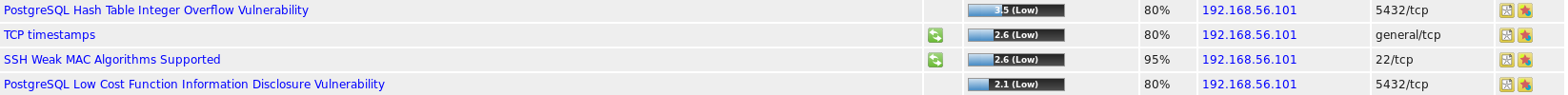
COSC382 Assignment

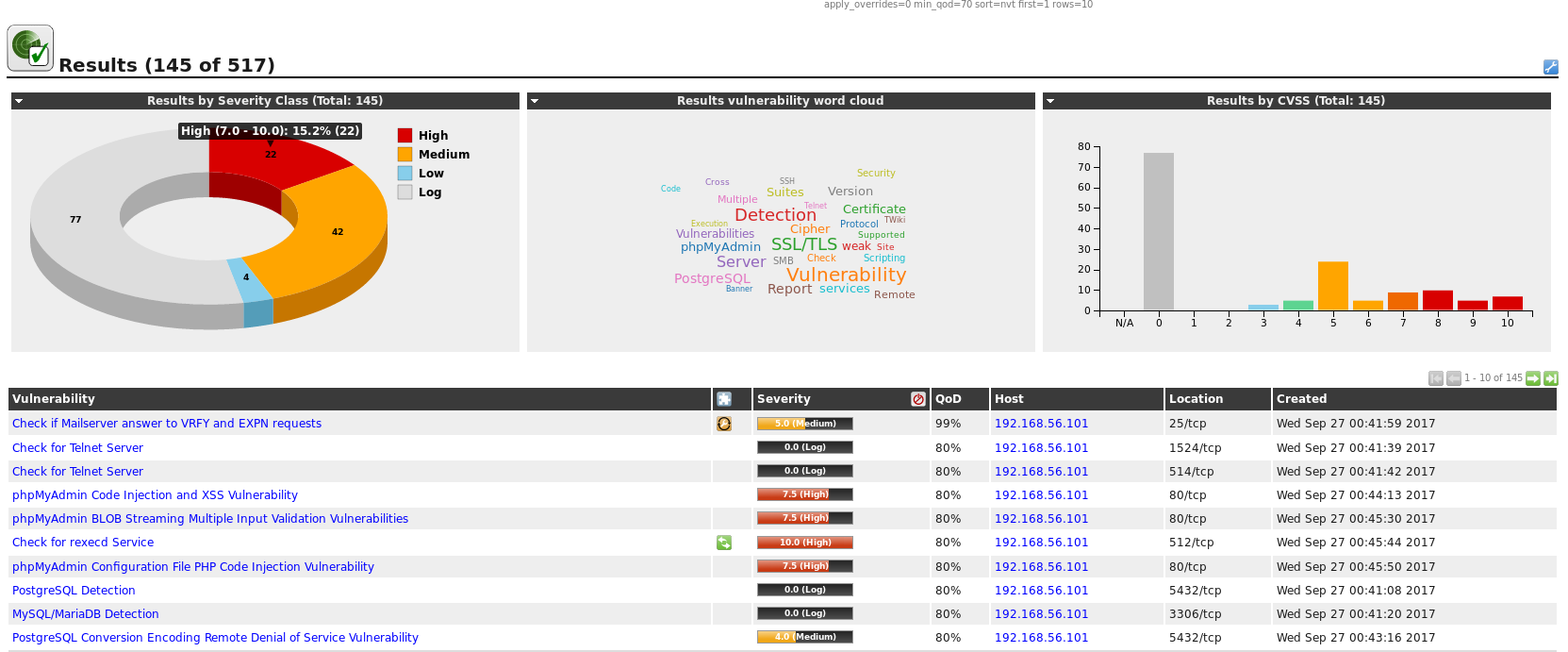
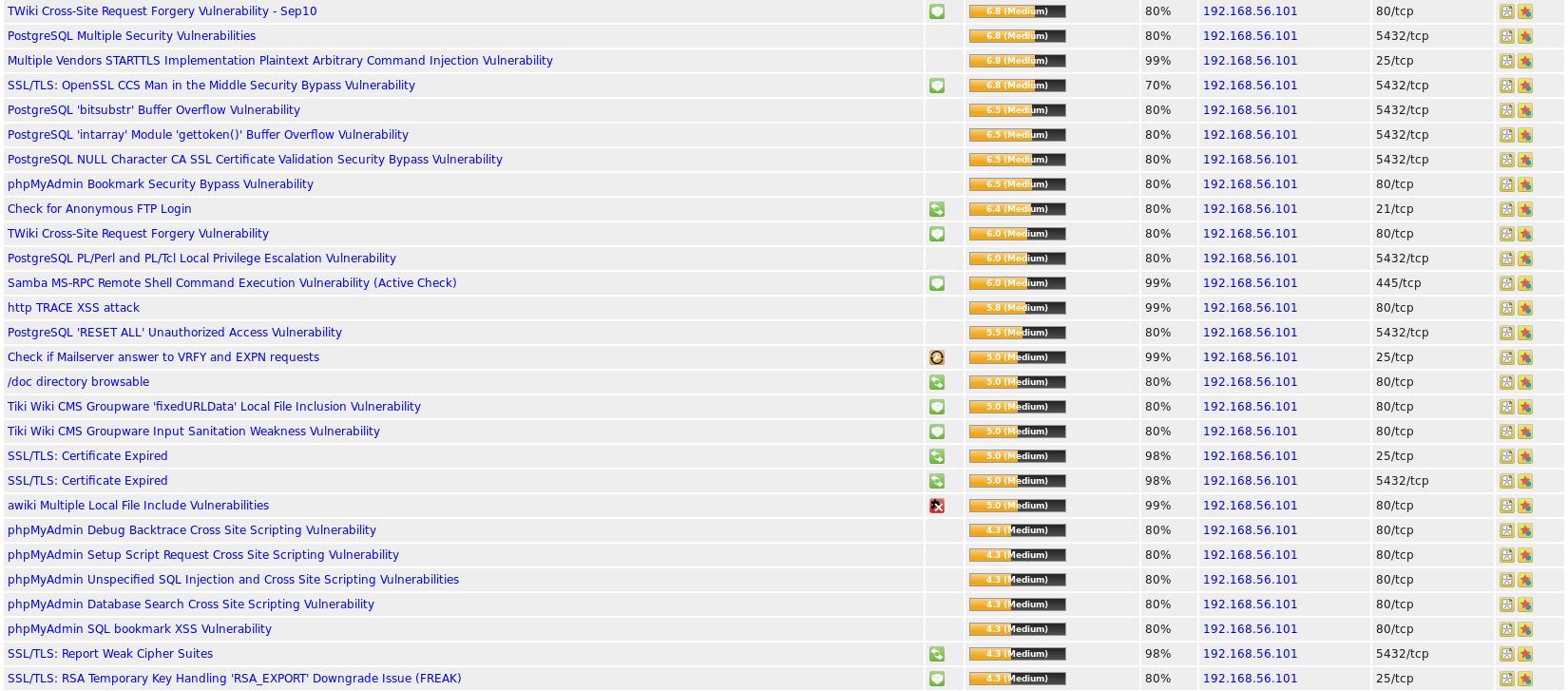
3.1: Vulnerability Scanning

3.1.1: Use OpenVAS for Vulnerability Scanning

Full and Fast - Metasploitable  
  
  
Full Deep and Ultimate- Metasploitable



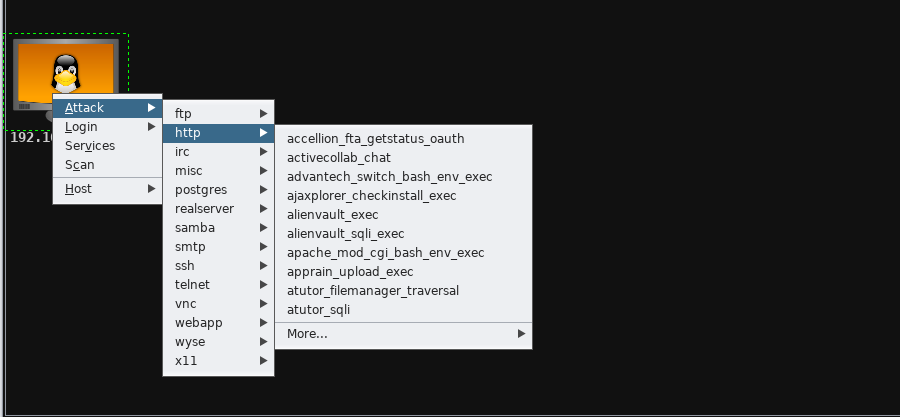


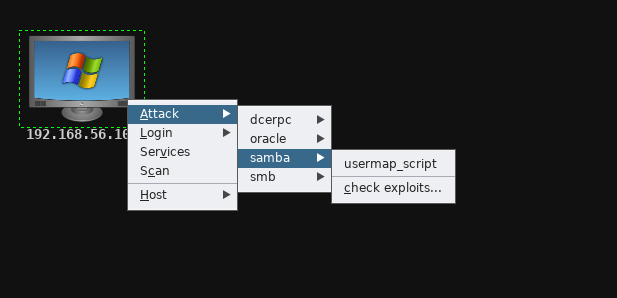
3.1.2: Use Nessus for Vulnerability Scanning

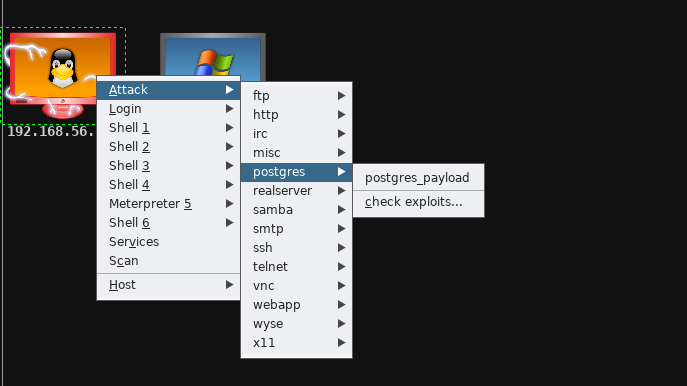
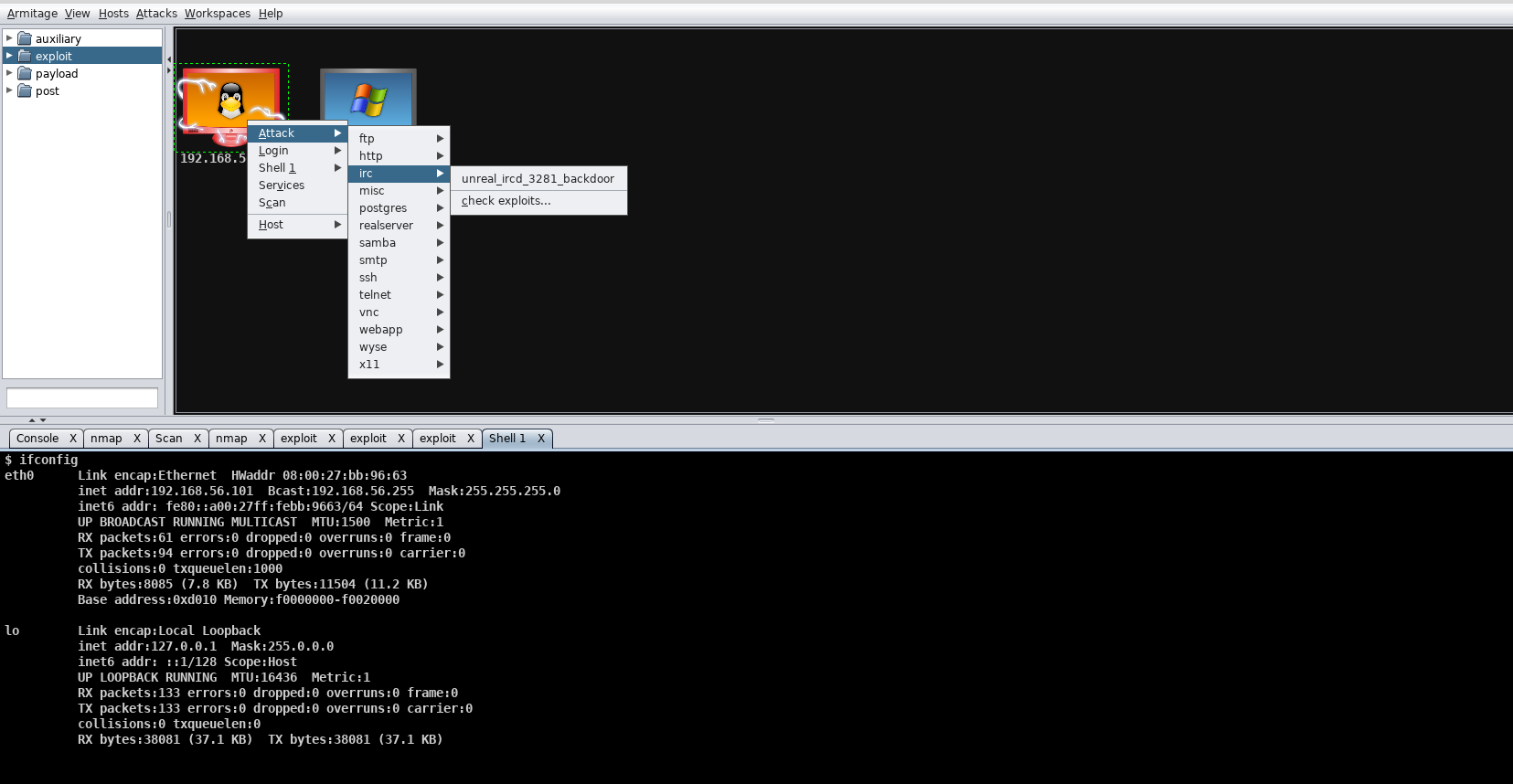
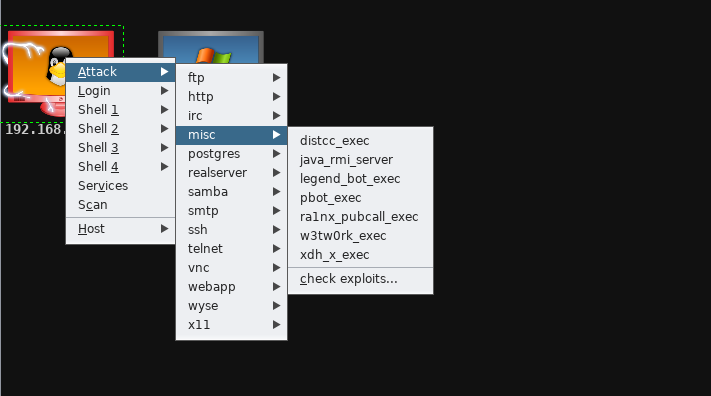
3.1.3: Compare OpenVAS and Nessus

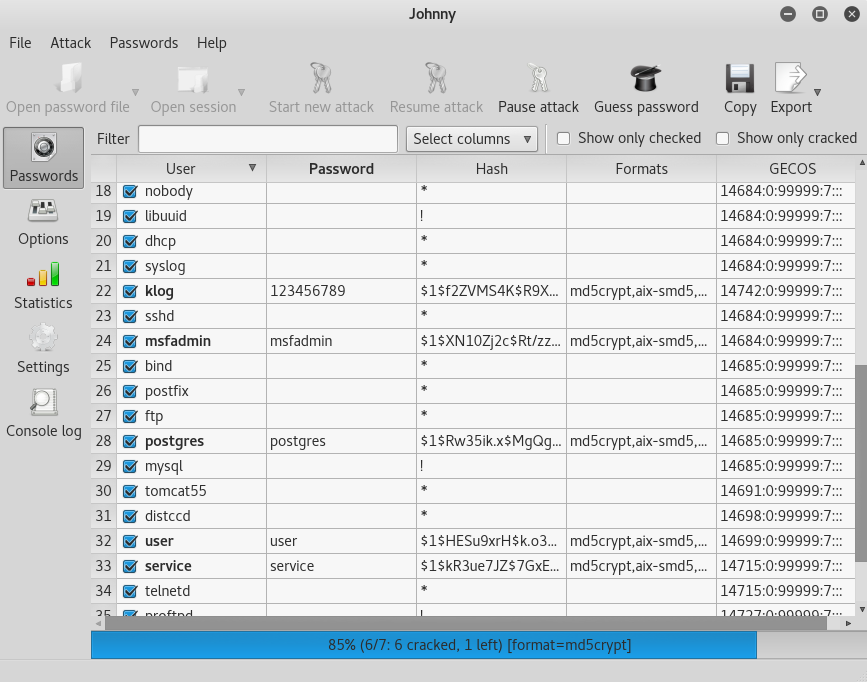
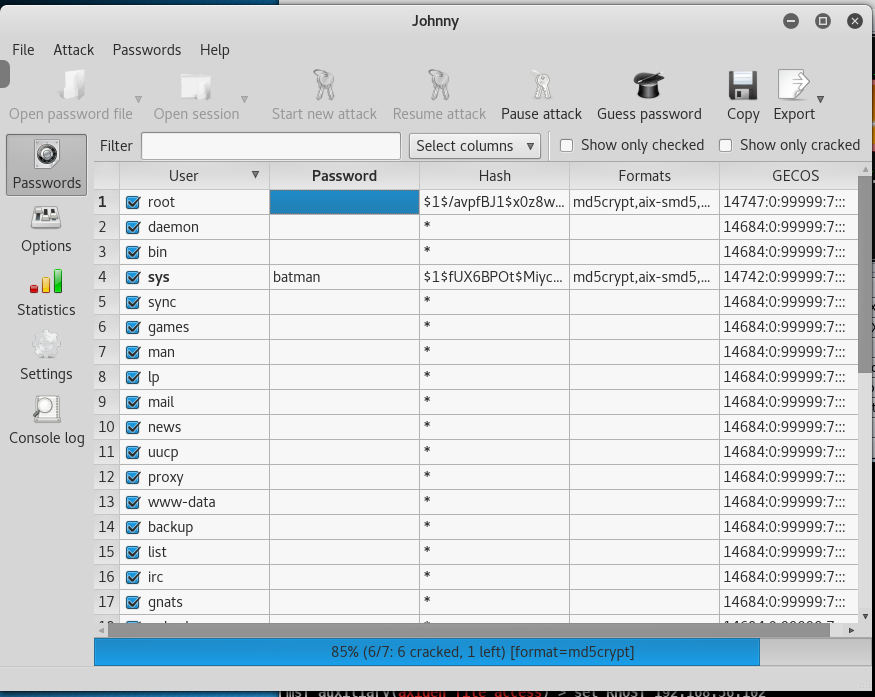
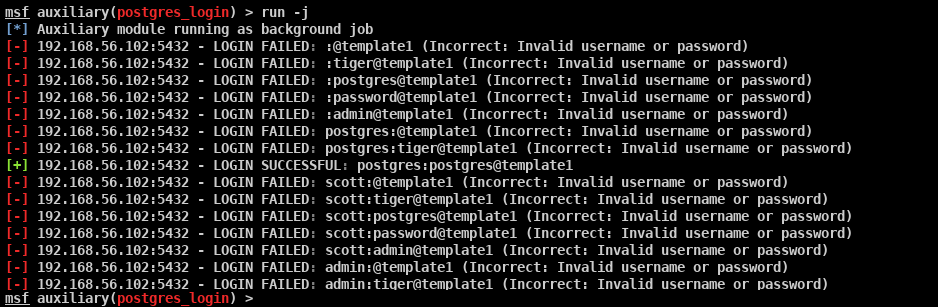
3.2: Exploitation and Exfiltration

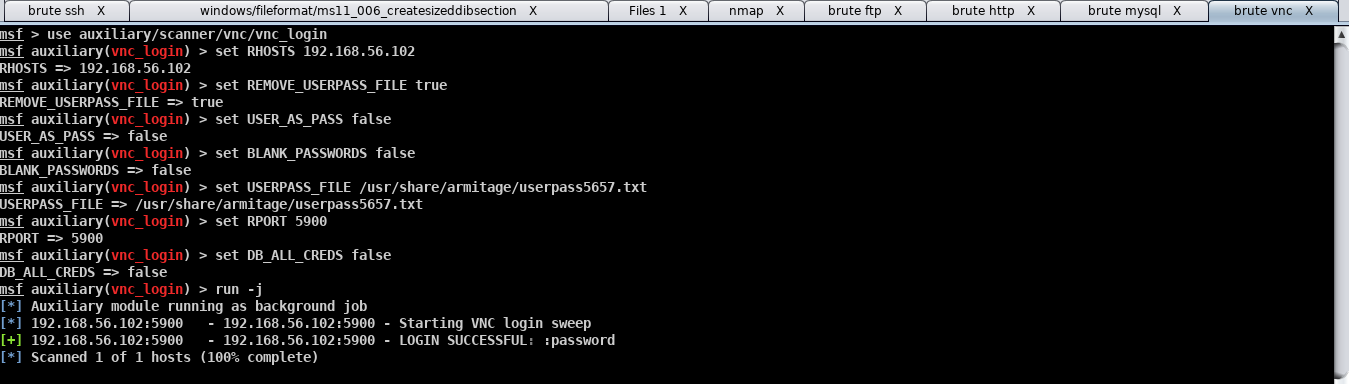
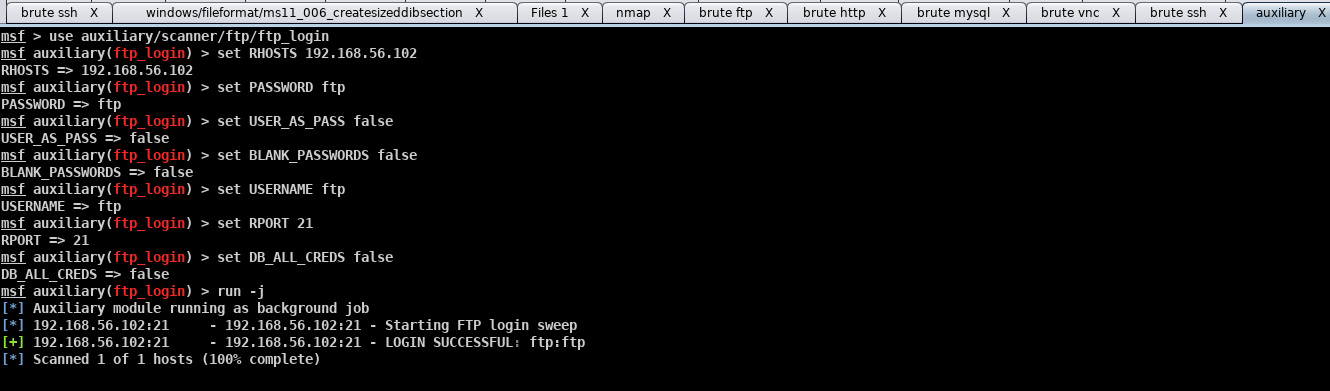
3.2.3: Exploiting Metasploitabl



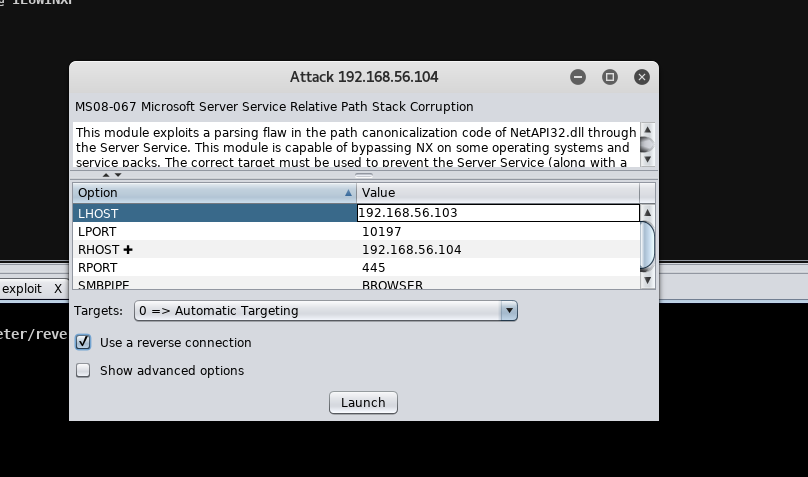


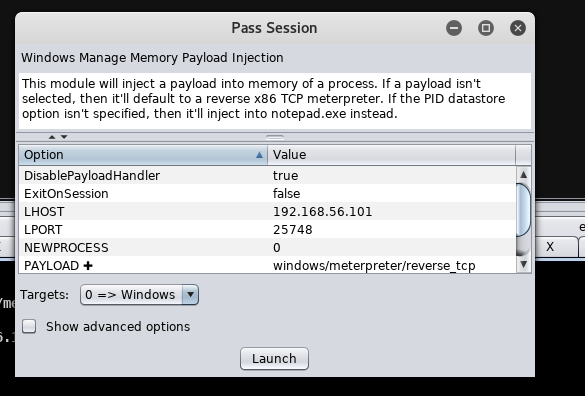
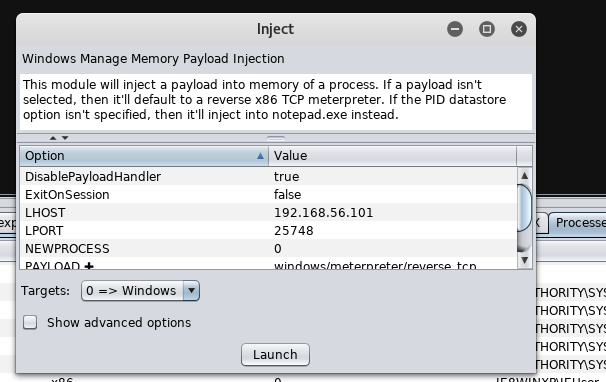


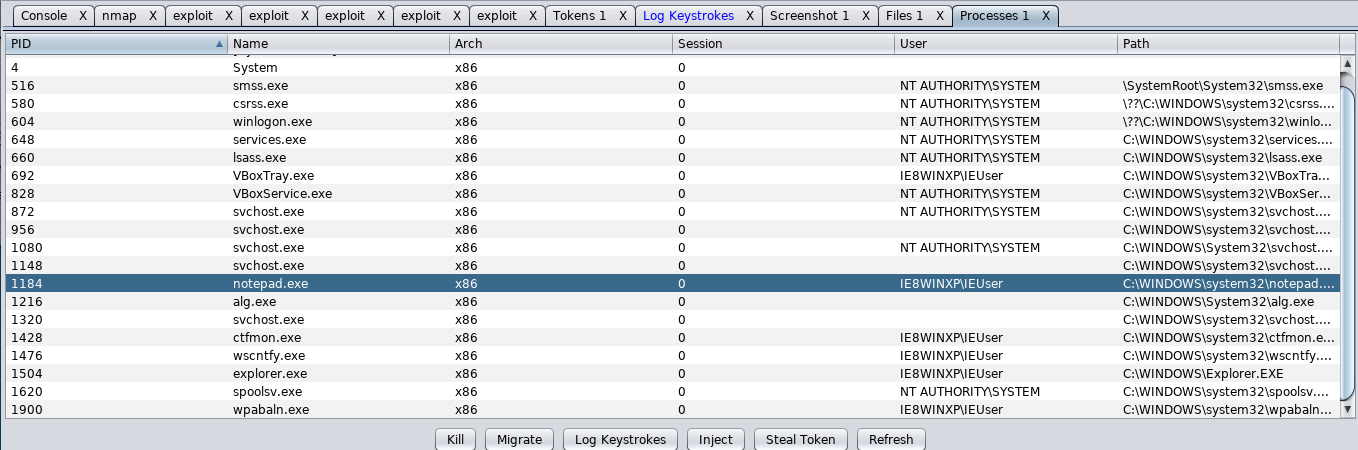
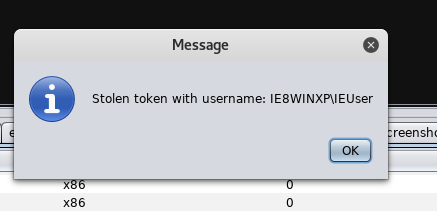
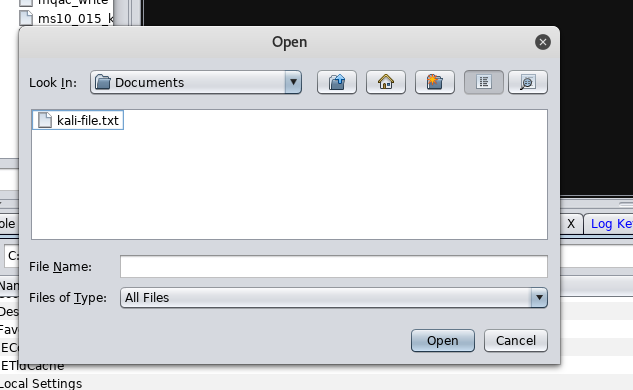
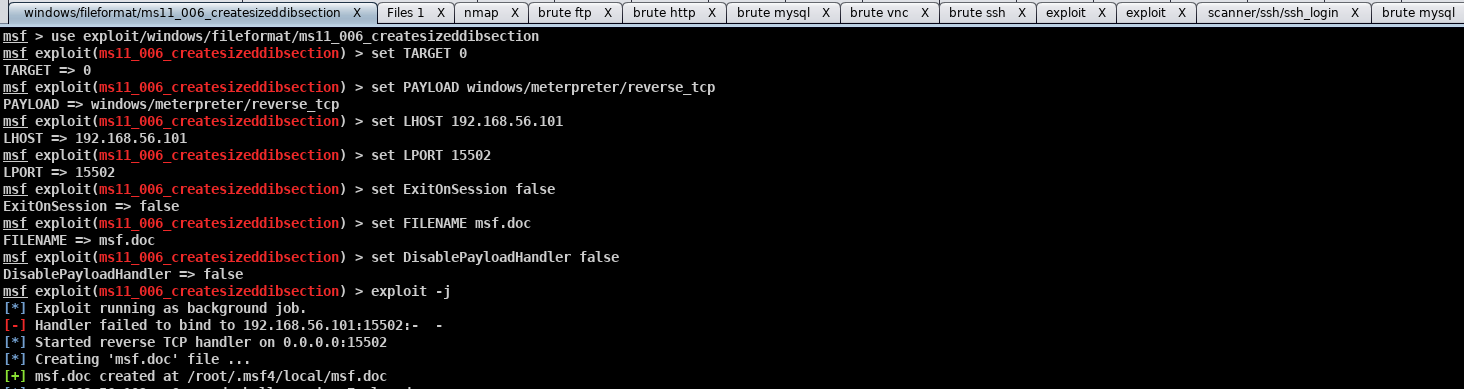
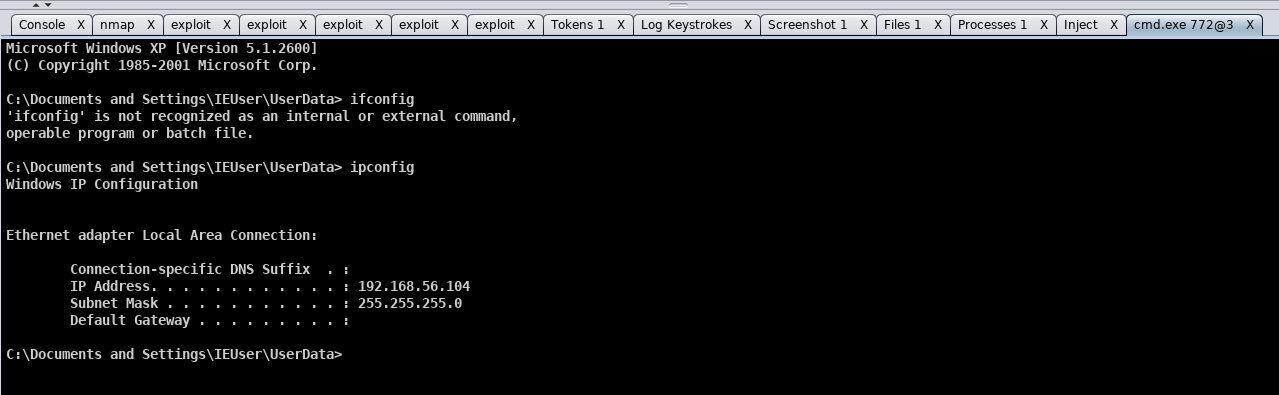
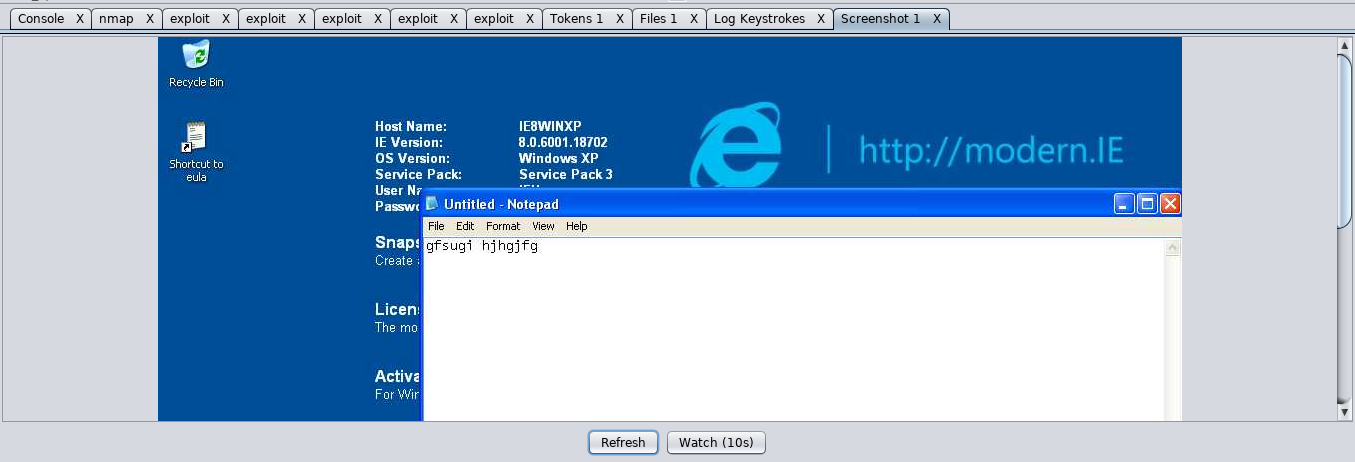
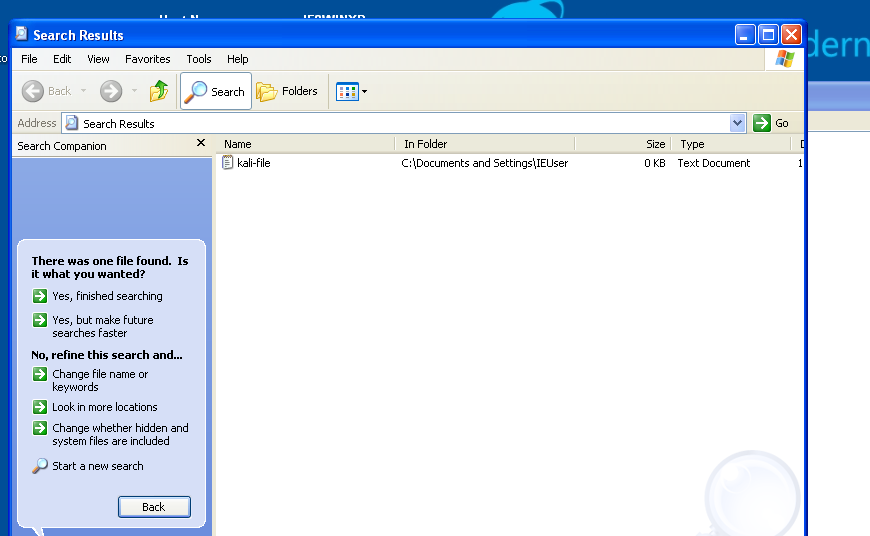
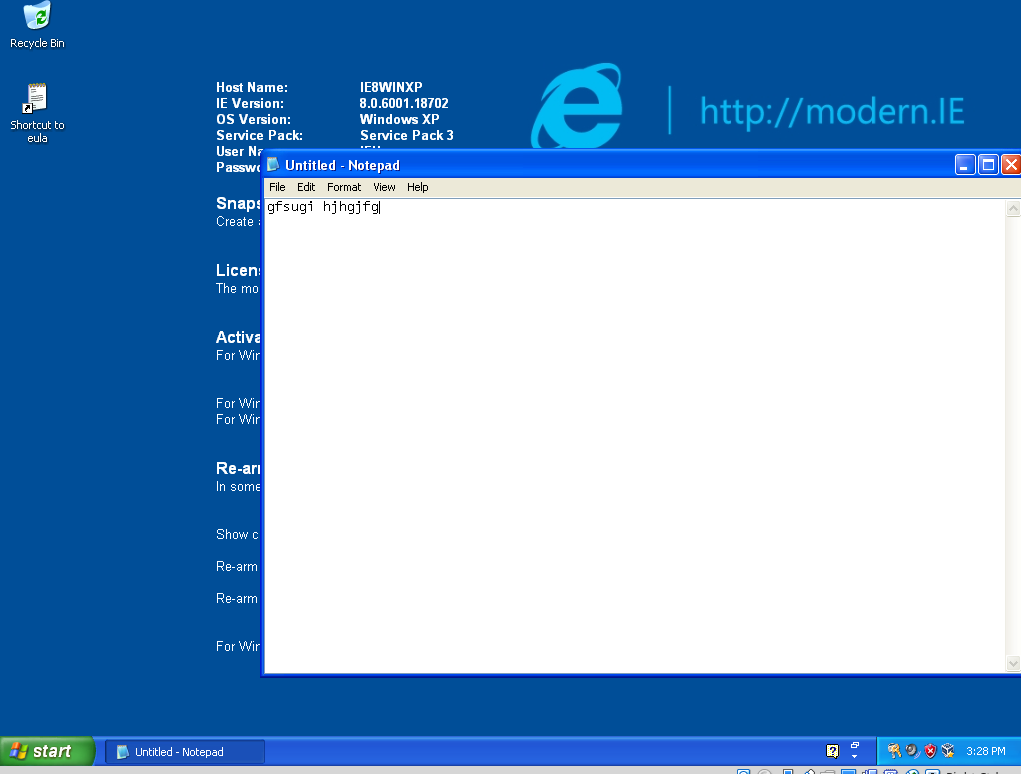
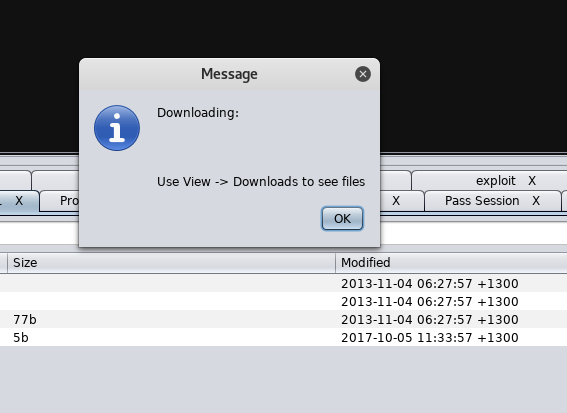
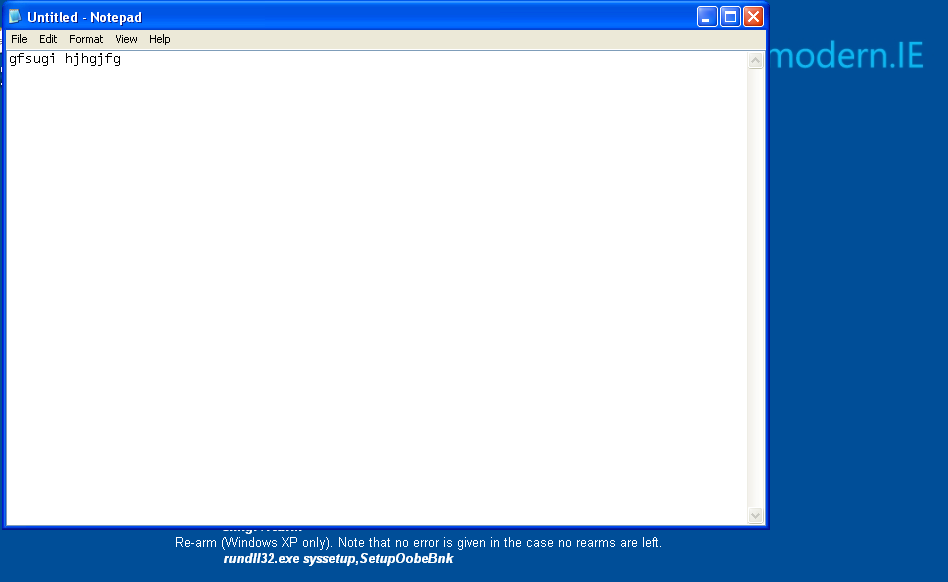
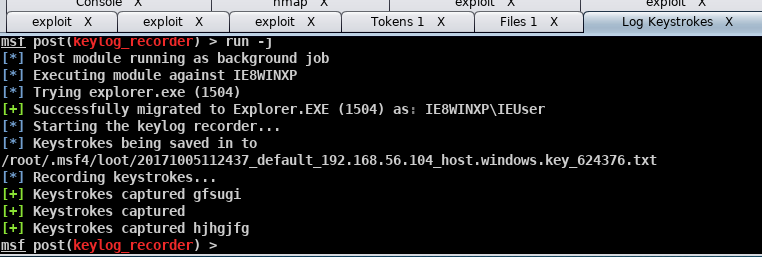
3.2.4: Harvesting Credentials from Metasploitable



3.2.5: Exploiting Vulnerabilities in Windows XP

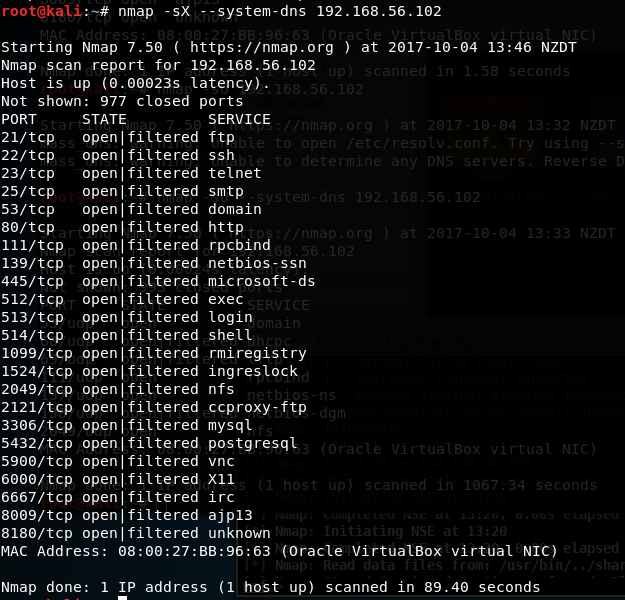
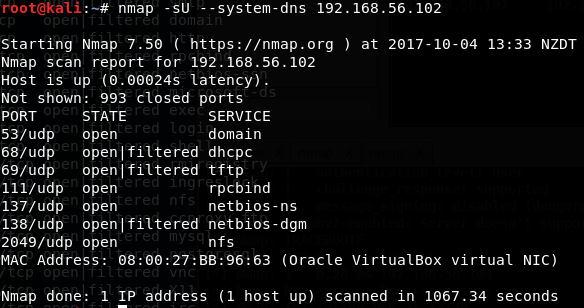
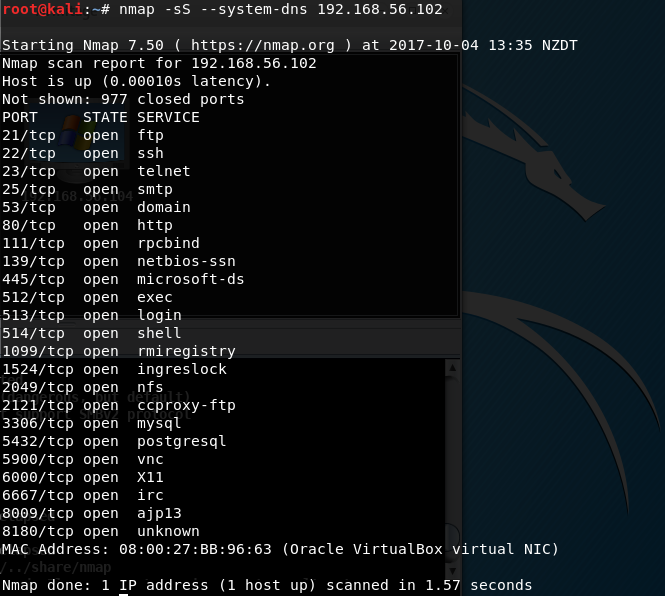
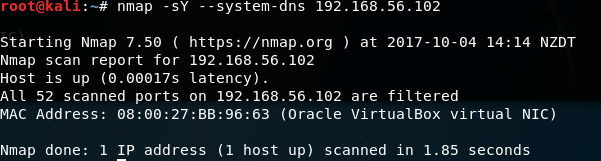
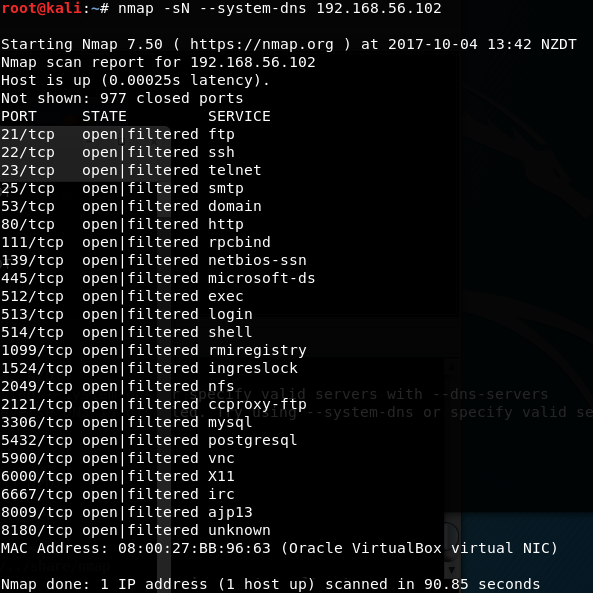
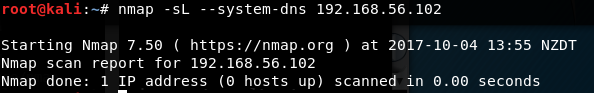
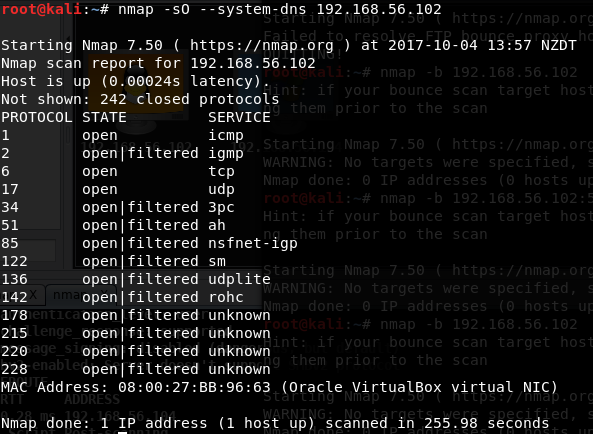
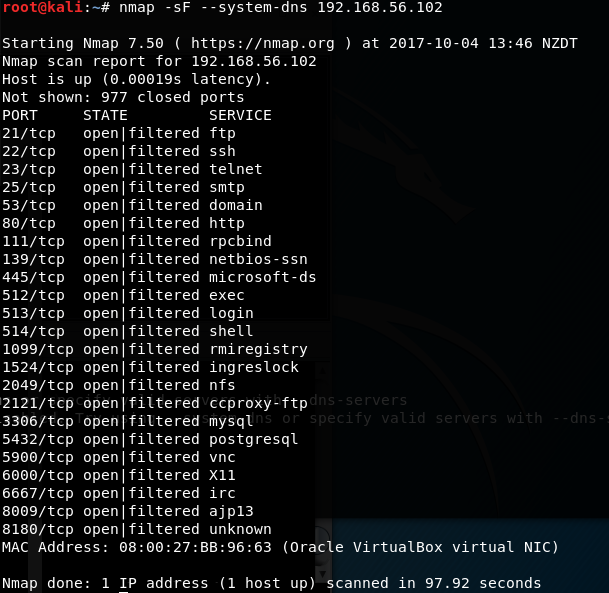




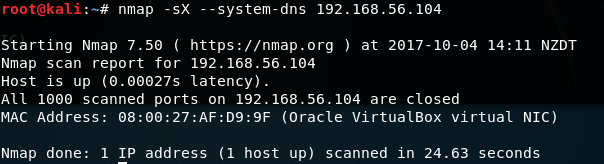
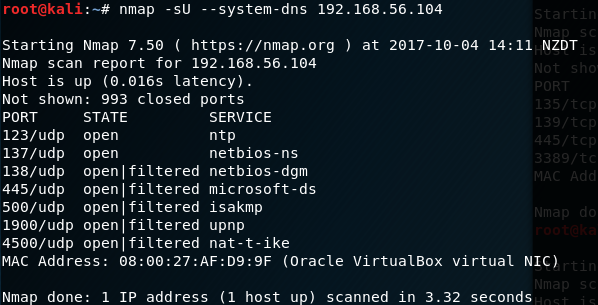
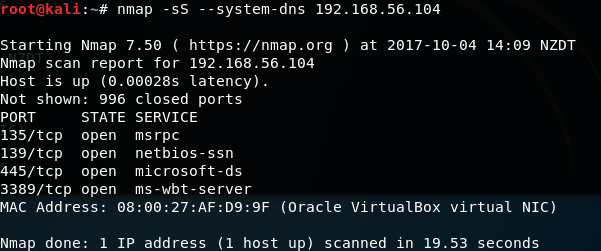
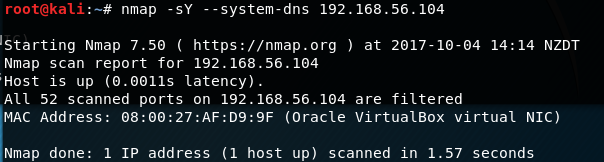
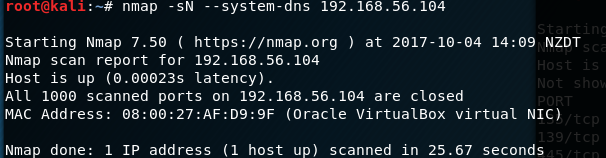
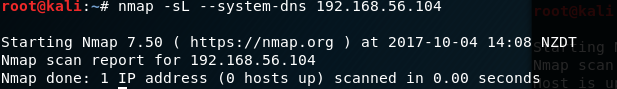
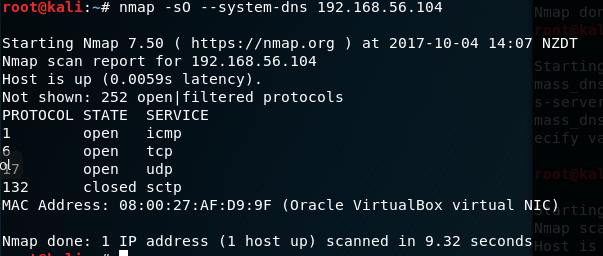
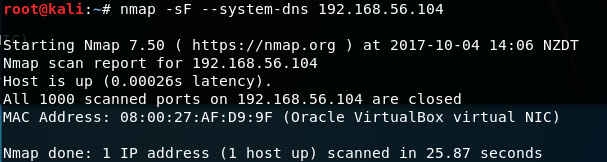
3.2.6: Exploring Post Exploitation Capabilities in Windows XP

3.3: Detection and Prevention

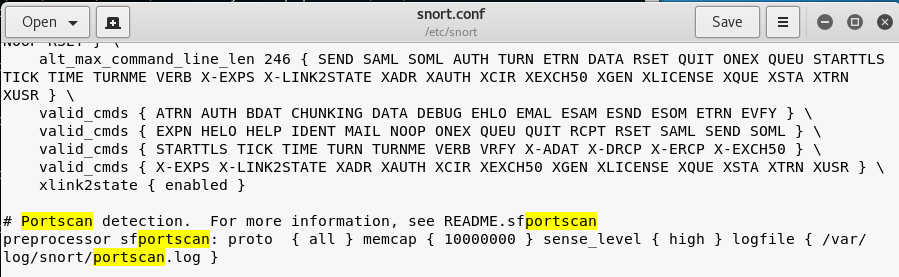
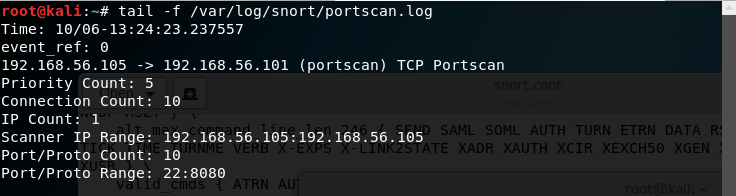
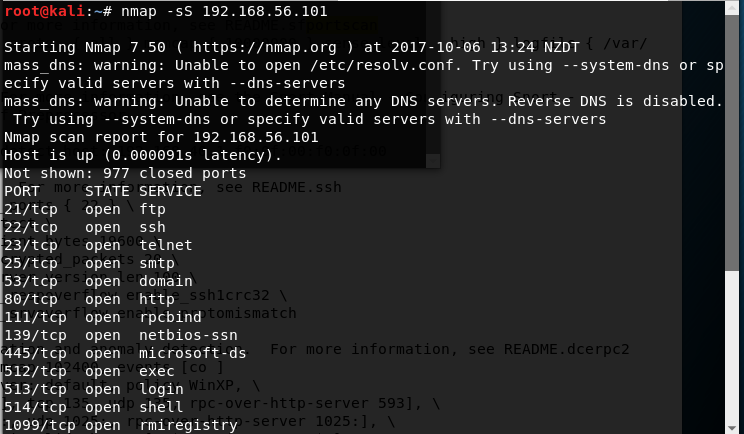
3.3.1: Perform a Port Scan with Nmap

Metasploitable  


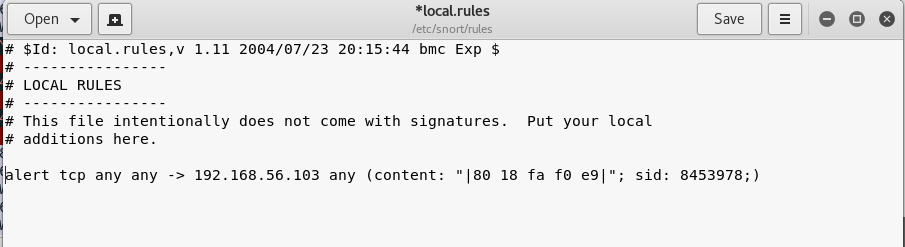
Windows



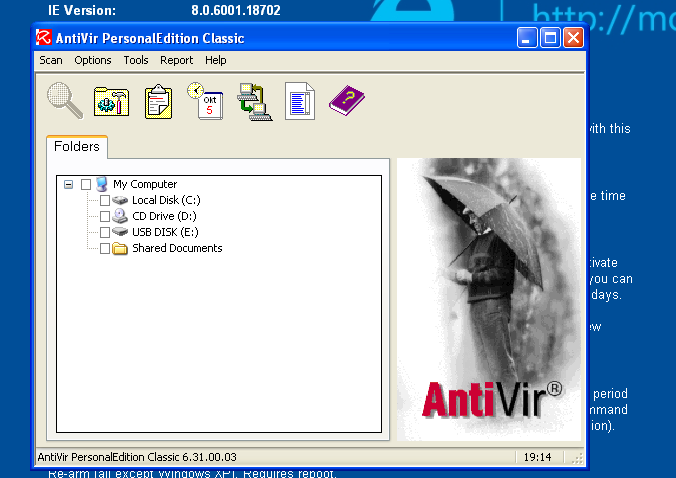
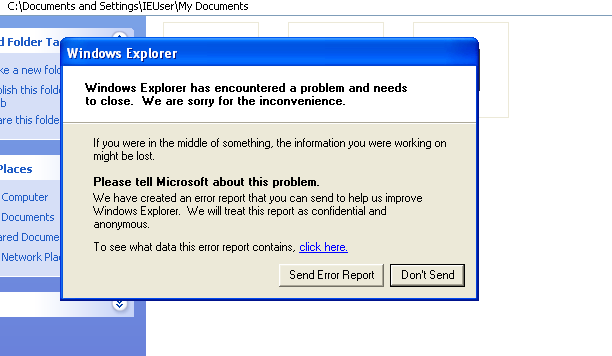
3.3.2: Mitigate Port Scanning with Snort



3.3.3: Mitigate Exploitation with Snort



3.3.4: Installing Host Based Protections



3.3.5: Discuss the Pros and Cons of Snort

Discuss Other Countermeasures and Mitigations

Launch all attacks

