1. Fuzz侧重于RRQ 和 WRQ的Fuzz
2. 漏洞类型

|  |  |  |
| --- | --- | --- |
| Buffer Overflow | Fuzzed | Software |
| <http://www.exploit-db.com/exploits/18345/> | Yes | TFTP Server 1.4 ST |
| <http://www.exploit-db.com/exploits/17618/> | No | CiscoKits 1.0 TFTP Server |
| <http://www.exploit-db.com/exploits/18188/> |  | HillStone Software HS TFTP Server |
| <http://www.exploit-db.com/exploits/16350/> | Yes | Allied Telesyn AT-TFTP Server 1.9 |
| <http://www.exploit-db.com/exploits/3388/> |  | 3Com tftp Service < 2.0.1 |

|  |  |  |
| --- | --- | --- |
| Directory Tranverse | Fuzzed | Software |
| <http://www.exploit-db.com/exploits/18866/>  <http://www.exploit-db.com/exploits/18718/> |  | Distinct TFTP 3.01 |
| <http://www.exploit-db.com/exploits/18189/> |  | Ipswitch tftp server |
| <http://www.exploit-db.com/exploits/17619/> |  | CiscoKits 1.0 TFTP Server |
| <http://www.exploit-db.com/exploits/17507/> |  | Avaya IP Office Manager TFTP Server |

Buffer Overflow集中于超长的filename 还有超长的mode。超长filename占主导。Directory Tranverse怎样才算不误报？