Northwestern University
MSIT 458
Information Security

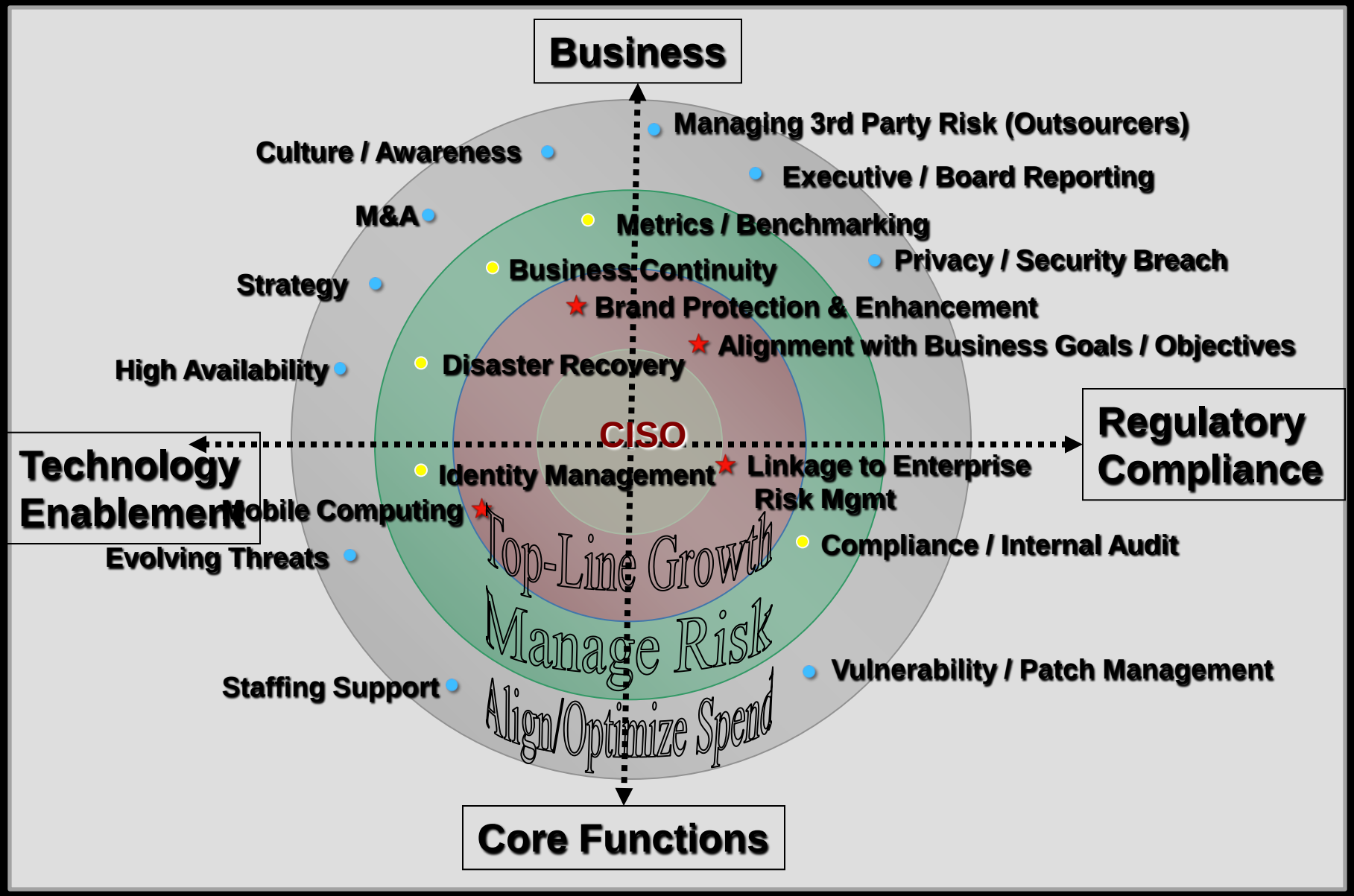
Security Policy
&
Ethical Hacking

Brandon Hoffman KPMG, LLP

Topics for Discussion

- IT Security in the Business
  - Risk, Audit Support, Compliance
- Policies, Standards, and Procedures
  - IT Security's Role in Creation and Enforcement
- Typical IT Security Technical Work
  - Ethical Hacking/Penetration Testing
  - Backtrack 4
  - Common Methods and Sample Outputs

The CISO Agenda



Risk

IT Security performs a critical role in assessing risk in the organization.

- Vulnerability Scanning
- Penetration Testing
- Industry Trends
- IT Strategy
- Familiarity with Audit and Compliance measures

Audit Support

In many cases, IT Security is heavily relied upon to perform in depth testing required by an audit organization. Security is enlisted by audit because:

- Technical expertise
- Familiarity with current issues from internal testing
- Familiarity with Policies, Standards, and Procedures

Compliance

Compliance may relate to internal compliance or external compliance.

Internal compliance:

- Policies and Standards
- Security and Configuration baselines
- Framework use – ISO, COBIT, ITIL, GAISP, NIST
- Best Practices

Compliance cont'd

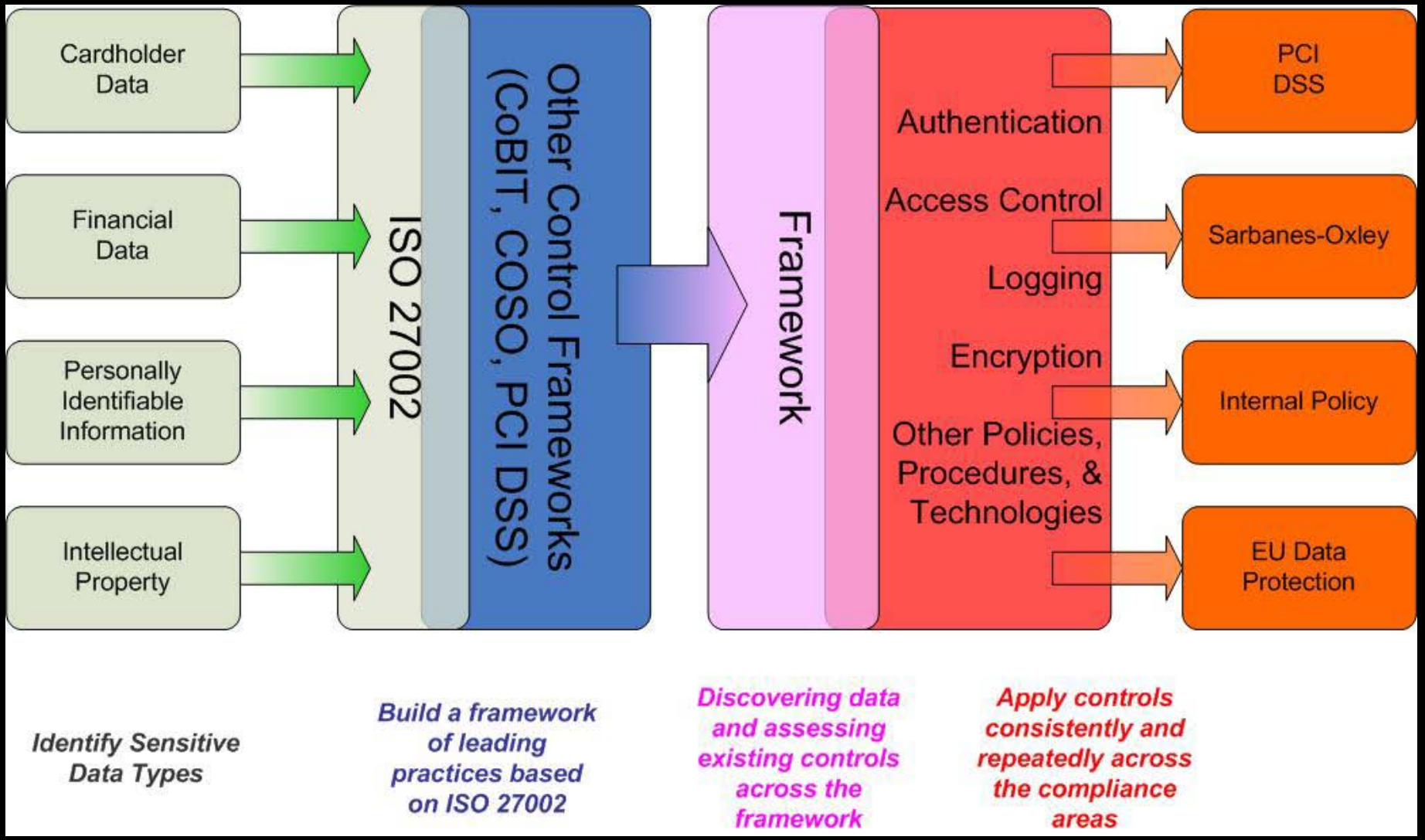
External compliance:

- SOX (Sarbanes Oxley)
  - COSO Framework
- HIPAA
- PCI
- Safe Harbor

ISO Leading Practices

ISO 27002 Best Practice	NIST	PCI DSS	SOX	HIPAA
4. Risk Assessment and Treatment	✓	✓	✓	✓
5. Security Policy	✓	✓	✓	✓
6. Organization of Information Security	✓			✓
7. Asset Management	✓		✓	✓
8. Human Resources Management	✓			✓
9. Physical and Environmental Security	✓	✓	✓	✓
10. Communications and Operations Management	✓	✓	✓	✓
11. Access Control	✓	✓	✓	✓
12, Information Systems Acquisition, Development and Maintenance	✓	✓	✓	✓
13. Information Security Incident Management	✓	✓	✓	✓
14. Business Continuity Management	✓		✓	✓
15. Compliance	✓		✓	✓

Compliance in Action



Internal Policy

IT Security is regularly tasked with creation and enforcement of IT policies, standards, and procedures. Creation and enforcement of these documents require:

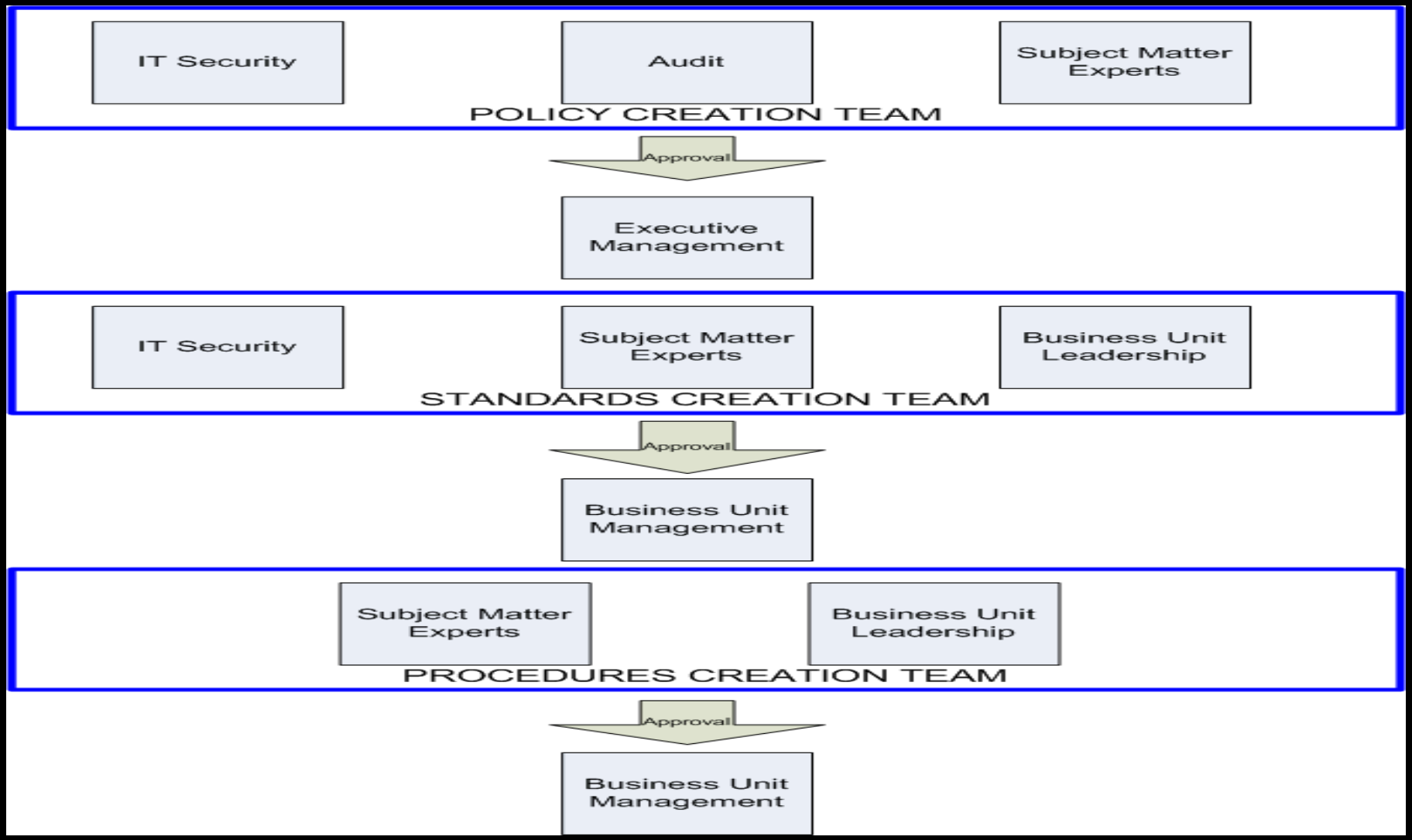
- Understanding of audit roles and procedures
- Familiarity with all systems, networks, and applications
- Compliance considerations

Internal Policy cont'd

Definitions:

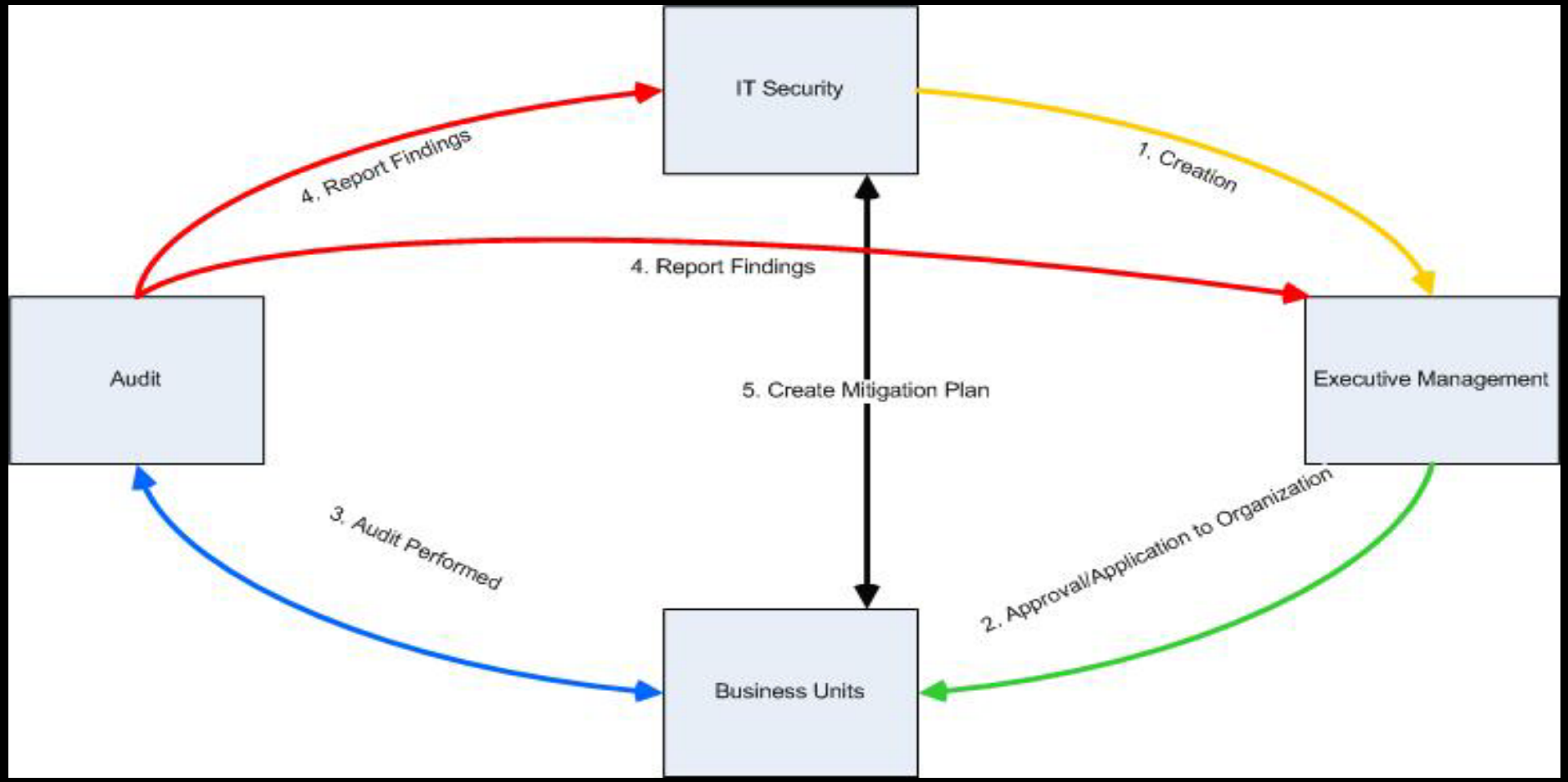
- A **Policy** is a set of directional statements and requirements aiming to protect corporate values, assets and intelligence. Policies serve as the foundation for related standards, procedures and guidelines.
- A **Standard** is a set of practices and benchmarks employed to comply with the requirements set forth in policies. A standard should always be a derivation of a policy, as it is the second step in the process of a company's policy propagation.
- A **Procedure** is a set of step-by-step instructions for implementing policy requirements and executing standard practices.

Internal Policy cont'd



Internal Policy cont'd

Policy creation and enforcement cycle



Policy Business Case

A top 5 global food retailer has a massive IT/IS infrastructure and good governance….but no real policies!

Policies are the foundation for enforcing IT compliance and governance.

What policies were written for the client…

Policy Business Case cont'd

Policies written for IT Security:

- Acceptable Use Policy
- Information Classification & Ownership Policy
- Risk Assessment & Mitigation Policy
- Access Control Policy
- Network Configuration and Communication Policy
- Remote Access Policy
- Business Continuity Policy
- Incident Response Policy
- Third Party Data Sharing Policy
- System Implementation & Maintenance
- Secure Application Development
- Cryptography & Key Management
- Mobile Computing
- Physical & Environmental Security

Policy Business Case cont'd

Sample Policies

Cryptography and
ey Management Polic

Network
Configuration Policy

Ethical Hacking

Ethical hacking is a very common profession within the IT security industry.

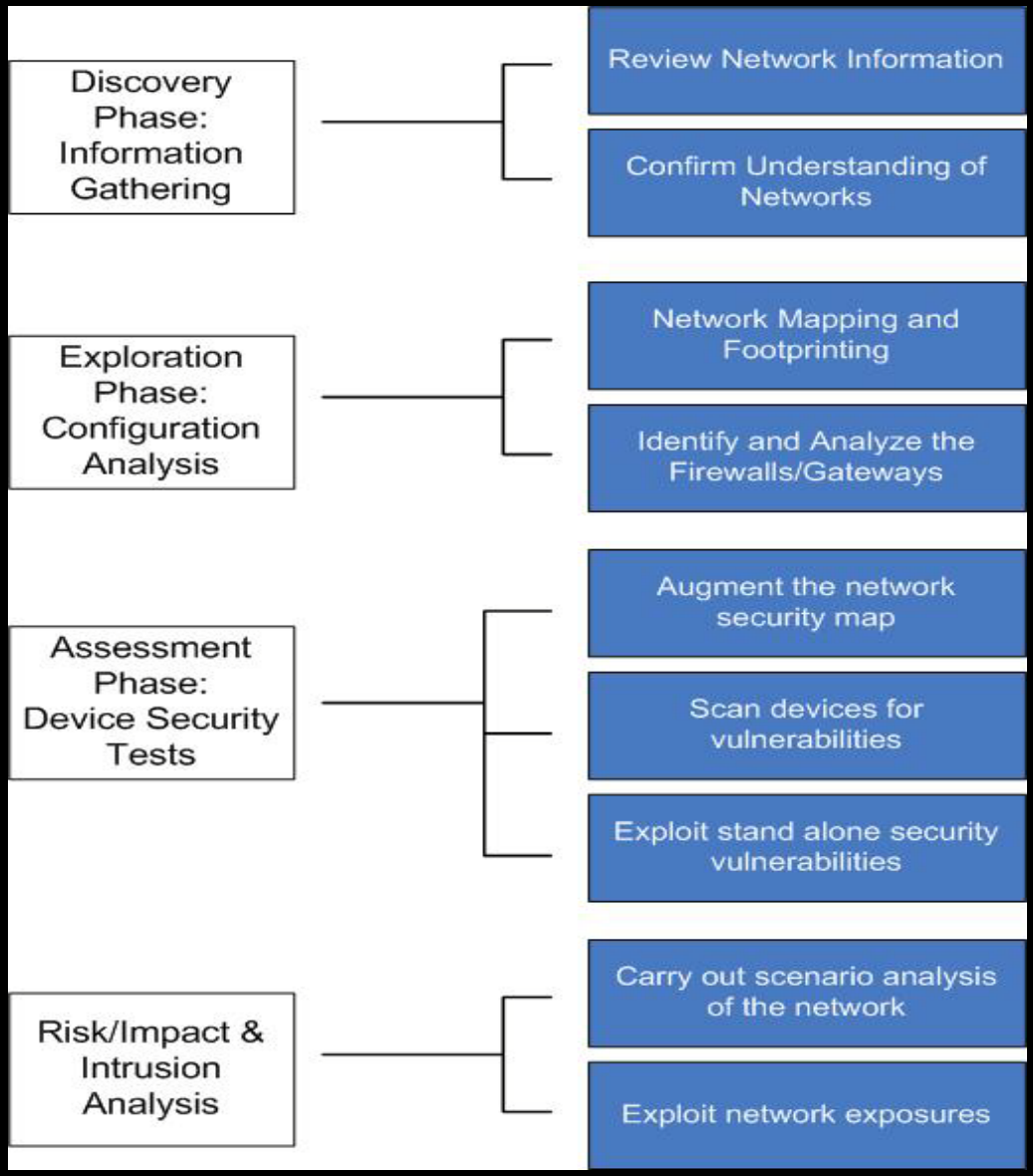
- White hat, Grey hat, Black hat
- Sometimes synonymous with penetration testing – A method of assessing the security posture of a system or network by simulating an “attack”

Ethical Hacking

Why perform an ethical hack?

- Determine flaws and vulnerabilities
- Provide a quantitative metric for evaluating systems and networks
- Measure against pre-established baselines
- Determine risk to the organization
- Design mitigating controls

Ethical Hacking



Ethical Hacking

Administrative items:

- Authorization letter – “Get out of jail free card”
- Risk report
  - Likelihood of risk
  - Mitigation plans
  - Trends (performed with recurring clients)

Backtrack

- Backtrack is a Linux based hacking toolkit provided by the people at www.remote-exploit.com
- It includes a massive amount of hacking tools all for free ☺
- Compile tools yourself? Maybe check this out instead.

Backtrack

- Tool categories in BT4:
  - Digital Forensics
  - Information Gathering
  - Access Maintenance
  - Network Mapping
  - Penetration
  - Privilege Escalation
  - Radio Network Analysis (Wireless)
  - Reverse Engineering
  - VOIP
  - Vulnerability Identification
  - Web Applications
  - Miscellaneous

Backtrack

- Backtrack Demo

Backtrack

- Ways to use backtrack
  - Live CD: The most popular method
    - No state save
    - Highly portable
  - USB Drive/Stick
    - Highly portable (more so than CD)
    - Can make stateful
    - Prone to loss
  - Full HD install
    - Using your machine as a “hacktop”
    - Dual boot
  - Virtual Machine
    - Networking gets tricky
    - Resource availability

Wanna Break In?

The first step in any ethical hack is to obtain information in the most stealth fashion.

NMAP

Powerful free linux tool – www.insecure.org

Syntax:

nmap [*<Scan Type>* ...] [*<Options>*] { *<target specification>* }

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

NMAP cont'd

HOST DISCOVERY:

-sL: List Scan - simply list targets to scan
-sP: Ping Scan - go no further than determining if host is online
-PN: Treat all hosts as online -- skip host discovery
-PS/PA/PU[portlist]: TCP SYN/ACK or UDP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO[protocol list]: IP Protocol Ping
-n/-R: Never do DNS resolution/Always resolve [default: sometimes]
--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host

SCAN TECHNIQUES:

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
--scanflags <flags>: Customize TCP scan flags
-sI <zombie host[:probeport]>: Idle scan
-sO: IP protocol scan
-b <FTP relay host>: FTP bounce scan

NMAP cont'd

PORT SPECIFICATION AND SCAN ORDER:

-p <port ranges>: Only scan specified ports

Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080

-F: Fast mode - Scan fewer ports than the default scan

-r: Scan ports consecutively - don't randomize

--top-ports <number>: Scan <number> most common ports

--port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info

--version-intensity <level>: Set from 0 (light) to 9 (try all probes)

--version-light: Limit to most likely probes (intensity 2)

--version-all: Try every single probe (intensity 9)

--version-trace: Show detailed version scan activity (for debugging)

NMAP cont'd

OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in milliseconds, unless you append 's'
  (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <time>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second

NMAP cont'd

FIREWALL/IDS EVASION AND SPOOFING:

-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP checksum

NMAP cont'd

OUTPUT:
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use twice or more for greater effect)
-d[level]: Set or increase debugging level (Up to 9 is meaningful)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

NMAP cont’d

Analyze your results:

NMAP OUTPUT PRINTED

Vulnerabilities

Find any hosts worthwhile? Your nest step should be scanning for exploitable vulnerabilities.

Nessus

Nessus scans based on an exhaustive list of vulnerabilities for all platforms of computing. Custom scripts are written by Nessus and their team to check for a vulnerable software component.

Nessus Sample Report

How Do We Exploit?

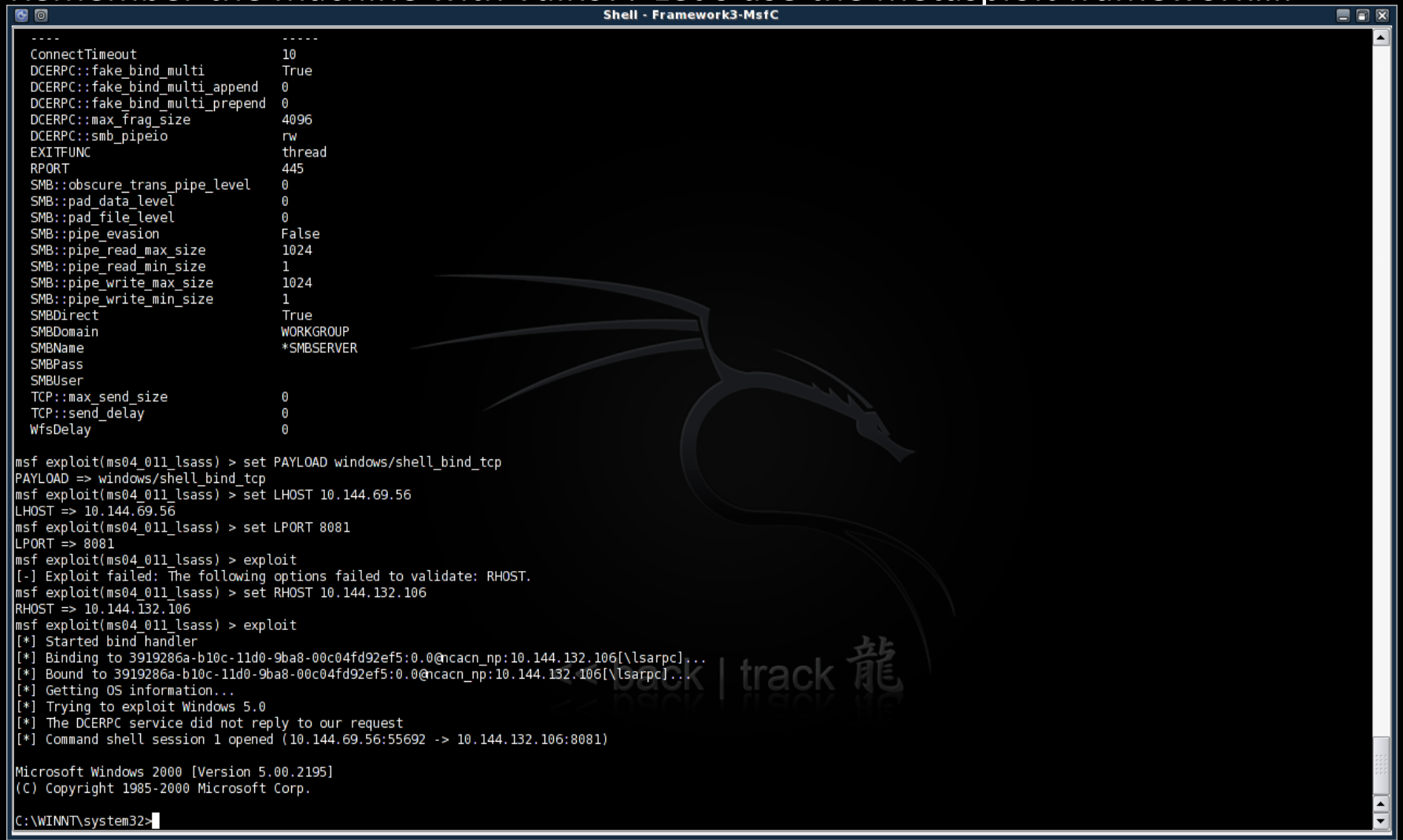
Now that you have found a useful exploit, what do we use?

MetaSploit

Metasploit was created in 2003 as a portable network game using the Perl scripting language. Later, the Metasploit Framework was then completely rewritten in the Ruby programming language. It is most notable for releasing some of the most technically sophisticated exploits to public security vulnerabilities. In addition it is a powerful tool for third party security researchers to investigate potential vulnerabilities.

MetaSploit cont'd

Remember the machine with vulns?? Let's use the metasploit framework….



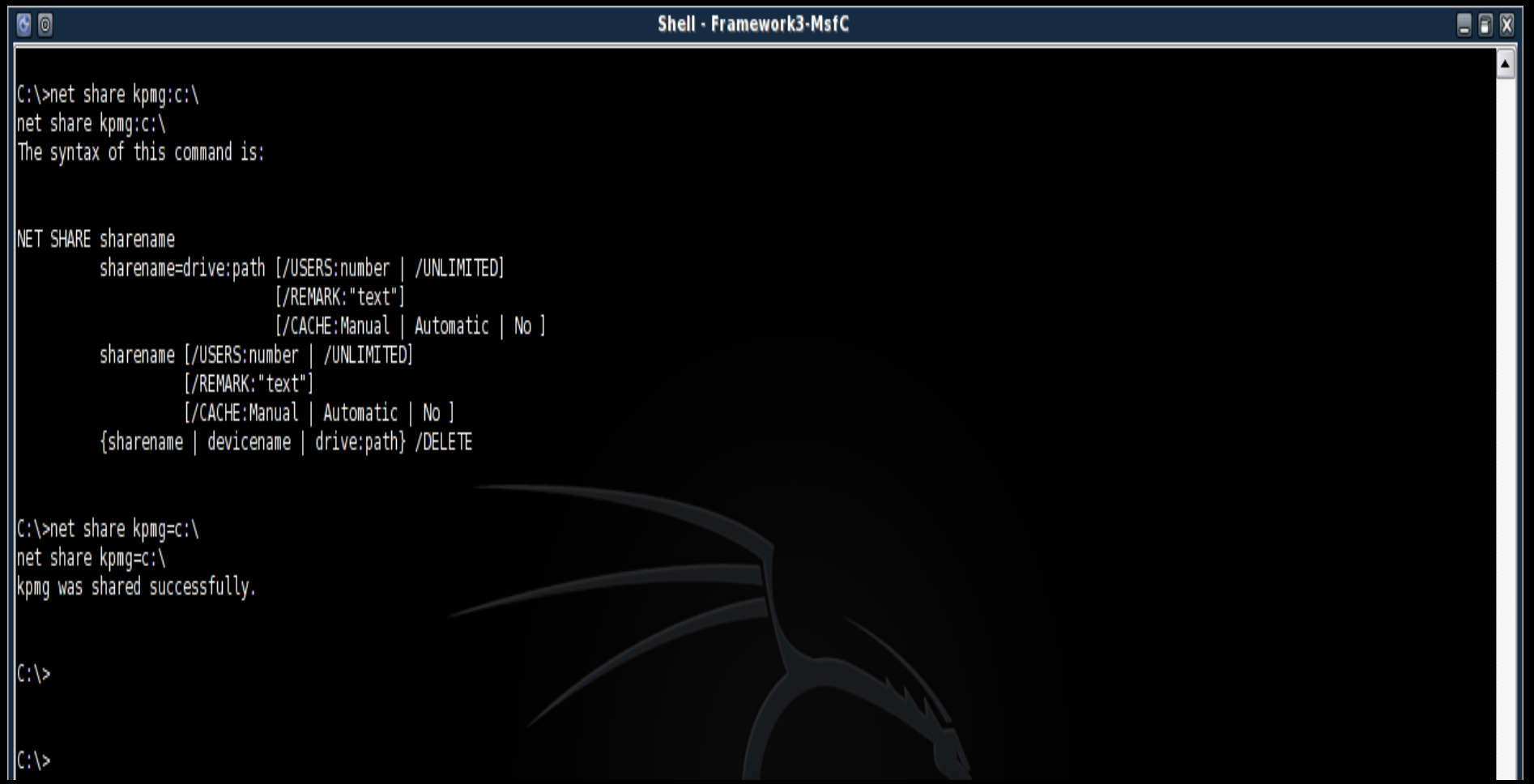
MetaSploit cont'd

What else can we do now that were in???

```
C:\>net user bhoffman kpmg /ADD
net user bhoffman kpmg /ADD
The command completed successfully.


C:\>net user bhoffman /ADD
net user bhoffman /ADD
The account already exists.

More help is available by typing NET HELPMSG 2224.


C:\>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            ASPNET                   bhoffman
Guest                    IUSR_ARIES               IWAM_ARIES
Liz                      TsInternetUser
The command completed with one or more errors.


C:\>
```

MetaSploit cont'd

We can add shares as root!!

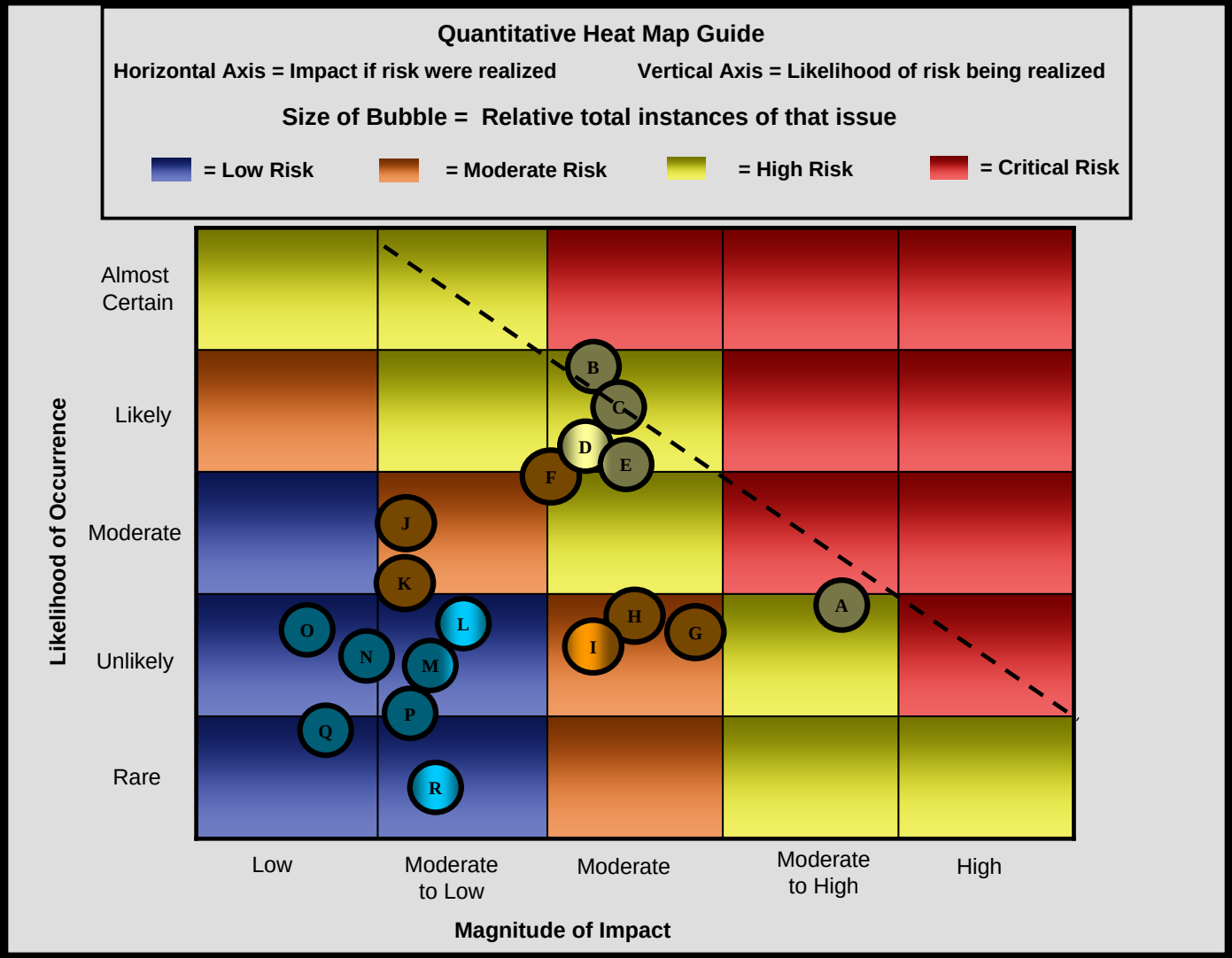


Ethical Hacking cont'd

Administrative items:

- Authorization letter – "Get out of jail free card"
- Risk report
  - Likelihood of risk
  - Mitigation plans
  - Trends (performed with recurring clients)

Ethical Hacking cont'd



Q & A

ANY QUESTIONS?