Overview

- Reconnaissance & Enumeration
  - Concepts, Examples, Motivations
- Hands-on Cyber Attacks
  - Concept
  - Establishing a Baseline
  - Demonstration of the Attack
  - Monitoring & Detection
  - Analyzing the Attack
  - Response & Recovery
  - Enacting Mitigation Actions

Port Scanning
DNS Zone Transfer

Reconnaissance & Enumeration

- Reconnaissance and Enumeration is the act of scanning a network to determine its layout, hosts, services, users, and other information which may be useful in a cyber attack

Reconnaissance & Enumeration

Some Examples:

- Network mapping – scanning a network to determine what hosts are present
- Port Scanning – scanning a network or hosts to determine what services (ports) are open and what applications are running behind those ports
- Website Crawling – gleaning useful information from publicly available websites
- Cold Calling – asking your personnel sensitive questions
- Running Process Lists – determining what programs are running and on what hosts
- User Accounts – determining what user accounts are available on a host

Reconnaissance & Enumeration

- Why are these attacks important to you?
  - Network attacks are often preceded by these actions and may be an indicator of a future attack

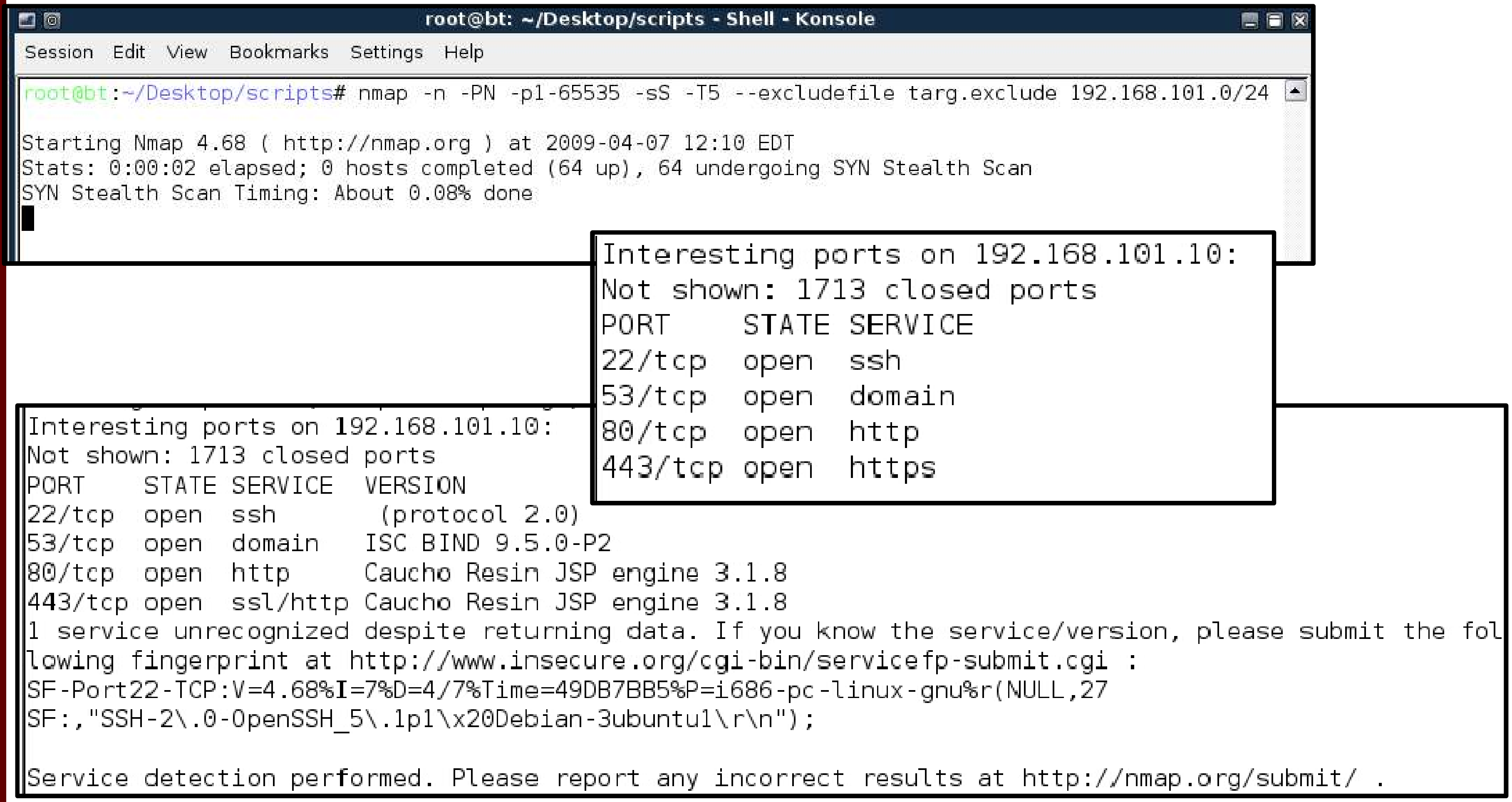
- These attacks may not actually affect your network
  - These attacks may serve as a “smoke screen”
  - Prioritize accordingly

Reconnaissance & Enumeration

Cyber Attack

- Port Scanning -

Attacker’s View



```
root@bt:~/Desktop/scripts# nmap -n -PN -p1-65535 -sS -T5 --excludefile targ.exclude 192.168.101.0/24

Starting Nmap 4.68 ( http://nmap.org ) at 2009-04-07 12:10 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.08% done
```

```
Interesting ports on 192.168.101.10:
Not shown: 1713 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
```

```
Interesting ports on 192.168.101.10:
Not shown: 1713 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh       (protocol 2.0)
53/tcp  open  domain   ISC BIND 9.5.0-P2
80/tcp  open  http     Caucho Resin JSP engine 3.1.8
443/tcp open  ssl/http Caucho Resin JSP engine 3.1.8
1 service unrecognized despite returning data. If you know the service/version, please submit the fol
lowing fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=4.68%I=7%D=4/7%Time=49DB7BB5%P=i686-pc-linux-gnu%r(NULL,27
SF:,"SSH-2\.0-OpenSSH_5\.1p1\x20Debian-3ubuntu1\r\n");

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

Your View

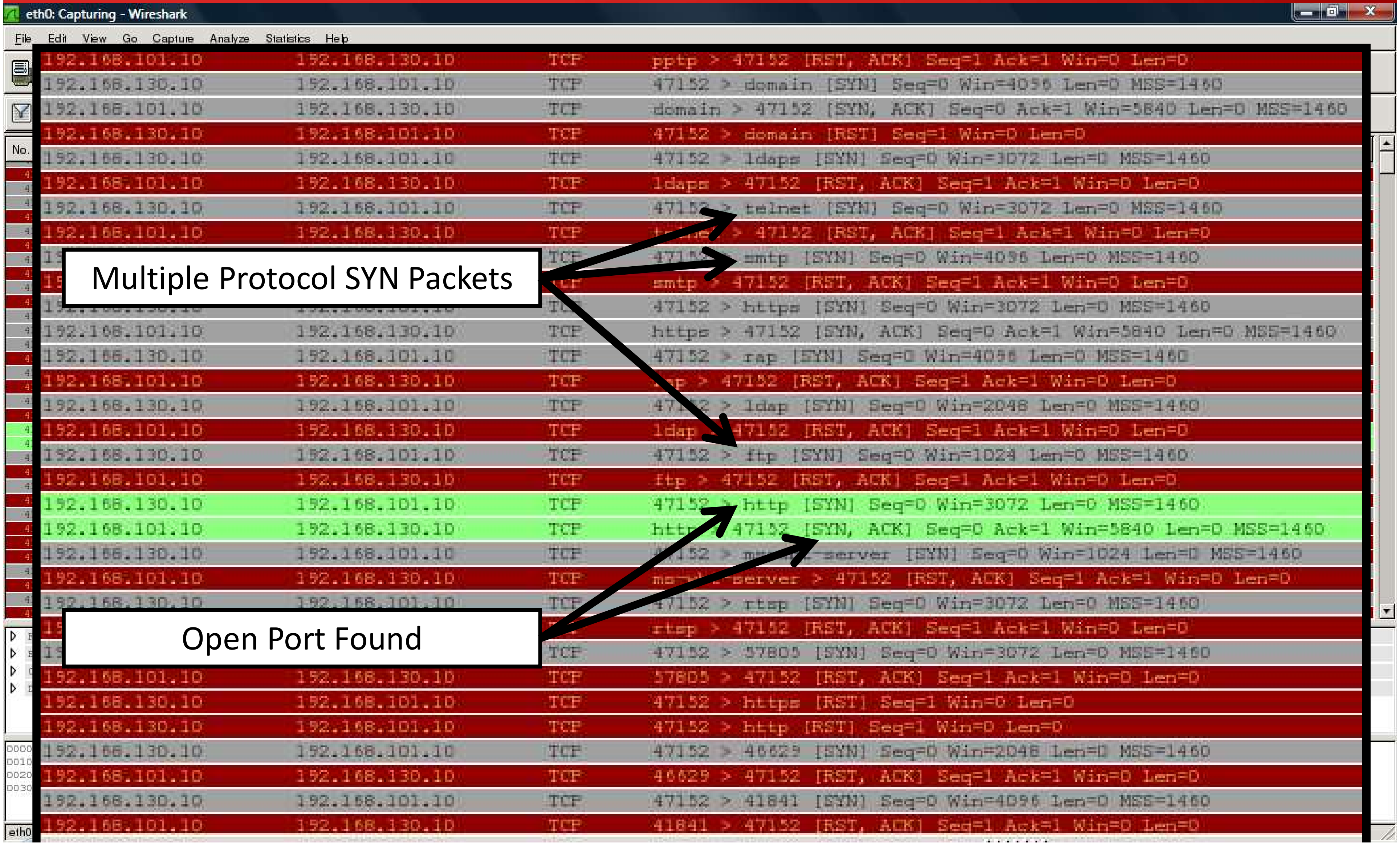
-
  ```
  sudo apt-get install tcpdump
  ```

-
  ```
  sudo tcpdump -n dst 10.101.186.147
  ```

-
  ```
  14:35:54.169249 IP 10.199.1.2.80 > 10.101.186.147.45824: Flags [S.], seq 2190602485, ack 3057500932, win 28960, options [mss 1460,sackOK,TS val 2188886 ecr 538985142,nop,wscale 7], length 0
  ```

-
  ```
  14:35:54.209002 IP 10.199.1.2.81 > 10.101.186.147.54062: Flags [R.], seq 0, ack 2605987418, win 0, length 0
  ```

Your View



eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
No.
eth0

```
192.168.101.10    192.168.130.10    TCP    pptp > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > domain [SYN] Seq=0 Win=4096 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    domain > 47152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.130.10    192.168.101.10    TCP    47152 > domain [RST] Seq=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > ldaps [SYN] Seq=0 Win=3072 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    ldaps > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > telnet [SYN] Seq=0 Win=3072 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    telnet > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
                                    TCP    47152 > smtp [SYN] Seq=0 Win=4096 Len=0 MSS=1460
                                    TCP    smtp > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > https [SYN] Seq=0 Win=3072 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    https > 47152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.130.10    192.168.101.10    TCP    47152 > rap [SYN] Seq=0 Win=4096 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    rap > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > ldap [SYN] Seq=0 Win=2048 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    ldap > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    ftp > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > http [SYN] Seq=0 Win=3072 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    http > 47152 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.130.10    192.168.101.10    TCP    47152 > ms-wbt-server [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    ms-wbt-server > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > rtsp [SYN] Seq=0 Win=3072 Len=0 MSS=1460
                                    TCP    rtsp > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
                                    TCP    47152 > 57805 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    57805 > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > https [RST] Seq=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > http [RST] Seq=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > 46629 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    46629 > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.130.10    192.168.101.10    TCP    47152 > 41841 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
192.168.101.10    192.168.130.10    TCP    41841 > 47152 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Multiple Protocol SYN Packets

Open Port Found

R&E Cyber Attack – Port Scanning

- Hosts on the network frequently have ports open that allow the host to communicate with other hosts on the network and offer services
  - e.g. Port 22 is SSH, Port 80 is WWW
- Port scanning is the act of scanning a host or hosts to determine what ports are open and closed

R&E Cyber Attack – Port Scanning

- Malicious actors use this technique to:
  - Determine what applications are remotely accessible on the host
  - Determine version or other useful information for those applications

- Why?
  - Build target lists for specific attacks
  - Curiosity

R&E Cyber Attack – Port Scanning

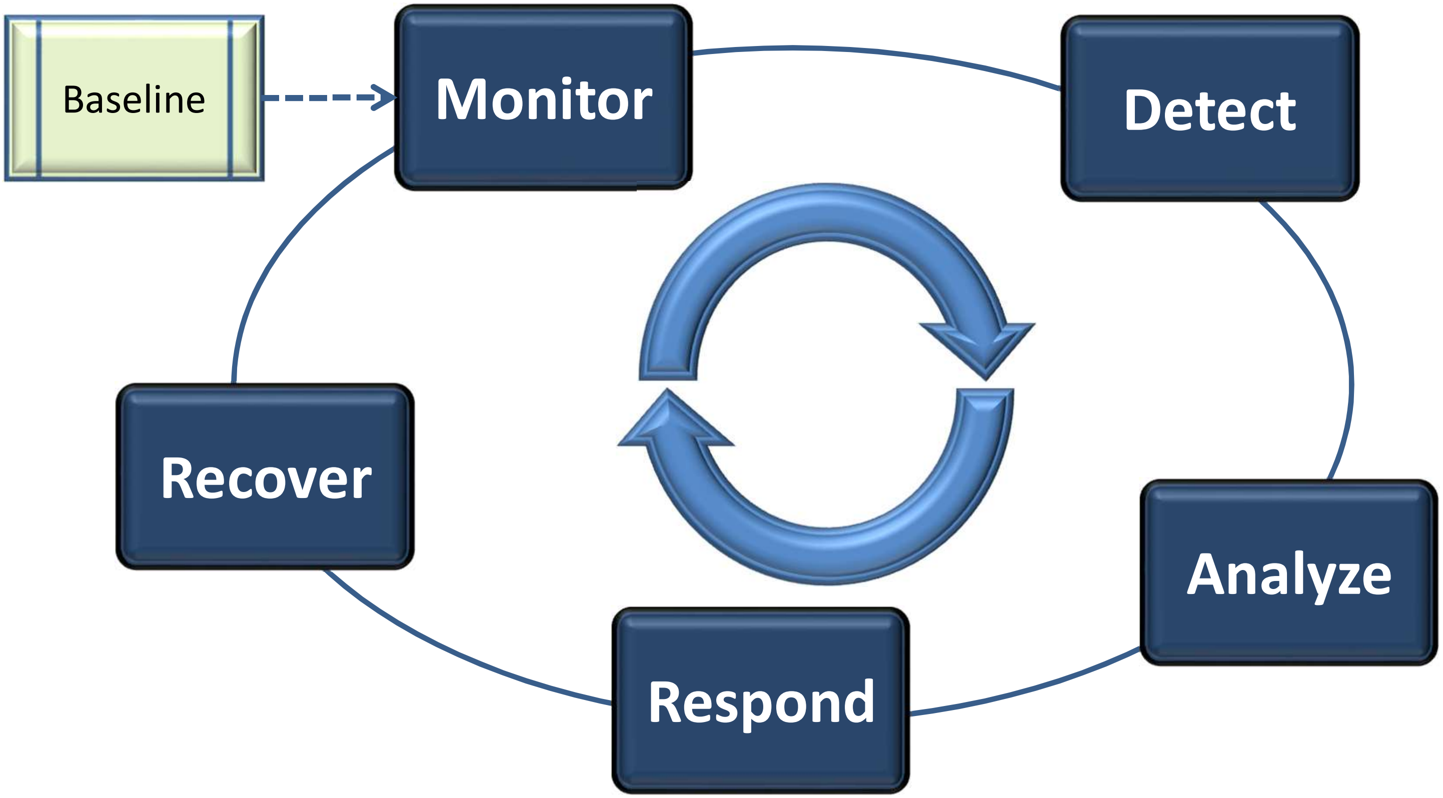
- Port scanning uses standard network protocols to query a host to find open ports and information

- This attack targets hosts that are remotely accessible and have services that are also remotely accessible

R&E Cyber Attack – Port Scanning

Website Graphic
Version & Port Information

R&E Cyber Attack – Port Scanning



Baseline

Monitor

Detect

Analyze

Respond

Recover

R&E Cyber Attack – Port Scanning

- Establish a Baseline for What's Normal for Your Network:
  - Do you have applications that regularly scan your network (e.g. vulnerability assessment tools)?
  - Do you have administrators that regularly scan your network looking for rogue devices?

- Use this baseline to compare what you currently see to what you expect
  - Any differences are a good indication of something going on!

Start Exercise on Port Scanning

R&E Cyber Attack – Port Scanning

Attack Demonstration

R&E Cyber Attack – Port Scanning

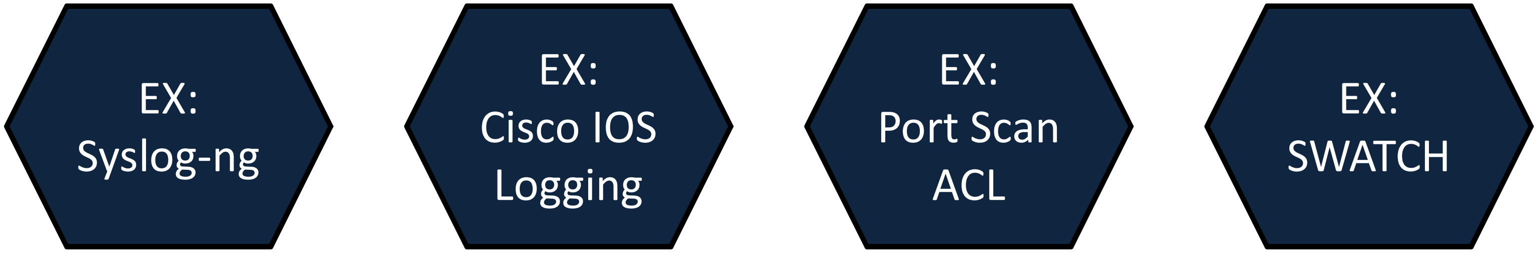
- Monitoring & Detection
  - Router ACLs & Logging
  - Log Analysis

Log Management

Cisco Configuration Elements

R&E Cyber Attack – Port Scanning

- Monitoring & Detection
  - Configure your network to detect port scanning
  - Monitor your detection tool(s)
  - Establish a Baseline



EX: Syslog-ng

EX: Cisco IOS Logging

EX: Port Scan ACL

EX: SWATCH

R&E Cyber Attack – Port Scanning

Attack Demonstration

(This time you can see how your network views the attack)

R&E Cyber Attack – Port Scanning

- Analysis - what did your detection tools report? Is this really an attack?
  - Router ACL Logging
  - Log Analysis
- Where is attack coming from?
- Are any IPs or Ports of particular interest?
  - Are there any recent attacks targeting these applications, operating systems, etc?
- Are there any patterns?

R&E Cyber Attack – Port Scanning

- Response Actions
  - aka "I'm Under Attack – What Do I Do Now?!"

  1) Prioritize – is anything else happening?
  2) If analysis indicates particular interest in an IP or Port, and a vulnerability exists, patch it or block it!

- Blocking source IPs is a losing game – a dedicated attacker can switch sources at the drop of a hat
  - Too many firewall rules make things ungainly & slow
  - If you choose to block it (and you can!), put it in for a set period of time (say 2 weeks), then remove it. This takes firewall discipline!

R&E Cyber Attack – Port Scanning

- Recovery Actions
  - The attack is over – how do I prevent this again?

1) Ask yourself “What _*could*_ have happened here?”
2) Consider “whitelisting” for critical applications that only certain people need to access
3) Other “mitigation” strategies… What is appropriate for your network & resources?

R&E Cyber Attack – Port Scanning

- What Other Mitigation Steps Would You Take?
  - Please don't make any changes right now – it may affect the other attacks we want to demonstrate!

? DISCUSSIONS ??

Adding a firewall - See Exercise

- `sudo apt-get install iptables ulogd`
- `create iptables: (see exercise)`
- `sudo iptables-restore --verbose < iptables`

R&E Cyber Attack – Port Scanning

Final Attack Demonstration

R&E Cyber Attack – Port Scanning

- Attack Discussion
  - Did the mitigation steps help?
  - How else can you protect your network?
- Other Thoughts Before We Move On?

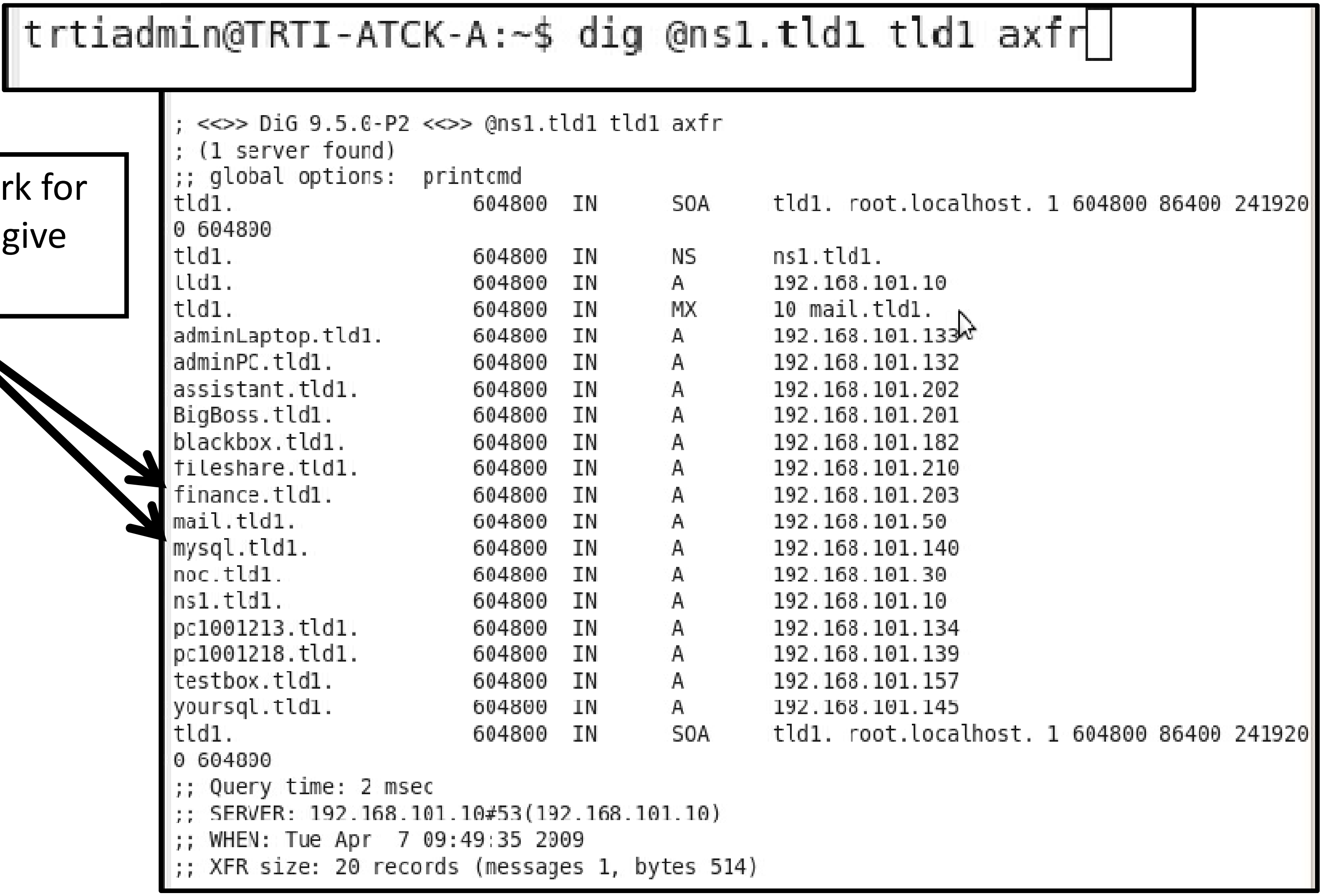
Reconnaissance & Enumeration

Cyber Attack

- Zone Transfer -

Attacker's View

Make them work for targets….don't give 'em away…..



```
trtiadmin@TRTI-ATCK-A:~$ dig @ns1.tld1 tld1 axfr
```

```
; <<>> DiG 9.5.0-P2 <<>> @ns1.tld1 tld1 axfr
; (1 server found)
;; global options:  printcmd
tld1.                   604800  IN      SOA     tld1. root.localhost. 1 604800 86400 241920
0 604800
tld1.                   604800  IN      NS      ns1.tld1.
tld1.                   604800  IN      A       192.168.101.10
tld1.                   604800  IN      MX      10 mail.tld1.
adminLaptop.tld1.       604800  IN      A       192.168.101.133
adminPC.tld1.           604800  IN      A       192.168.101.132
assistant.tld1.         604800  IN      A       192.168.101.202
BigBoss.tld1.           604800  IN      A       192.168.101.201
blackbox.tld1.          604800  IN      A       192.168.101.182
fileshare.tld1.         604800  IN      A       192.168.101.210
finance.tld1.           604800  IN      A       192.168.101.203
mail.tld1.              604800  IN      A       192.168.101.50
mysql.tld1.             604800  IN      A       192.168.101.140
noc.tld1.               604800  IN      A       192.168.101.30
ns1.tld1.               604800  IN      A       192.168.101.10
pc1001213.tld1.         604800  IN      A       192.168.101.134
pc1001218.tld1.         604800  IN      A       192.168.101.139
testbox.tld1.           604800  IN      A       192.168.101.157
yoursql.tld1.           604800  IN      A       192.168.101.145
tld1.                   604800  IN      SOA     tld1. root.localhost. 1 604800 86400 241920
0 604800
;; Query time: 2 msec
;; SERVER: 192.168.101.10#53(192.168.101.10)
;; WHEN: Tue Apr  7 09:49:35 2009
;; XFR size: 20 records (messages 1, bytes 514)
```

R&E Cyber Attack – Zone Transfer

- The DNS allows a “Zone Transfer” to keep secondary servers in sync with their master
  - This is a *normal* part of DNS operations
- A zone transfer copies all the data in the zone file from the DNS server to the requester

R&E Cyber Attack – Zone Transfer

- Malicious actors use this technique to:
  - Easily determine what domains are registered (and therefore, which ones are not)
  - Easily determine key servers and hosts that are publicly accessible (why else would they be in the DNS?)
  - Easily find potentially sensitive information DNS zone administrators have left in their zone files

- Why?
  - Build target lists for attacks
  - Potentially find key hosts (i.e. administrators workstation) to attack

R&E Cyber Attack – Zone Transfer

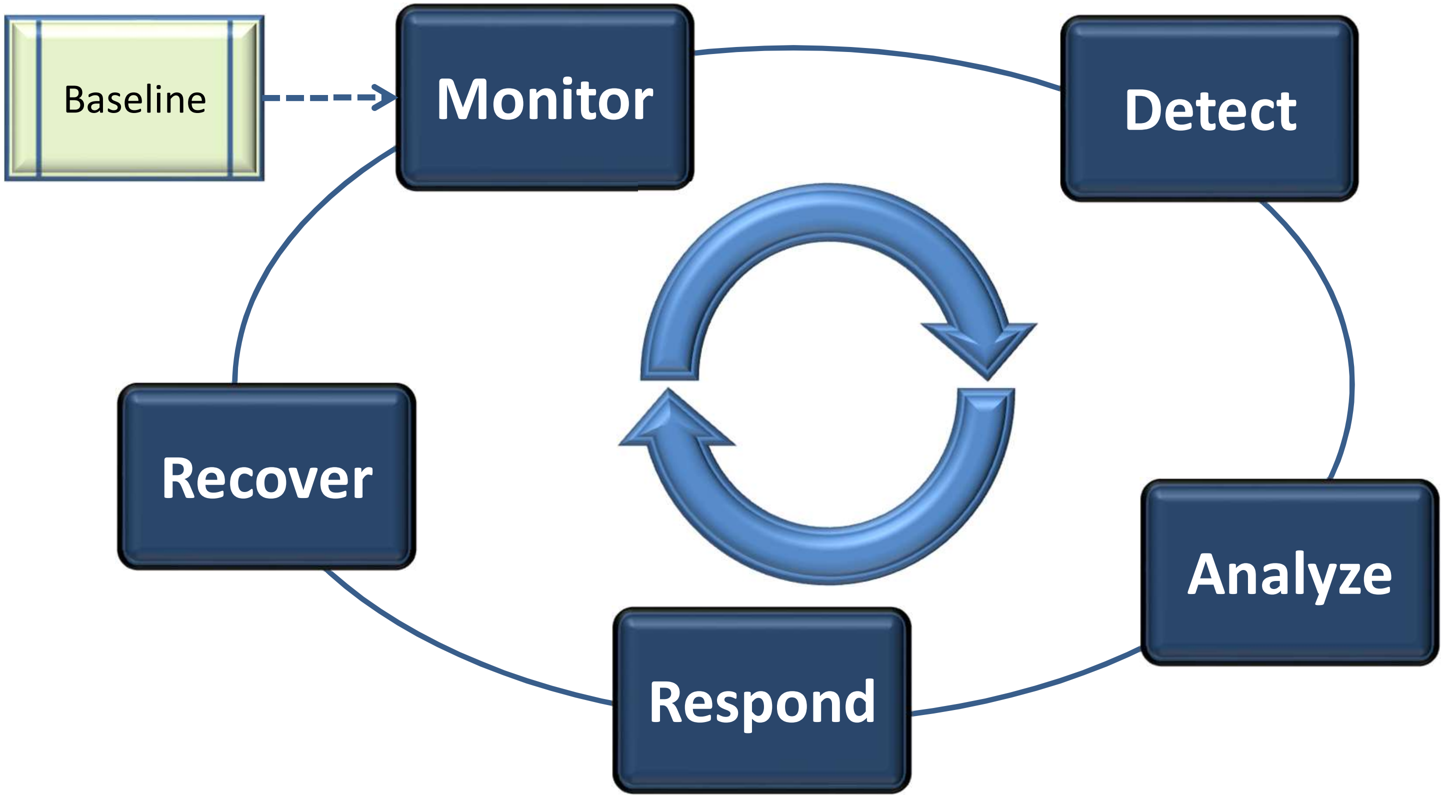
- Zone transfers use standard DNS protocols to transfer data from a server

- This attack targets authoritative DNS servers that are remotely accessible and allow zone transfers from “unverifiable” sources

R&E Cyber Attack – Zone Transfer

Sample Output from Zone Transfer

R&E Cyber Attack – Zone Transfer



Baseline

Monitor

Detect

Analyze

Respond

Recover

R&E Cyber Attack – Zone Transfer

- Establish a Baseline for What’s Normal for Your Network:
  - What servers are supposed to conduct zone transfers?
  - Don’t forget the time component – When are zone transfers supposed to occur?
  - Do you administrators conduct zone transfers to check the contents of their zones?
  - Do you have applications that do this?

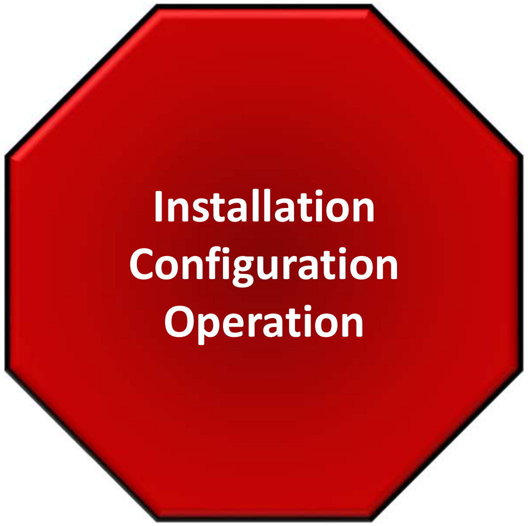
- Use this baseline to compare what you currently see to what you expect
  - Any differences are a good indication of something going on!

R&E Cyber Attack – Zone Transfer

Attack Demonstration

R&E Cyber Attack – Zone Transfer

- Monitoring & Detection
  - BIND (or DNS Server) Configuration
  - Log Analysis



Installation
Configuration
Operation

R&E Cyber Attack – Zone Transfer

- Monitoring & Detection
  - Configure your network to detect zone transfers
  - Monitor your detection tool(s)
  - Establish a Baseline

EX: Zone Transfer Detection

R&E Cyber Attack – Zone Transfer

Attack Demonstration

(This time you can see how your network views the attack)

R&E Cyber Attack – Zone Transfer

- Analysis - what did your detection tools report? Is this really an attack?
- Did a zone transfer actually occur?
  - Log Analysis
- Where is attack coming from?

R&E Cyber Attack – Zone Transfer

- Response Actions
  - – aka “I’m Under Attack – What Do I Do Now?!”
  1) Prioritize – is anything else happening?
  2) If analysis determines a zone transfer occurred to an unauthorized host, what was compromised?
     - If anything sensitive was compromised – take appropriate action!

R&E Cyber Attack – Zone Transfer

- Recovery Actions
  - The attack is over – how do I prevent this again?

1) Ask yourself “What _*could*_ have happened here?”
2) Scrub zone file for any sensitive information…
3) Configure DNS server to only allow zone transfers from authorized hosts (“whitelisting”)
4) Other “mitigation” strategies… What is appropriate for your network & resources?

R&E Cyber Attack – Zone Transfer

- What Mitigation Steps Would You Take?
  - Configuring BIND to allow authorized zone transfers…

? DISCUSSIONS ??

EX: Zone Transfer Mitigation

R&E Cyber Attack – Zone Transfer

Final Attack Demonstration

R&E Cyber Attack – Zone Transfer

- Attack Discussion
  - Did the mitigation steps help?
  - How else can you protect your network?
- Other Thoughts Before We Move On?

QUESTIONS?

- Do you have any questions about …
  - Reconnaissance & Enumeration
  - Detecting This Type of Attack
  - Responding & Recovering From This Type of Attack