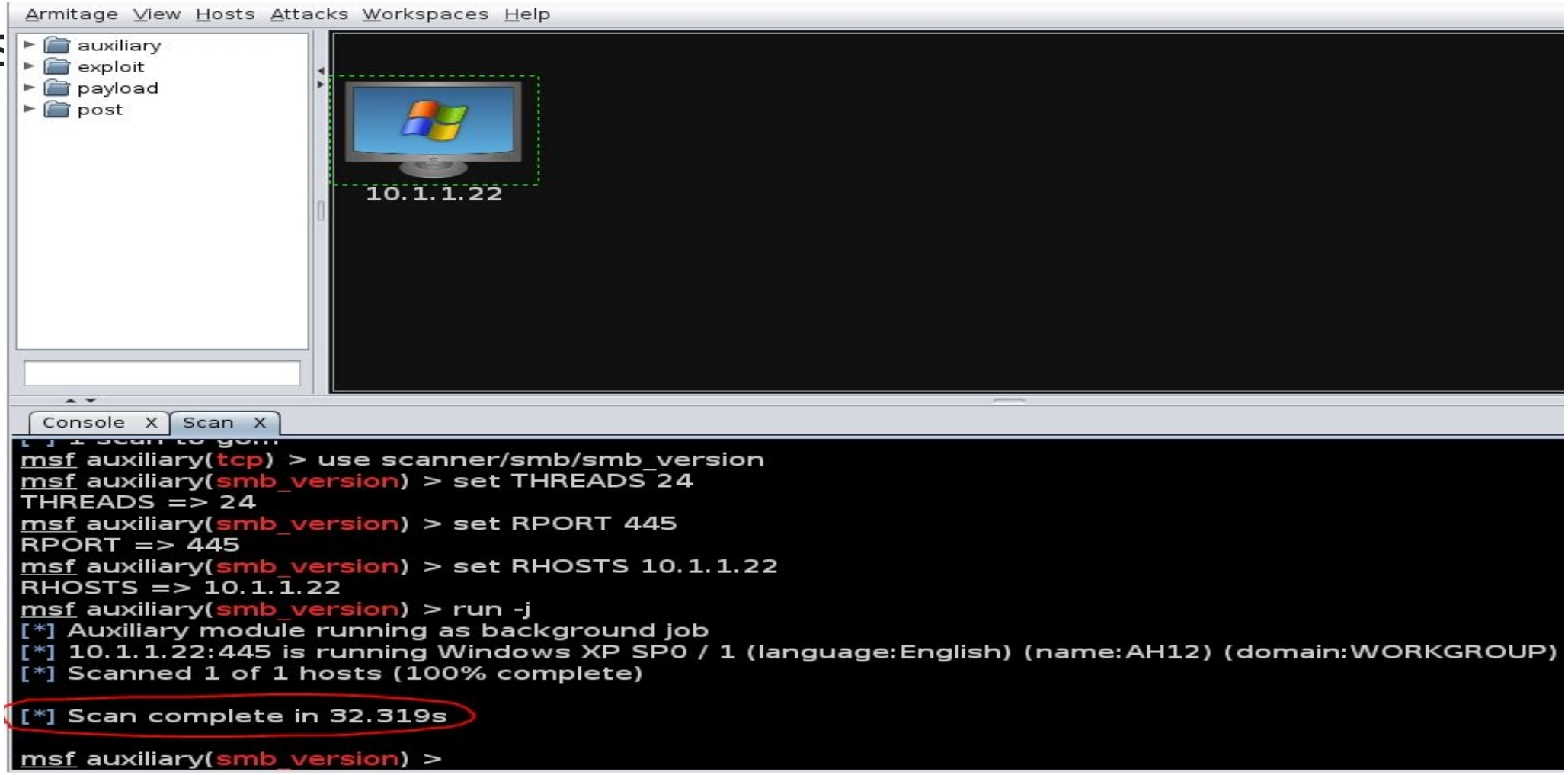
5. Scan the target(s) for open ports, services, operating system, etc.

- Right-c



Exploiting multiple targets with Armitage

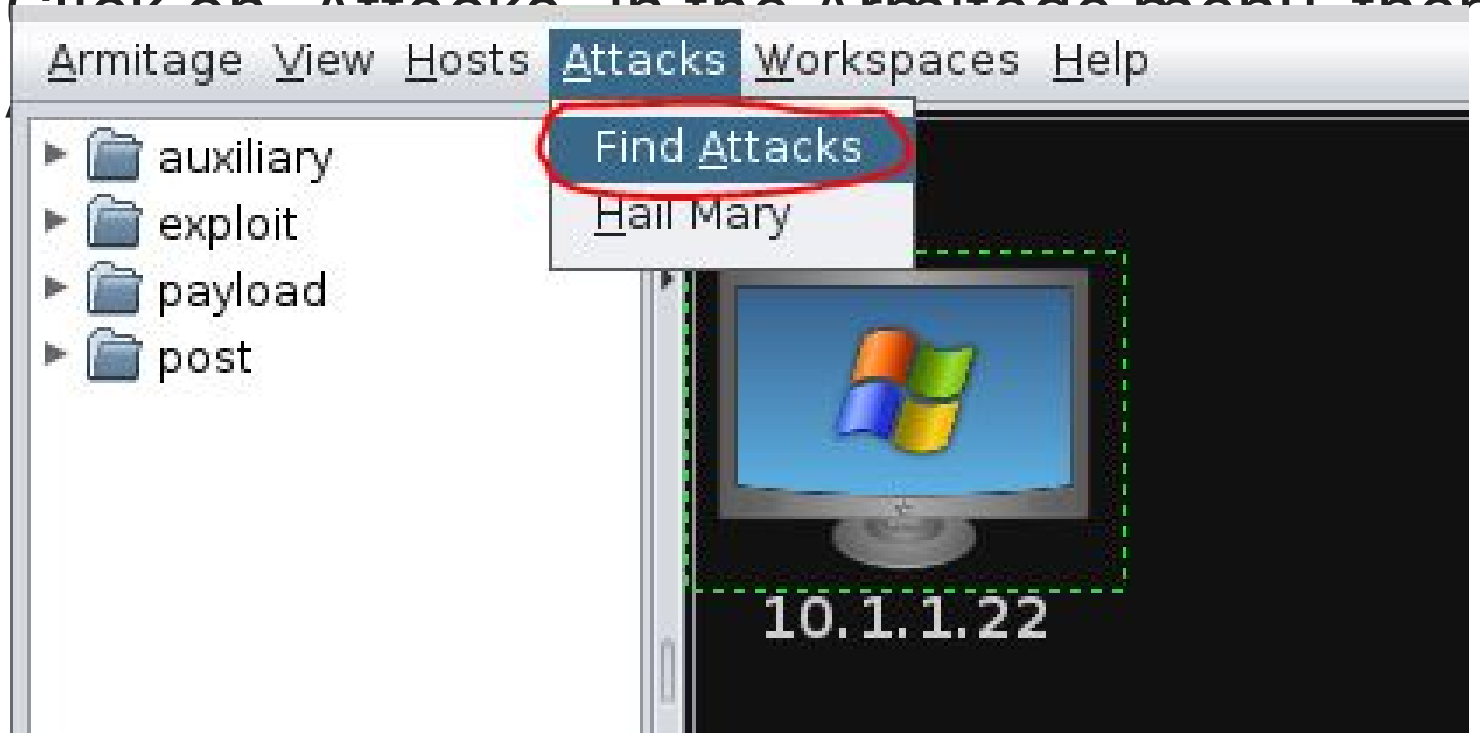
As
in



Exploiting multiple targets with Armitage

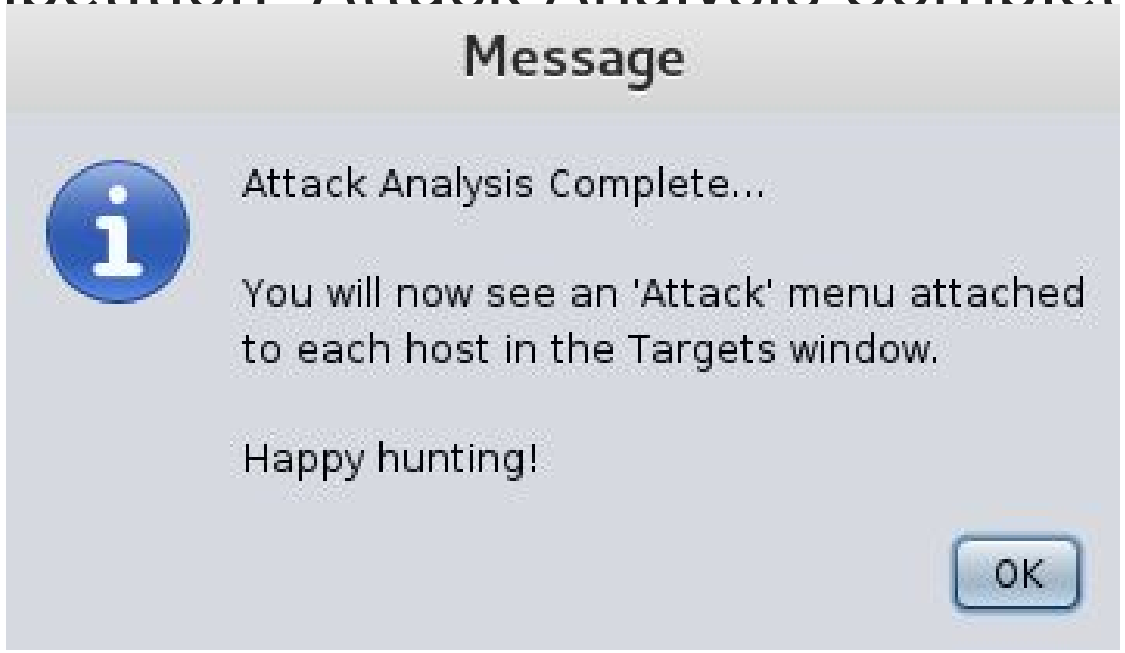
6. Find Exploits

- Click on “Attacks” in the Armitage menu, then select “Find



Exploiting multiple targets with Armitage

After competition “Attack Analysis Complete…” message:

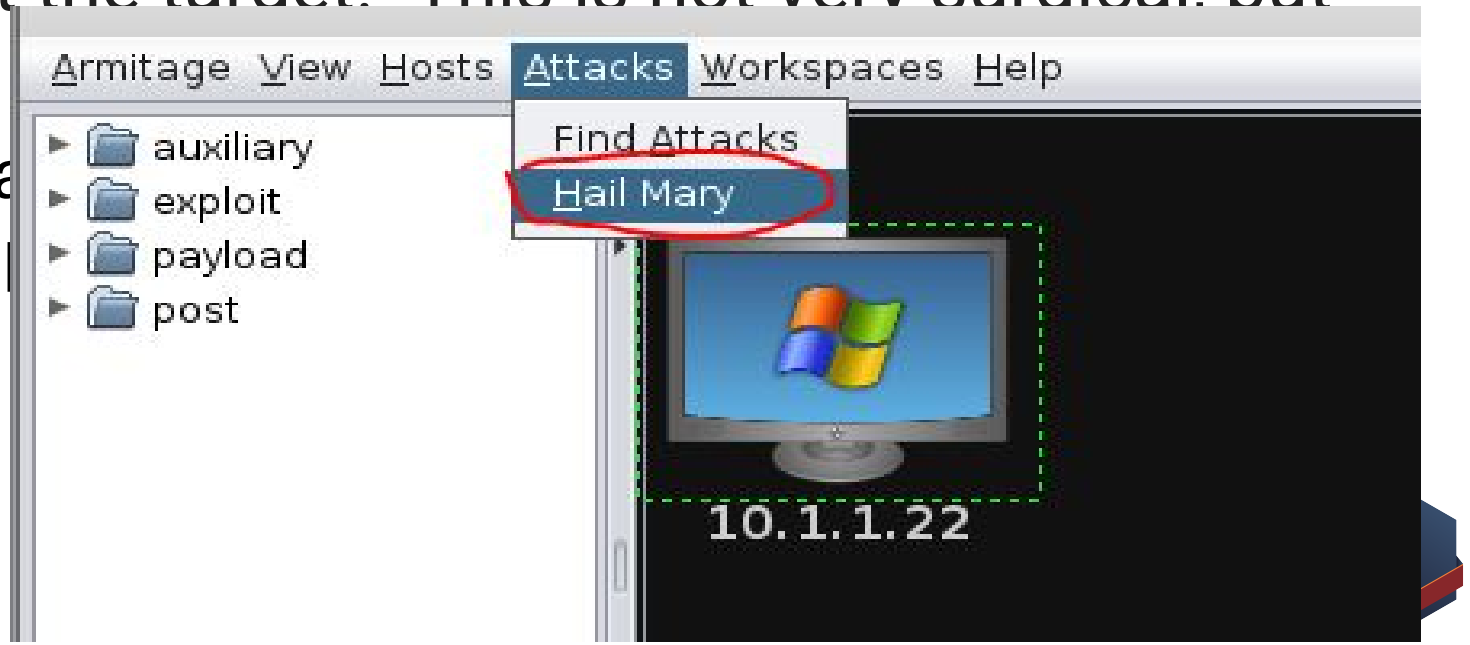


Exploiting multiple targets with Armitage

THE NORTHCAP UNIVERSITY

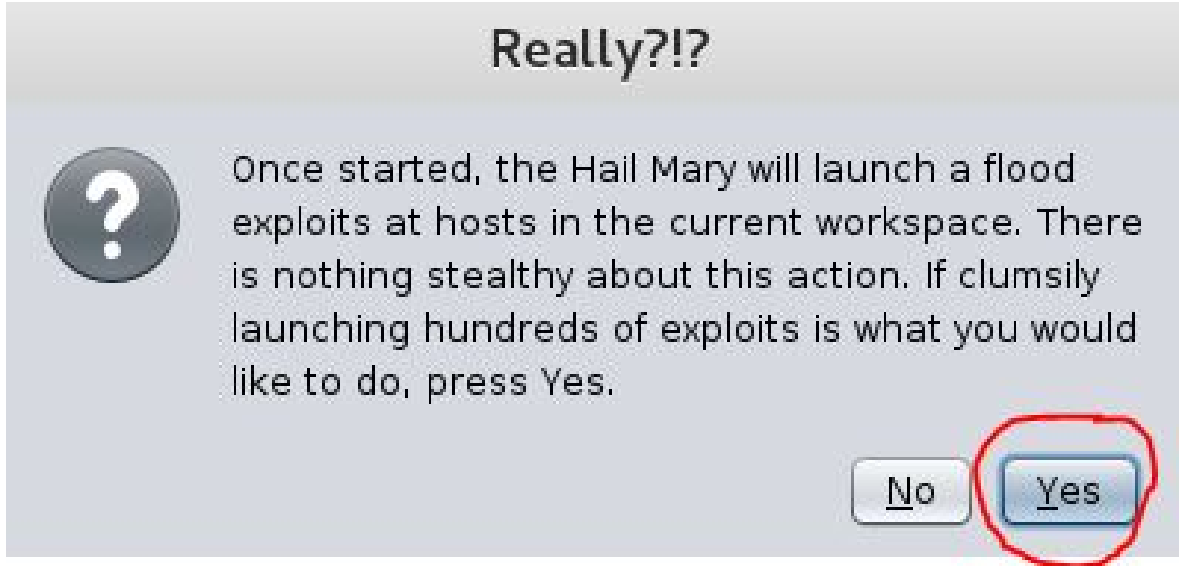
7. Launch Exploit(s)

- In this case, we'll do a "Hail Mary" attack. The Hail Mary is not very stealthy because it will try every attack that Armitage thinks may work against the target. This is not very surgical, but often effective.
- (make sure that the opera
this does not always hap



Exploiting multiple targets with Armitage

Click on “Yes” to the Armitage Really?!? warning.



Exploiting multiple targets with Armitage

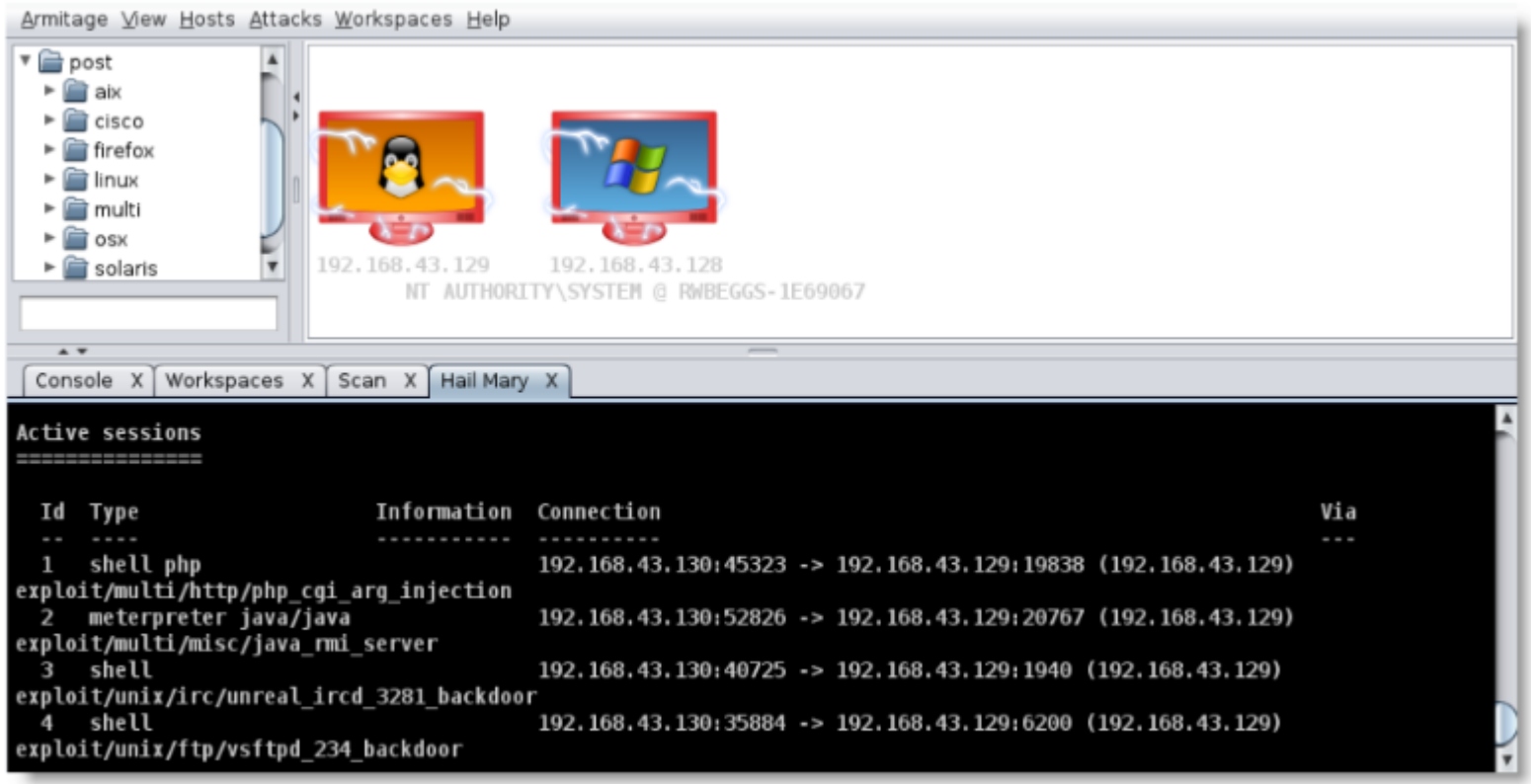
If one of the many attacks the Hail Mary tried works,

may get a Meterpreter session, represented graphically by the lightning looking hands around the red target:

Exploiting multiple targets with Armitage

THE NORTHCAP UNIVERSITY

For Multiple targets: A system that is compromised shows up as an icon w

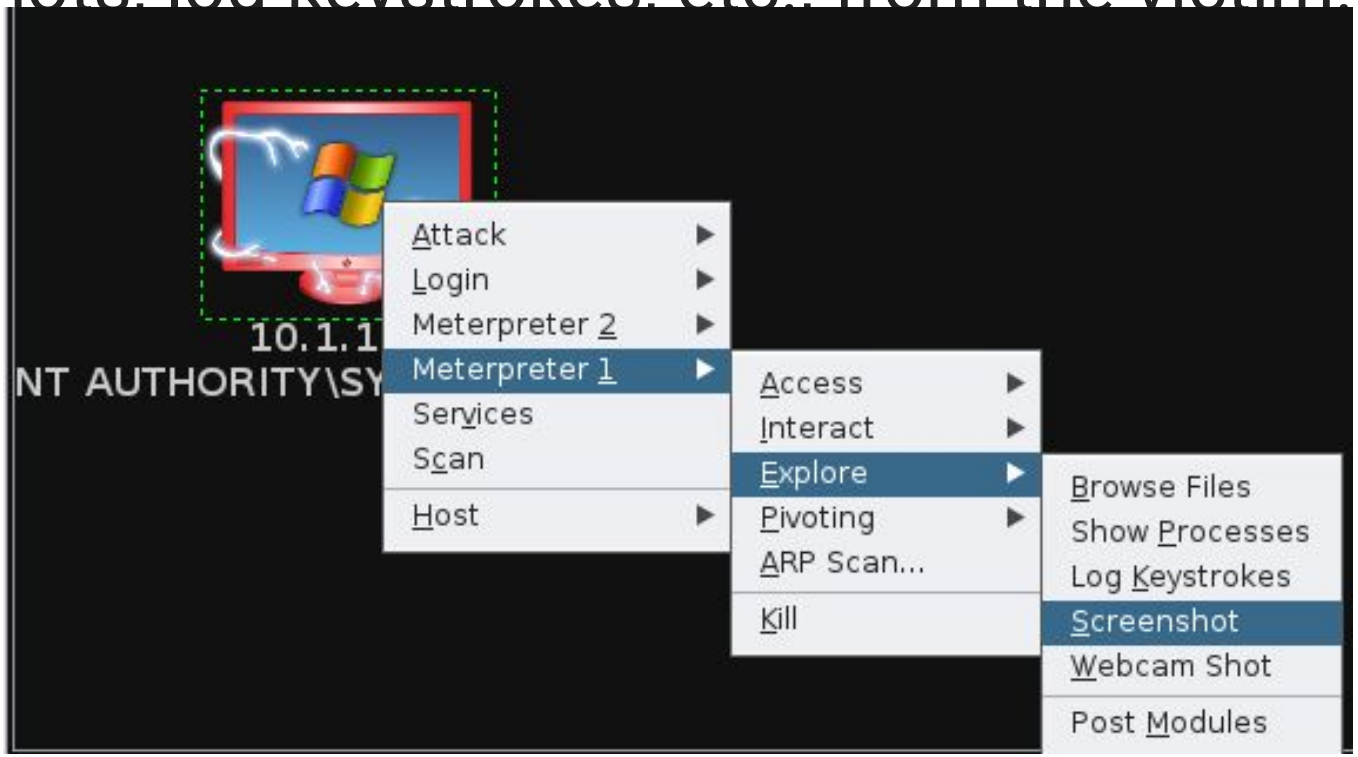


YEARS OF EXCELLENCE

NAAC Accredited

Exploiting multiple targets with Armitage

Play around with the Meterpreter shell to dump hashes, take screenshots, log keystrokes, etc., from the victim:



- https://alpinesecurity.com/blog/7-steps-to-hack-a-target-with-virtually-no-experience/