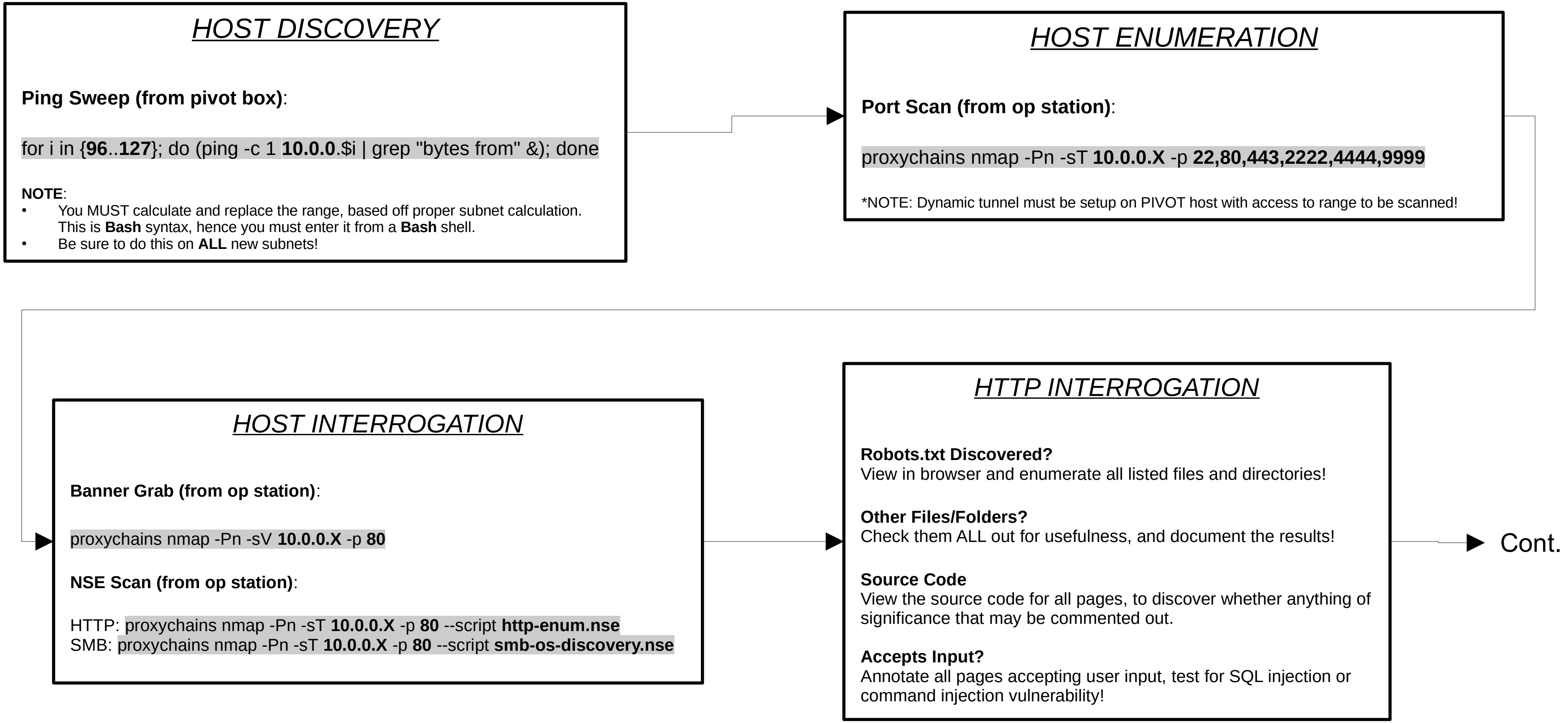
OPS METHODOLOGY QUICK REFERENCE



HOST DISCOVERY

Ping Sweep (from pivot box):

```
for i in {96..127}; do (ping -c 1 10.0.0.$i | grep "bytes from" &); done
```

NOTE:

- You MUST calculate and replace the range, based off proper subnet calculation. This is **Bash** syntax, hence you must enter it from a **Bash** shell.
- Be sure to do this on **ALL** new subnets!

HOST ENUMERATION

Port Scan (from op station):

```
proxychains nmap -Pn -sT 10.0.0.X -p 22,80,443,2222,4444,9999
```

*NOTE: Dynamic tunnel must be setup on PIVOT host with access to range to be scanned!

HOST INTERROGATION

Banner Grab (from op station):

```
proxychains nmap -Pn -sV 10.0.0.X -p 80
```

NSE Scan (from op station):

```
HTTP: proxychains nmap -Pn -sT 10.0.0.X -p 80 --script http-enum.nse
SMB: proxychains nmap -Pn -sT 10.0.0.X -p 80 --script smb-os-discovery.nse
```

HTTP INTERROGATION

Robots.txt Discovered?
View in browser and enumerate all listed files and directories!

Other Files/Folders?
Check them ALL out for usefulness, and document the results!

Source Code
View the source code for all pages, to discover whether anything of significance that may be commented out.

Accepts Input?
Annotate all pages accepting user input, test for SQL injection or command injection vulnerability!

Cont.