Afeefah Manzoor

ITN 277: Forensics 2

Network Forensics Homework

* The infected computer's host name

Leonardo-PC

* The infected computer's MAC address

80:c1:6e:6a:0b:f2

* The infected computer's operating system and browser

OS: Windows 7

Browser: Internet Explorer 11

* Exploit kit (Angler, Magnitude, or Nuclear?)

Angler Exploit kit

* IP address and domain name used by the exploit kit

IP:185.43.223.164

Domain name: kiralya.arcadiumentertainment.com

* Compromised website that caused the exploit kit traffic

Twentyone-development.com

* Domains and IP addresses from the CryptoWall 3.0 post-infection traffic

188.165.164.184 ip-addr.es

198.211.120.49 biganddigital.com

85.204.50.99 bibubracelets.ro

50.87.150.75 ehsansurgical.com

77.67.21.209 cnet-vh.akamaihd.net

* What was vulnerable one the user's computer (the browser, Flash, Java, Silverlight, etc.)?

Flash 18.0.0.203























